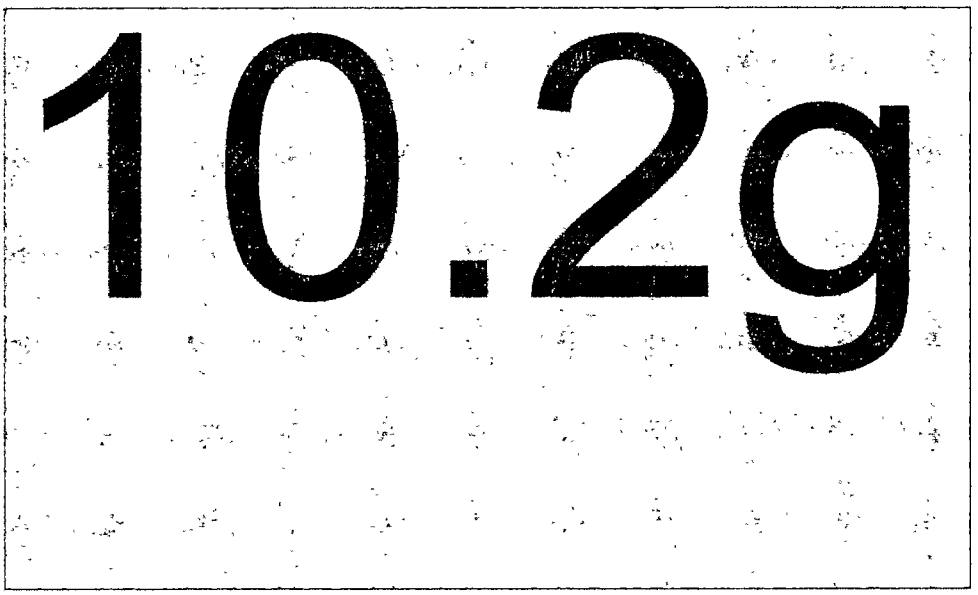
In het beheerportaal is het mogelijk om berichten te schrijven en te bewerken:



In het voorbeeld hierboven is te zien dat er een afbeelding wordt toegevoegd met als URL `http://10.234.171.16:1234`. Zodra een gebruiker het bericht bezoekt stuurt de browser een verzoek naar die URL om de afbeelding te kunnen tonen. Hieronder is te zien dat de machine met IP-adres 10.234.171.16 een verzoek binnenkrijgt op poort 1234:

```
root@kali:/# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.234.171.16] from (UNKNOWN) [10.234.171.16] 36508
GET / HTTP/1.1
Host: 10.234.171.16:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

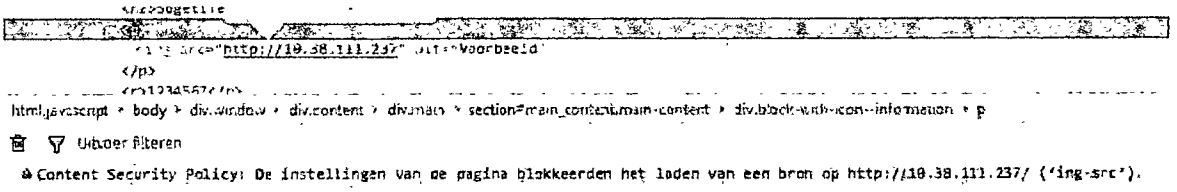
Het is belangrijk om op te merken dat het momenteel alleen binnen het beheerportaal mogelijk is om op deze manier verzoeken naar andere domeinen te doen; binnen dit portaal wordt de CSP-header[2] niet gebruikt waardoor het mogelijk is afbeeldingen van andere domeinen in te laden. In de DigiD-applicatie voor burgers wordt de CSP-header wel gebruikt, waardoor moderne browsers het inladen van afbeeldingen van andere domeinen zullen tegenhouden.

Een 'afbeelding' die een verzoek uitvoert *binnen* het DigiD-domein zal ook werken binnen de DigiD-applicatie voor burgers; Hierdoor kan een beheerder eventueel verzoeken binnen DigiD uitvoeren namens burgers.

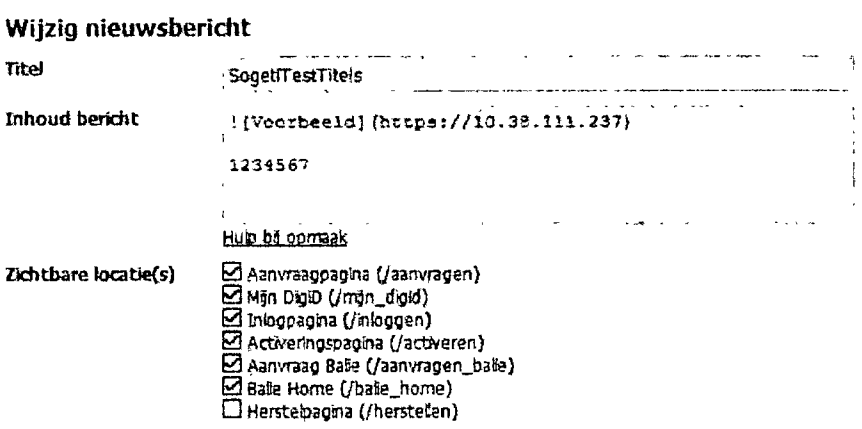
Update hertest:
De bevinding is nog steeds aanwezig. In de DigiG-applicatie voor burgers zorgt de CSP-header er voor dat deze content niet wordt geladen:

[2] *Content Security Policy, zie ook https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP en bevindingen* ***Error! Reference source not found.*** *en* ***Error! Reference source not found.*** *in dit rapport.*

derubricering



Op de beheeromgeving wordt de pagina echter nog steeds geladen, in dit geval door de HTTPS-versie aan te roepen:




```
<strong>Inhoud</strong>

<div class='form_wrapper' id='news_item' style='padding: 4px; width:
400px; height: 130px; margin-top: 4px; overflow: auto'><p><img
src="https://10.38.111.237" alt="Voorbeeld"></p>


<p>1234567</p>

</div>

</div>

</div>
```

4.1.7 *Directe gebruikersnaam enumeratie*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.8	Nnb	Zeer laag	Zeer laag	Laag

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het systeem geeft informatie over het bestaan van gebruikersnamen.

Bedreiging

Kennis over bestaande gebruikersnamen geeft een aanvaller mogelijkheden voor verdere aanvallen. Het systeem kan aangevallen worden door bijvoorbeeld een bruteforce aanval uit te voeren op de gebruikersnamen. De gebruiker kan aangevallen worden door een denial-of-service aanval middels account blokkades, of social engineering wanneer email addressen achterhaald kunnen worden.

Aanbeveling

Het systeem maar dient generieke meldingen te tonen die geen informatie geeft over het bestaan van gebruikersnamen. Bijvoorbeeld voor een wachtwoord vergeten functionaliteit: "Indien het account bestaat, zijn de instructies voor het wijzigen van het wachtwoord verzonden".

Details

De Mijn DigiD-omgeving biedt in het scherm gebruiksgeschiedenis aan de eindgebruiker de mogelijkheid om in te zien welke acties zijn uitgevoerd op de omgeving. Wanneer het account voor de eerste keer wordt geactiveerd, dan wordt de gebruikersnaam getoond in de geschiedenis:

```
<tr class='table-row'>
<td class='table-cell--history-date'>20-11-2017 11:39:06</td>
<td class='table-cell'>Activeren gelukt (u_000000036, basis)</td>
</tr>
```

In het geval dat een sessie wordt overgenomen, dan kan de aanvaller via de geschiedenis de gebruikersnaam achterhalen. Dit is een zeer laag risico, maar voor *defence in depth* is het aanbevolen om geen gebruikersnamen te tonen binnen de omgeving.

5 PAP eisen

Hieronder wordt van de eisen uit het document aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

Id	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Geen bevindingen		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
Reflection injection aanwezig (Bevinding 6)		
ACC2.2.3	DigID bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Geen bevindingen		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en tolerantles Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.	DNSSEC
Geen bevindingen		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der	Ingetrokken certificaten

	Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is
Geen bevindingen	

6 Bijlagen

6.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

6.1 Aanpak

Tijdens de test wordt een groot aantal controles uitgevoerd. Hierbij wordt onder andere gebruikgemaakt van een checklist op basis van de *Web Application Hacker's Handbook* met de volgende onderdelen:

Logic	Client-side checks	Hidden fields
		Cookies - HTTP / Secure flag etc.
		Local privacy vulnerabilities
		Autocomplete forms
		Preset parameters
		ASP.net ViewState
		Field length limit
		Javascript Validation
		ClickJacking
		Disabled elements
		Java applets
		ActiveX
		Shockwave Flash
		Executables
	Logic Errors	Multistage
		Incomplete input
		Transaction logic
Authentication	Direct attacks	Password quality rules
		Username enumeration

		Password guessing
	Speciale functies	Account recovery
		Remember me functions
		Impersonation / Account hijacking
	Managing credentials	Username uniqueness
		Credential predictability
		Unsafe transmission
		Unsafe distribution
	Logic Errors	Autentication errors
		Fail-open conditions
		Multistage
Session management	Generation	Token logic/meaning
		Token predictability
	Handling	Insecure transmission of tokens
		Token disclosure in logs
		Mapping of tokens to sessions
		Concurrent sessions
		Session termination
		Fixation
		CSRF
		Caching
		Persistent cookies
		Fixed session ID
		Cookie Scope
Access	Segregation	Different accounts
		Insecure access control method
		Horizontal Privilige escalation
		Vertical Privilige escalation
	Controle	Anonymous
Input handling	Fuzzing	SQL injection
		Reflected XSS
		Stored XSS
		OS Command injection
		Path traversal
		Script Injection
		File upload fields
		File Inclusion
	Functie specifiek	SMTP injection
		Code flaws
		DOM-based attacks
		Frame injection
		HTTP Header Injection
		Arbitrary Redirection

		SOAP injection
		LDAP injection
		XPATH injection
Environment	Interfaces	Segregation in shared infrastructures
		Segregation between ASP-hosted apps
Server	Implementation	Default credentials
		Default content
		HTTP method
		Proxy
		Virtual hosting
	Software	Native software flaws
		Known vulnerabilities
	Configuration	Known bugs
		Services
		Disclosure
		OS
		Ports
		TLS encryption
		SSL Certificate
		TLS Implementation
		TLS version

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD release 5.8

Kenmerk: Nnb

Datum	12-09-2018
Status	Definitief
Versie	1.0

Na oplossen is deze rubricering beëindigd.

Rubricering	derubricering
Vaststeller	10.2e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**Nnb**
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	**Versie**	**Auteur**	**Opmerkingen**
16-08-2018	0.1	Sogeti	Initiële versie
20-08-2018	0.2	Sogeti	Hertest verwerkt
21-08-2018	0.3	Sogeti	Interne review
23-08-2018	0.4	Sogeti	Opmerkingen verwerkt
10-09-2018	0.5	Sogeti	Opmerkingen verwerkt
12-09-2018	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	**Rol**	**Functie**	**Bedrijf**
10.2e			

Inhoud

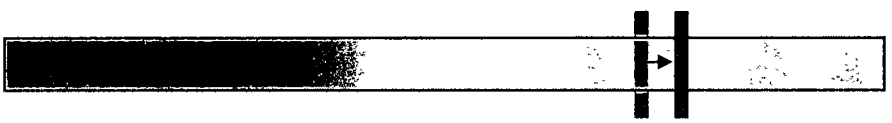
Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest betreft de aanstaande release 5.8 van DigiD. De test is bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook worden er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.8, zoals getest op de A3-omgeving voldoende is. Er zijn nieuwe bevindingen gedaan, maar deze zijn tijdens de test opgelost of als geaccepteerd opgenomen. Wel zijn er verschillende bevindingen onopgelost gebleven sinds de vorige test.



Onvoldoende Voldoende

Punten ter verbetering (terugkerende bevindingen)

- De bevinding uit de voorgaande test die als 'opgelost' aangemerkt was is slechts voor een deel van de domeinen in de scope opgelost. Bevinding 5.4.2 (laag).
  Aanbeveling: los de bevinding ook voor de resterende domeinen op.
- Een aantal headers die de gebruiker beschermen tijdens het gebruiken van de applicatie worden door de server niet standaard meegestuurd. Bevinding 5.7.3 (laag), Bevinding 5.7.4 (laag).
  Aanbeveling: Stuur deze headers mee vanuit de server om de gebruiker beter te beschermen tijdens het gebruik van de applicatie.
- De mogelijkheid bestaat dat een aanvaller bepaalde waardes in meegestuurde headers kan veranderen, zodat er cookies voor het verkeerde domein worden aangeleverd door de server. Bevinding 5.7.6 (laag).
  Aanbeveling: Zorg ervoor dat de invoer van een gebruiker nooit zonder controle gereflecteerd wordt als de server de invoer terugstuurt.

Aanvullingen Logius

Logius heeft kennisgenomen van de resultaten van de Securitytest R5.8. De gerapporteerde bevindingen zijn beoordeeld op impact. Ten aanzien van 2 bevindingen is tijdens de testperiode een oplossing doorgevoerd. Opvolging en verdere analyse van deze bevindingen en aanbevelingen vindt plaats vanuit het reguliere beheerproces. Het Security Testrapport en de ingeschatte impact van de bevindingen zal onderdeel uitmaken van het advies dat aan de stuurgroep DigiD zal worden gegeven ten aanzien van de vrijgave van DigiD R5.8.

Sogeti heeft ook op eerdere releases een securitytest uitgevoerd en bevindingen gedaan. Reactie van Logius ten aanzien van nog openstaande bevindingen uit deze voorgaande rapportages:

ID	Bevinding	Risico inschatting	Status Logius	Oplossen?
5.4.3	Gelijktijdige sessies	Midden	Is op dit moment gewenste functionaliteit. DigiD architect geeft aan dat dienstaanbieders (waaronder MijnDigiD) eigenlijk toestaan dat er meerdere gelijktijdige sessies aanwezig zijn. DigiD kern kan niet de (lokale) sessie beëindigen. Hij gaat nog na hoe banken hier mee omgaan. Mogelijk aanpassen in een volgende release.	Impact nog onvoldoende bekend.
5.5.1	Content-Security-Policy header Implementatiefout	Zeer Laag	Beleid omtrent CSP en de wijze van toepassen dient nog vastgesteld te worden.	Gepland voor R5.8.
5.5.3	Wachtwoordsterkte onvoldoende	Zeer Laag	In de context van DigiD-gebruik is het ophogen van een minimumaantal karakters voor een wachtwoord van 8 naar 12 karakters niet wenselijk. Naar het nu bestaande maximum van 32 karakters wordt nog een keer gekeken.	Nee.
5.5.4	Open poorten	Zeer Laag	In de context van DigiD is het dichtzetten van poort 80 op dit moment geen optie. Voor de domeinnaam digid.nl staat naast poort 443 ook poort 80 open. Voor een publieke dienst als DigiD is het noodzakelijk om voor een zo groot mogelijke groep burgers toegankelijk te zijn. Om die reden is het een "by design" keuze om poort 80 (http) open te houden, om gebruikers automatisch door te kunnen sturen naar poort 443 (https).	Nee.

			Wanneer de loadbalancer in tier 1 van de betreffende omgeving een http request ontvangt, wordt dit automatisch redirected naar https, dit voorkomt dat een burger een "page not found" krijgt wanneer hij DigiD via http benadert.	
5.5.5	BEAST (Browser Exploit Against SSL/TLS)	Laag	Deze Cipher Block Chaining (CBC) suites worden ondersteund door DigiD. Die kunnen op dit moment nog niet uitgezet worden omdat daarmee (te) veel burgers uitgesloten worden. Het is een browser attack en in moderne browsers zit daarvoor een beveiligingsmechanisme ingebouwd.	Voorlopig niet, tenzij de betreffende ciphers als onbetrouwbaar worden geclassificeerd.
5.6.1	Cookie-domein te breed	Laag	De beveiligingsspecialist geeft aan dat de cookie-policy nog besproken wordt. Oplossing heeft veel impact op het huidige design. Oplossen is pas zinvol als er een beslissing is genomen over de cookie-policy.	Impact nog onvoldoende bekend.
5.6.2	Onvoldoende invoervalidatie Daring Fireball markup	Laag	Dit risico beperkt zich tot de beheermodule en de beheerdersrollen. Mogelijk oplossen in een volgende release.	Ja, nog niet ingepland.
5.6.3	SSL/TLS downgrade	Zeer Laag	De aard van deze bevinding en de mogelijkheid van misbruik is nog niet geheel duidelijk en zal nog nader onderzocht worden.	Impact nog onvoldoende bekend.
5.6.8	Directe gebruikersnaam enumeratie	Zeer Laag	Indien een aanvaller een sessie kan overnemen of toegang zou krijgen tot de loggegevens dan kan deze meer zien dan alleen de gebruikersnaam. Ook zaken als BSN en telefoon nummer (06) zijn dan zichtbaar. Dit is inherent aan de zaken die we loggen.	Nee.
5.7.3	Anti-Cross-Site-Scripting-header ontbreekt	laag		
5.7.4	X-Content-Type-Options header ontbreekt	laag		
5.7.6	Reflectie in header	laag		

1 Inleiding

1.1 Opdrachtformulering

DigiD Release 5.8 is een release waarin veel kleine aanpassingen en uitbreidingen zijn gedaan. De scope van deze securitytest was de gehele DigiD-applicatie, waarbij de nadruk lag op de risico's door de wijzigingen en/of uitbreidingen die in release 5.8 worden doorgevoerd.

In brede zin wordt in R5.8 gerealiseerd:

- Nieuwe switch voor app functionaliteit
- Digid app activering vanaf 1 device
- Twee usability test-bevindingen en enkele kleine tekstuele aanpassingen ihkv DigiD Hoog
- App als zelfstandig middel
- Restpunten
- Verhogen naar substantieel bij zuil
- Refactor interne API tussen DigiD balie en kern
- Regressiebevindingen uit 5.7 en eerder
- Inlezen EAC AT certificaat RDW in HSM

In scope waren:

- Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
- Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
- Het verkeer tussen systemen buiten Kern (RDA server, Status Controller, eID server) en DigiD kern voor zover zichtbaar.

Tijdens eerdere tests op DigiD is een aantal bevindingen gedaan welke in release 5.8 zijn opgelost en daarom specifiek opnieuw moest worden getest of waarvan bekend is dat het risico is geaccepteerd. Deze bevindingen zijn:

Opgeloste bevindingen

5.3.17 Denial of Service – Email versturen
5.4.2 Content-Security-Policy (CSP) header ontbreekt

IB bevindingen die bekend zijn en niet opgelost

5.7.3 Anti-Cross-Site-Scripting-header ontbreekt
5.7.4 X-Content-Type-Options header ontbreekt
5.7.6 Reflectie in header
5.6.3 SSL/TLS downgrade

Daarnaast zijn er bevindingen waarvan de aanwezig bekend is maar het risico geaccepteerd is tijdens eerdere tests. Deze bevindingen zijn daarom in deze rapportage niet nogmaals opgenomen.

IB bevindingen die geaccepteerd zijn

5.4.3 Gelijktijdige sessies
5.5.3 Wachtwoordsterkte onvoldoende
5.5.4 Open poorten
5.5.5 BEAST (Browser Exploit Against SSL/TLS)
5.5.1 Content-Security-Policy header implementatiefout
5.6.1 Cookie-domein te breed
5.6.2 Onvoldoende invoervalidatie Daring Fireball markup

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. De securitytest bestond uit een vulnerability assessment met een diepgang greybox (hierbij krijgen de testers beschikking over documentatie en gebruikersrechten op het systeem, zodat het systeem met enige diepgang kan worden onderzocht) en betrof een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A3-omgeving.

2 Resultaten

2.1 Cumulatief overzicht

Hieronder staat een totaaloverzicht van de bevindingen in dit rapport. Zie paragraaf 5.1 voor een toelichting op de risicoclassificatie.

In de tabel hieronder zijn zowel nieuwe bevindingen opgenomen als terugkerende bevindingen die nog niet opgelost zijn.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Opgelost	Totaal
Client-side controls					2		**2**
Functie specifieke invoer						1	**1**
Servers			1	2	1		**4**
Totaal			**2**	**2**	**3**	**1**	**7**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Oordeel	
Buiten scope voor deze test.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope voor deze test.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Buiten scope voor deze test.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Buiten scope voor deze test.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Bevinding 5.7.6, 5.7.17	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Bevindingen 5.7.3, 5.7.4 en 5.7.5	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Bevinding 5.6.3	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Geen bevindingen.	
U/WA.07	**Webapplicatie-integratie**

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Geen bevindingen.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Buiten scope voor deze test.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Geen bevindingen.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Geen bevindingen.	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	
Geen bevindingen.	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Buiten scope voor deze test.	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Buiten scope voor deze test.	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Geen bevindingen.	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting	
U/NW.02	**Beschikbaarheid van netwerken**

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Buiten scope voor deze test.	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Buiten scope voor deze test.	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Buiten scope voor deze test.	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Buiten scope voor deze test.	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Geen bevindingen.	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Geen bevindingen.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Buiten scope voor deze test.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Buiten scope voor deze test.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Buiten scope voor deze test.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Buiten scope voor deze test.	
C.04	**Penetratietestproces**

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Deze test is onderdeel van het voldoen aan deze richtlijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Buiten scope voor deze test.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Buiten scope voor deze test.	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Buiten scope voor deze test.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Buiten scope voor deze test.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Buiten scope voor deze test.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope voor deze test.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Geen bevindingen.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Content-Security-Policy (CSP) header ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	5.4.2	Zeer laag	Zeer Laag	Laag

Hosts
balie-a3.digid.nl
was-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl
digidbeheer-a3.digid.nl
eid-a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP-header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"

Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en 'inline-scripts' niet worden uitgevoerd:
Content-Security-Policy: default-src self

Details
Tijdens de voorgaande test is vastgesteld dat voor een aantal domeinen de CSP-header niet meegestuurd werd door de server. Deze bevinding is opnieuw onderzocht. De bevinding is deels opgelost.
Voor de volgende domeinen wordt de CSP-header nu wel meegestuurd.

- balie-a3.digid.nl
- cis-a3

```
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
```

Voor de volgende domeinen wordt de CSP-header nog steeds niet meegestuurd.
https://digidbeheer-a3.digid.nl::

```
HTTP/1.0 302 Found
Location: http://www.al.digid.nl
Connection: close
Content-Length: 0
```

https://eid-a3.digid.nl::

```
HTTP/1.1 403 Forbidden
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Date: Mon, 13 Aug 2018 08:28:37 GMT
Connection: close
X-Content-Type-Options: nosniff
Content-Type: text/html
Content-Language: en-US
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

https://rda-a3.digid.nl::

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488876285000"
Last-Modified: Tue, 07 Mar 2017 08:44:45 GMT
Content-Type: text/html
Content-Length: 13
Date: Mon, 13 Aug 2018 08:27:31 GMT
Connection: close
Set-Cookie: _persist=---cookie_verwijderd---;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

https://was-a3-digid.nl::

```
HTTP/1.1 404 Not Found
Date: Mon, 13 Aug 2018 08:25:37 GMT
X-Request-Id: 4bf82ec8-af4b-4ad9-b352-1cfb13e07b3a
X-Runtime: 0.002322
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Set-Cookie: _persist=---cookie_verwijderd---;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.1.2 *Content-Security-Policy header implementatiefout*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	5.8.1	Zeer laag	Zeer Laag	Laag

Hosts
mijn.a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven. De policy welke door de server verstuurd wordt is niet correct/veilig.

Bedreiging
Wanneer de CSP-header niet correct is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwen code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-policy zo strak mogelijk, waarbij onveilig gedrag niet toegelaten wordt. Bouw vanuit hier de policy uit met alleen die functionaliteit welke nodig is. Gebruik hierbij voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Details
Sommige domeinen maken gebruik van onveilige instellingen voor de CSP-header. Deze instellingen staan het gebruik van inline-scripts en -opmaak toe. Daarnaast wordt het gebruik van de JavaScript-functie *eval* toegestaan. Deze instellingen maken het voor een aanvaller gemakkelijker een eventuele cross-site-scripting-kwetsbaarheid in de applicatie uit te buiten.
Voor de volgende domeinen wordt een onveilige CSP-header meegestuurd.

- balie-a3.digid.nl
- cis-a3

```
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Een overzicht van deze bevindingen.

3.6.1 Denial of Service – Email versturen

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3	5.3.17	Opgelost	Laag	Midden

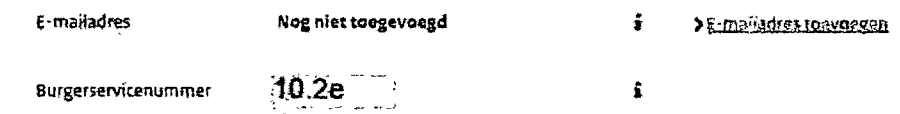
Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Het systeem is zo te manipuleren dat de server een grote hoeveelheid emails naar een gebruiker stuurt.

Bedreiging
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling
Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een email is gestuurd naar de gebruiker.

Details
Het is mogelijk om via de DigiD applicatie een continue stroom e-mails te versturen naar een willekeurig e-mailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.



Wanneer er een e-mailadres wordt opgegeven en op de volgende knop wordt knop wordt gedrukt wordt onderstaande request verzonden:

```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Referer: https://mijn.a3.digid.nl/email/nieuw
Content-Type: application/x-www-form-urlencoded
Content-Length: 197
Cookie: _session_id=1b8163296735cb883728de1c2ebeef40;
_persist='UI1EYj4+Tj2Ypb1OB73J21z0JkeAkkKZUzYzMF/rUJMgbHC+WB8zJYVODQDG
yKg6fdcqdCLpEzbp/x32OHW0n9imZLlu9UC+sIk2nEI=
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=N9Fvp3HFEejF%2B7J78FVGeiw5Sv8M4tEMGX
GxsJ3hJnPlzOAguRpwNcOWRA5YE16VD%2BZd4XQdDDPYyqrX1iD02w%3D%3D&email%5Ba
ddress%5D=1029                                    &commit=Volgende
```

De response zorgt ervoor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatiecode naar het e-mailadres. Deze code moet binnen een bepaalde periode worden opgegeven, anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wil versturen verschijnt de melding dat er al een code onderweg is en na meer dan 5 minuten een nieuwe code kan worden aangevraagd.

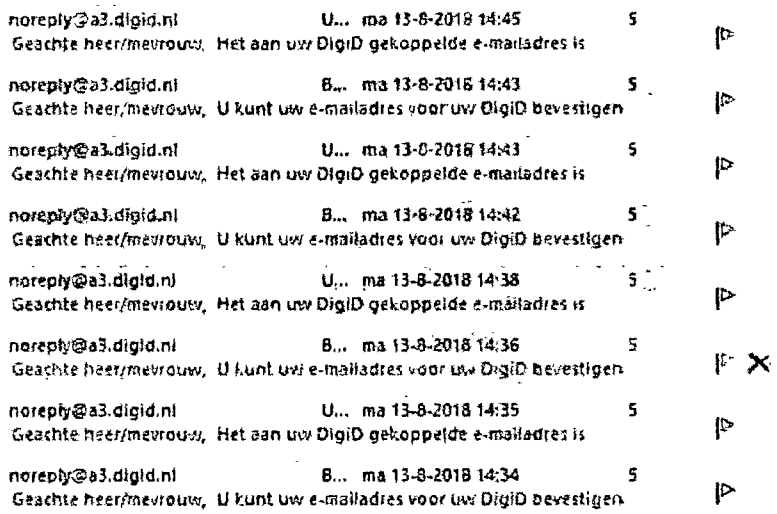
"Er is nog een e-mail onderweg naar u. Vanaf xx:xx uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen."

Echter is het mogelijk om het nog niet geactiveerde e-mailadres te verwijderen van het account.

Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg is dat de gebruiker bovenstaande actie nog een keer kan uitvoeren voor hetzelfde of andere e-mailadressen.
Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.

https://mijn.a3.digid.nl	POST	/email	✓	302	851	HTML
https://mijn.a3.digid.nl	GET	/email/nieuw		200	7027	HTML
https://mijn.a3.digid.nl	GET	/		200	14449	HTML
https://mijn.a3.digid.nl	POST	/email	✓	302	818	HTML
https://mijn.a3.digid.nl	GET	/email/verwijderen		200	7437	HTML
https://mijn.a3.digid.nl	GET	/		200	15135	HTML
https://mijn.a3.digid.nl	GET	/email/bevestiging		302	798	HTML
https://mijn.a3.digid.nl	POST	/check_wachtwoord	✓	302	853	HTML
https://mijn.a3.digid.nl	GET	/check_wachtwoord		200	7321	HTML
https://mijn.a3.digid.nl	POST	/email	✓	302	851	HTML
https://mijn.a3.digid.nl	GET	/email/nieuw		200	7027	HTML
https://mijn.a3.digid.nl	GET	/		200	14450	HTML
https://mijn.a3.digid.nl	POST	/email	✓	302	818	HTML
https://mijn.a3.digid.nl	GET	/email/verwijderen		200	7437	HTML
https://mijn.a3.digid.nl	GET	/		200	15132	HTML
https://mijn.a3.digid.nl	GET	/email/bevestiging		302	798	HTML
https://mijn.a3.digid.nl	POST	/check_wachtwoord	✓	302	853	HTML
https://mijn.a3.digid.nl	GET	/assets/error-e574be469de777d		200	634	XML
https://mijn.a3.digid.nl	POST	/check_wachtwoord	✓	200	7467	HTML
https://mijn.a3.digid.nl	GET	/check_wachtwoord		200	7321	HTML
https://mijn.a3.digid.nl	POST	/email	✓	302	851	HTML
https://mijn.a3.digid.nl	GET	/email/nieuw		200	7027	HTML

Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:



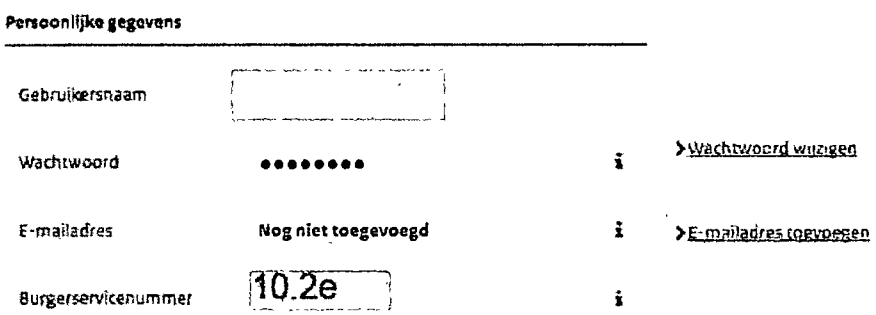
Er bestaat een risico als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail. De mail kan dan worden aangemerkt als spam of phishing waarmee het verzendadres op een spamblacklist kan komen te staan. Mailservers die daarvan gebruikmaken zullen dan geen mails meer accepteren van dit adres.

In versie 5.8 van DigID is daarom een limiet toegevoegd aan het aantal emails dat per account per dag kan worden verzonden.

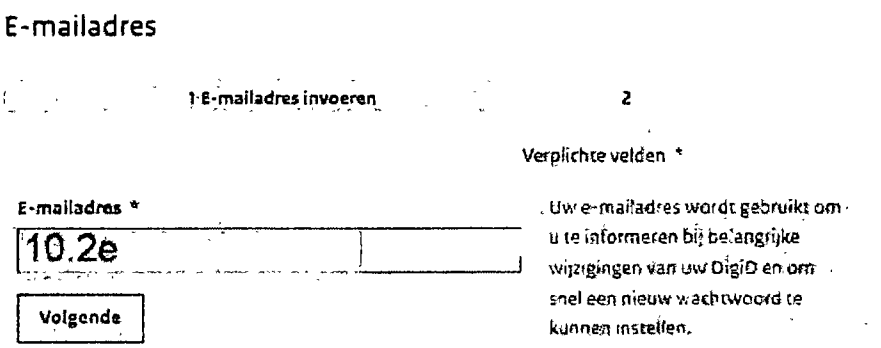
> Er zijn vandaag al 5 e-mails naar u verstuurd met een code om uw nieuwe e-mailadres te bevestigen. Morgen (15 augustus 2018) kunt u uw e-mailadres weer wijzigen of toevoegen.

Ok

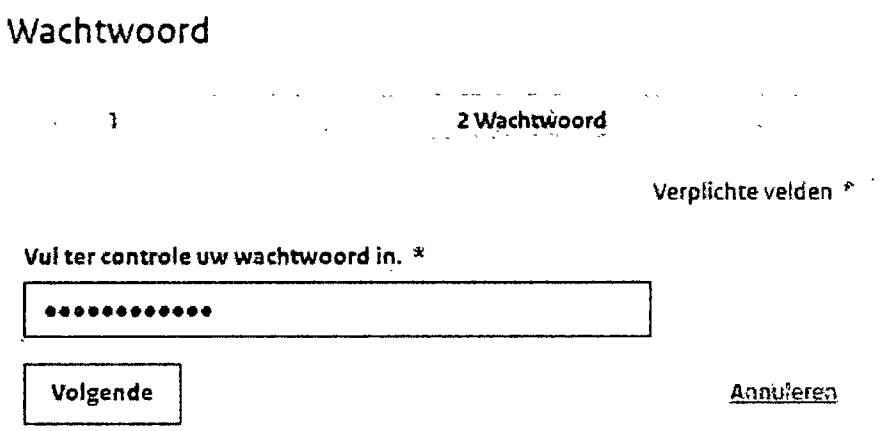
Het is echter mogelijk om dit limiet te omzeilen door een fout in het toevoegen van een emailadres proces. Dit proces wordt gestart vanaf de mijn pagina door de link E-mailadres toevoegen:



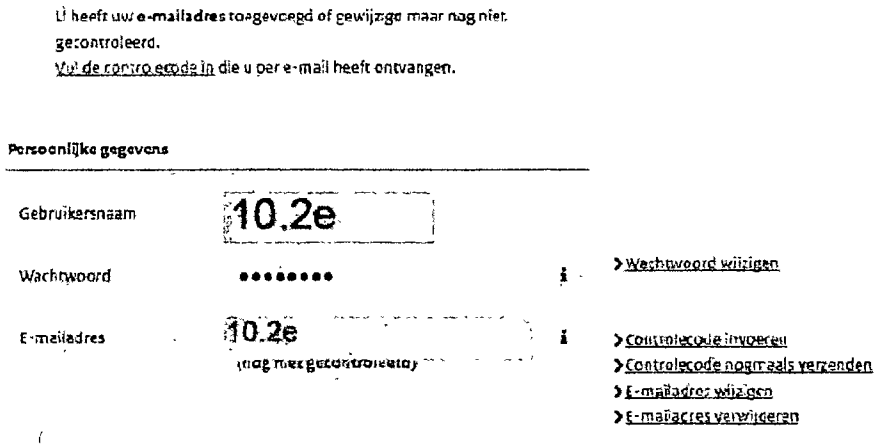
Het proces heeft 2 stappen; 1. E-mailadres invoeren, zoals in het scherm hieronder is te zien:



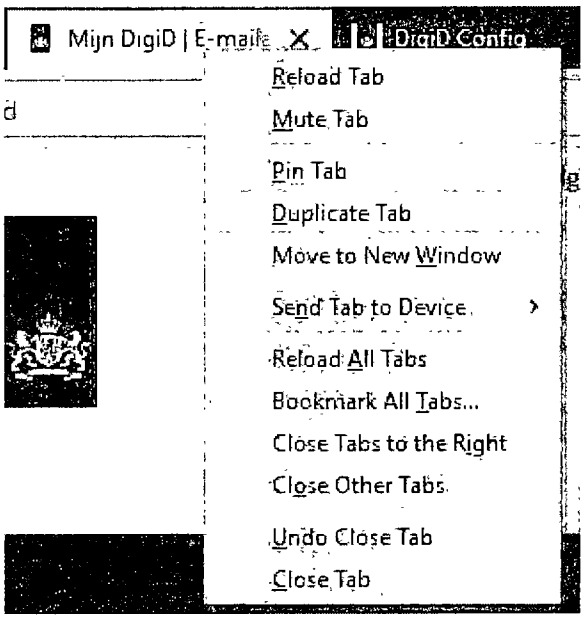
Na het opgeven van het gewenste e-mailadres volgt stap 2, waarin ter controle het wachtwoord van de ingelogde burger nogmaals wordt gevraagd:



Als op volgende wordt geklikt wordt het algemene mijn DigiD-scherm weer getoond met de melding dat het e-mailadres is toegevoegd maar nog niet is gecontroleerd.



Wanneer een aanvaller tijdens de 2e stap het wachtwoord scherm dupliceert, of het HTTP-request opslaat, kan hij deze stap later nogmaals uitvoeren.



Het probleem is dat deze stap niet aan de limiet is gekoppeld. De limiet wordt alleen bij het instantiëren van het proces gecontroleerd.

Dit is te zien als het emailadres weer wordt verwijderd:

E-mailadres verwijderen

Vul ter controle uw wachtwoord in.

Let op! U ontvangt hierna geen e-mails meer ter controle van belangrijke wijzigingen van uw DigiD. Tevens kunt u er niet meer voor kiezen om, indien u uw wachtwoord bent vergeten, een nieuw wachtwoord in te stellen via e-mail en sms.

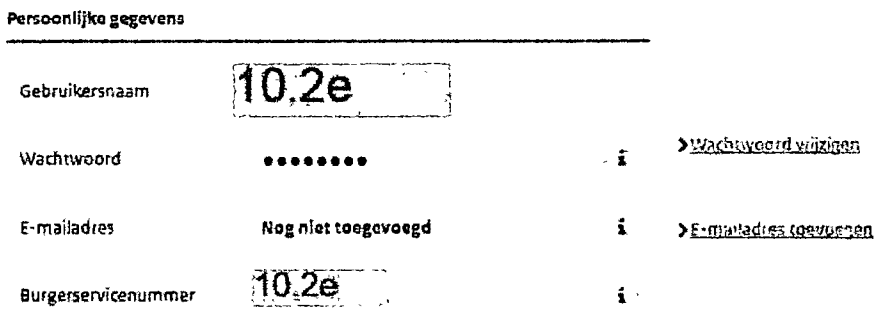
Verplichte velden *

Wachtwoord *

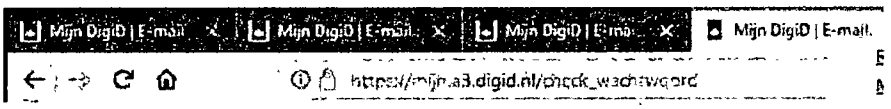
••••••••••••

Verwijderen Annuleren

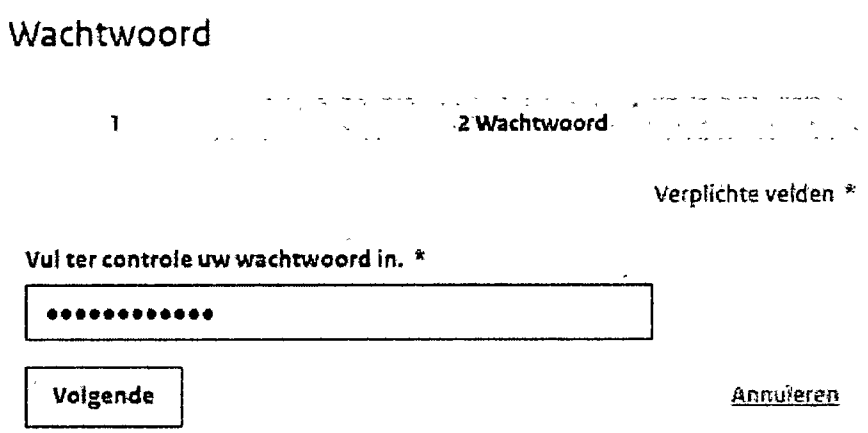
Hierdoor ziet het mijn DigiD scherm er weer uit als initieel:



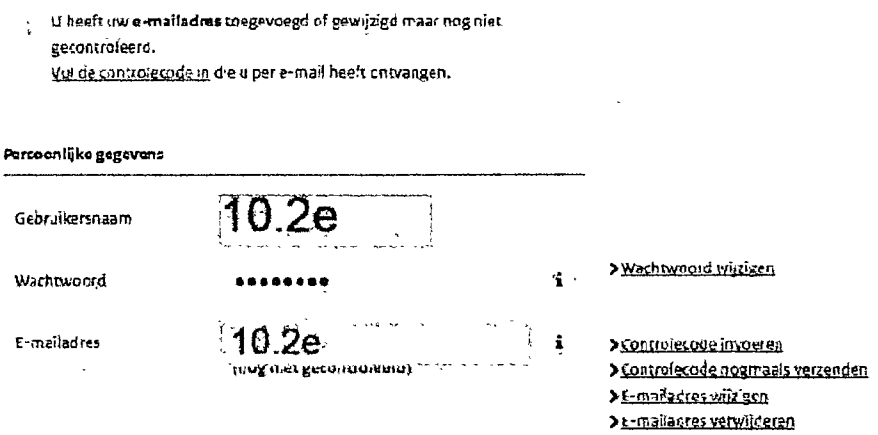
Als de aanvaller dan naar een van zijn opgeslagen tabs gaat:



En wederom op de volgende knop drukt:



Dan wordt de email wederom verzonden en staat het e-mailadres weer als niet gecontroleerd.



De aanvaller zou de bestaande kopie van het wachtwoordscherm wederom kunnen kopiëren en die opsturen. Wanneer deze actie

herhaaldelijk wordt afgetrapt is het mogelijk om meer e-mails te sturen dan de limiet toelaat:


noreply@a3.digid.nl E di 14-8-2018 12:07 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 12:06 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 12:04 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 12:04 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl L di 14-8-2018 12:02 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 12:02 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl E di 14-8-2018 12:01 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 12:01 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 11:58 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:58 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 11:57 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:57 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 11:56 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:54 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 11:54 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl E di 14-8-2018 11:54 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:54 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

noreply@a3.digid.nl E di 14-8-2018 11:54 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:53 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

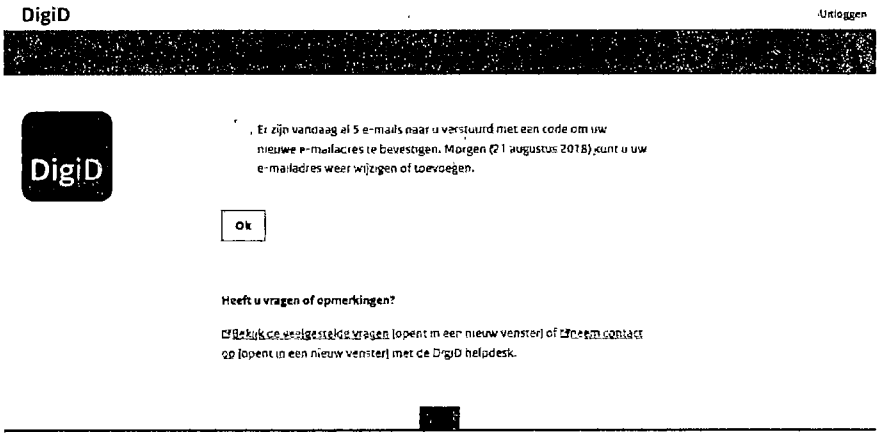
noreply@a3.digid.nl E di 14-8-2018 11:53 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

noreply@a3.digid.nl L di 14-8-2018 11:53 5
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is

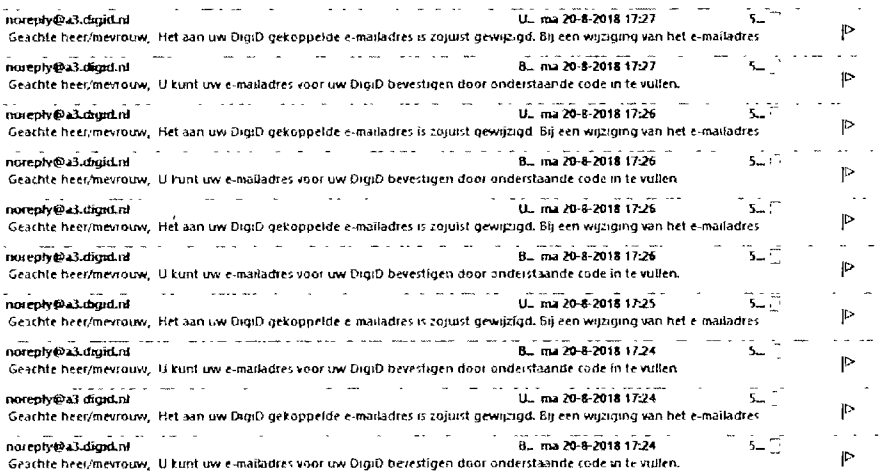
noreply@a3.digid.nl E di 14-8-2018 11:53 5
Geachte heer/mevrouw, U kunt uw e-mailadres voor uw DigiD bevestigen

Hertest 20-06-2018

Het is niet meer mogelijk om op de hiervoor genoemde manier herhaaldelijk e-mails te blijven sturen. De applicatie toont na het versturen van de tweede stap en na eerdere mails nu onderstaande melding.



Los van de melding komen er ook geen additionele mails meer binnen.



3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 *SSL/TLS downgrade*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4	5.6.3	Zeer laag	Zeer Laag	Zeer Laag

Betreffende hosts
mijn.a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl
a3.digid.nl
eid-a3.digid.nl

Omschrijving
De applicatie maakt gebruik van een SSL/TLS tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.
openssl s_client -connect host:443 -state -fallback_scsv -tls1_1

Bedreiging
Als een aanvaller kan optreden als 'man in the middle' kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 12).
Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details
Voorbeeld voor was-a3.digid.nl:

```
root@kali:~# sslscan was-a3.digid.nl
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server was-a3.digid.nl on port 443 using SNI name was-
a3.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported
```

```
  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256
DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256
DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  a3.digid.nl
Altnames: DNS:a3.digid.nl, DNS:was-a3.digid.nl, DNS:mijn.a3.digid.nl,
DNS:balie-a3.digid.nl, DNS:digidbeheer-a3.digid.nl, DNS:config-
a3.digid.nl, DNS:www.a3.digid.nl, DNS:stubs-a3.digid.nl, DNS:app-
a3.digid.nl, DNS:cis-a3.digid.nl, DNS:cts-a3.digid.nl
Issuer:   KPN PKIoverheid Organisatie CA - G2

Not valid before: Apr  7 11:03:44 2017 GMT
Not valid after:  Apr  7 11:03:44 2019 GMT
```

3.9.2 *Reflectie in header*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5	5.7.6	Laag	Laag	Laag

Betreffende hosts
a3.digid.nl
mijn.a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl
eid-a3.digid.nl

Omschrijving

Gegevens die door de server worden gestuurd naar de gebruiker bevatten veelal instructies voor browsers in de vorm van headers, naast natuurlijk de uiteindelijke content van de pagina. Meestal kunnen de meegestuurde headers niet worden beïnvloed of aangepast door de gebruiker. In dit geval is dit wel mogelijk.

Bedreiging
Door het wijzigen van bepaalde invoer die naar de server wordt gestuurd, kan een aanvaller bijvoorbeeld de inhoud van een teruggestuurde header controleren. De invoer wordt direct gereflecteerd naar de gebruiker in de uitvoer.

Aanbeveling
Filter alle mogelijke invoer van de gebruiker en zorg dat er geen headerwaardes direct gewijzigd kunnen worden door invoer in een web request te veranderen.

Details
De waarde van het cookie *_persist* in headers van de a3.digid.nl site is te beïnvloeden door in de request de Host header aan te passen.

Normaal request:

```
GET / HTTP/1.1
Host: a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv.52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie. _session_id=b640d1fb07302d6f8d7fae7ccce63c40;
_persist='ncdoBr3rpOe8ui9OB73J21z0JkeAkrUG9kBX+XWc6lRNIU7E4nSUukFJFTps
ngQ+no5QpLTE1T2jRMApCHxrXUTxvp3WxLIbey9M+Uw=
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Thu, 16 Aug 2018 11:15:55 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: blec8605-4011-4429-ad60-0d28c2ee6f3c
X-Runtime: 0.015872
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=b9d0a8d6d9337d3def493dc8843cb87e;Secure;
domain=.digid.nl; path=/; HttpOnly
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie:
_persist='Hokys0QOapKlo0VOB73J21z0JkeAksVo+eceHEdNlQV5M9om9E4FUvuVHvMO
+CL0Wkk4UYKHy6UCT188HKOPul2sTEPjsUD2IT66LpA=;domain=.digwid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Als de host in de request wordt aangepast:

```
GET / HTTP/1.1
Host: sogeti.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Thu, 16 Aug 2018 11:16:24 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 22ac2ebe-a7a0-422f-ad20-74df5021a06e
X-Runtime: 0.012355
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=a36d9324fdaf97cfb4a0138ddecd6d4f;Secure;
domain=.digid.nl; path=/; HttpOnly
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie:
_persist='la5TnSpubk3EMtdOB73J21z0JkeAkgD7ILESVq0FsAV1MXdPrkBR09rHRt17
Yb5V2B+ca2q6oPn+M0TrK0Fq/TjcHz2LDdZSWARZYPM=;domain=.sogeti.com;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Het cookie is nu geldig voor het domein sogeti.com. Het invoeren van bepaalde andere tekens zorgt voor een 400 Bad Request. Er kan niet uit de header regel worden gebroken, dus het toevoegen van extra headers is niet mogelijk.

Request met toevoegen Secure;

```
GET / HTTP/1.1
Host: sogeti.com; Secure
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64, x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Thu, 16 Aug 2018 11:16:58 GMT
Content-Length: 347
Connection: close
Content-Type: text/html; charset=iso-8859-1
Set-Cookie:
_persist='jfIlxAp7+eUVh4ROB73J21z0JkeAklM6qqsGJbdGvuansNxRWj41oGQirpST
iswLJ68OvhwgSdNoHXycJX72s47CZqXmocs/S5bQMEU=;domain=.sogeti.com;
Secure; HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
```

```
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not
understand.<br />
</p>
<p>Additionally, a 400 Bad Request
error was encountered while trying to use an ErrorDocument to handle
the request.</p>
</body></html>
```

3.9.3 *X-Content-Type-Options header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6	5.7.4	Laag	Laag	Laag

Betreffende hosts
was-a3.digid.nl
rda-a3.digid.nl

Omschrijving
De anti-MIME-sniffing header X-Content-Type-opties is niet ingesteld op nosniff.

Bedreiging
Door het ontbreken van deze header wordt in oudere versies van Internet Explorer en Chrome MIME-sniffing toegepast op de response-body. Dit kan de response-body in een ander formaat weergeven dan het opgegeven content-type. Huidige (sinds begin 2014) versies van Firefox maken altijd gebruik van het opgegeven content-type (als er een is ingesteld).

Aanbeveling
Zorg ervoor dat de webserver de Content-Type header goed meestuurt, en dat de header X-Content-Type-Options is ingesteld op nosniff voor alle webpagina's.

Details
Het volgende voorbeeld is voor rda-a3.digid.nl.
In de header van het request mist de *X-Content-Type-Options*.

Request:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Host: rda-a3.digid.nl
Connection: Keep-Alive
```

Response:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488876285000"
Last-Modified: Tue, 07 Mar 2017 08:44:45 GMT
Content-Type: text/html
Content-Length: 13
```

```
Date: Thu, 16 Aug 2018 11:18:56 GMT
Connection: keep-alive
Set-Cookie:
_persist=!4T4KA2sC0xvMBhNOB73J21z0JkeAkrOzk5l0hBrYD2GKI73joSC6vrufMD93
F4vBhAcEuBhmsWUpdAMY6BL80iscmhn4yoQG9zKD9qE=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

3.9.4 *Anti-Cross-Site-Scripting-header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7	5.7.3	Midden	Laag	Hoog

Betreffende hosts
was-a3.digid.nl
rda-a3.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden standaard bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Gebruikers kunnen de bescherming handmatig uitschakelen, waardoor het voor aanvallers makkelijker wordt om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
'X-XSS-Protection: 1'
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging:
X-XSS-Protection: 1; mode=block
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie:
https://blogs.msdn.microsoft.com/ieinternals/2011/01/31/controlling-the-xss-filter/

Details
Het volgende voorbeeld is voor rda-a3.digid.nl.
In de header van het request mist de anti-cross-site-scripting header.

Request:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
```

```
Host: rda-a3.digid.nl
Connection: Keep-Alive
```

Response:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488876285000"
Last-Modified: Tue, 07 Mar 2017 08:44:45 GMT
Content-Type: text/html
Content-Length: 13
Date: Thu, 16 Aug 2018 11:21:33 GMT
Connection: keep-alive
Set-Cookie:
_persist='ttsMInaXRr4pDdlOB73J21z0JkeAktrj2vQmK81Ngq03dCL0SSfdKwHc8ZtN
Gty78xpoQibvo8myXFcc8AcH4JgUAIsii4HxVgqL+Gk=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

4 PAP-eisen

Hieronder wordt van de eisen uit het document aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

ID	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Geen bevindingen		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
5.7.4 Reflectie in header, 5.4.2 CSP-header ontbreekt		
ACC2.2.3	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Geen bevindingen		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en tolerantles Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.	DNSSEC
Geen bevindingen		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der	Ingetrokken certificaten

Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is
Geen bevindingen

5 Bijlagen

5.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

5.1 Aanpak

Tijdens de test wordt een groot aantal controles uitgevoerd. Hierbij wordt onder andere gebruikgemaakt van een checklist op basis van de *Web Application Hacker's Handbook* met de volgende onderdelen:

Logic	Client-side checks	Hidden fields
		Cookies - HTTP / Secure flag etc.
		Local privacy vulnerabilities
		Autocomplete forms
		Preset parameters
		ASP.net ViewState
		Field length limit
		Javascript Validation
		ClickJacking
		Disabled elements
		Java applets
		ActiveX
		Shockwave Flash
		Executables
	Logic Errors	Multistage
		Incomplete input
		Transaction logic
Authentication	Direct attacks	Password quality rules
		Username enumeration

		Password guessing
	Speciale functies	Account recovery
		Remember me functions
		Impersonation / Account hijacking
	Managing credentials	Username uniqueness
		Credential predictability
		Unsafe transmission
		Unsafe distribution
	Logic Errors	Autentication errors
		Fail-open conditions
		Multistage
Session management	Generation	Token logic/meaning
		Token predictability
	Handling	Insecure transmission of tokens
		Token disclosure in logs
		Mapping of tokens to sessions
		Concurrent sessions
		Session termination
		Fixation
		CSRF
		Caching
		Persistent cookies
		Fixed session ID
		Cookie Scope
Access	Segregation	Different accounts
		Insecure access control method
		Horizontal Privilige escalation
		Vertical Privilige escalation
	Controle	Anonymous
Input handling	Fuzzing	SQL injection
		Reflected XSS
		Stored XSS
		OS Command injection
		Path traversal
		Script Injection
		File upload fields
		File Inclusion
	Functie specifiek	SMTP injection
		Code flaws
		DOM-based attacks
		Frame injection
		HTTP Header Injection
		Arbitrary Redirection

		SOAP injection
		LDAP injection
		XPATH injection
Environment	Interfaces	Segregation in shared infrastructures
		Segregation between ASP-hosted apps
Server	Implementation	Default credentials
		Default content
		HTTP method
		Proxy
		Virtual hosting
	Software	Native software flaws
		Known vulnerabilities
	Configuration	Known bugs
		Services
		Disclosure
		OS
		Ports
		TLS encryption
		SSL Certificate
		TLS Implementation
		TLS version

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD Release 5.9

Kenmerk: Nnb

Datum	30-11-2018
Status	Definitief
Versie	1.0

Na 30-11-2019 is deze rubricering beëindigd.

Rubricering	derubricering
Vaststeller	10.2e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**Nnb**
Versienummer	1.0
Contactpersoon	[redacted]
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	**Versie**	**Auteur**	**Opmerkingen**
20-11-2018	0.1	Sogeti	Initiële versie
21-11-2018	0.2	Sogeti	Interne review
30-11-2018	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	**Rol**	**Functie**	**Bedrijf**
[redacted]			

Inhoud

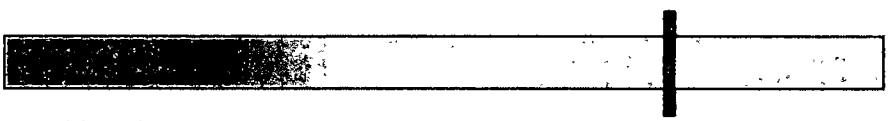
Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest was de aanstaande release 5.9 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is gedurende de test extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook zijn er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.9, zoals getest op de A4-omgeving voldoende is. Er zijn enkele nieuwe bevindingen gedaan met een midden, laag en zeer laag risico. Daarnaast zijn er verschillende bevindingen onopgelost gebleven sinds de vorige test.



Onvoldoende Voldoende

Punten ter verbetering (nieuw):

- De applicatie toont wachtwoorden in de beheerinterface. Dit zorgt ervoor dat iemand die op het scherm meekijkt die wachtwoorden in handen kan krijgen. Zie bevinding 4.

  Aanbeveling: Toon bij voorkeur nooit wachtwoorden in een applicatie. Indien het echt noodzakelijk is voor de gebruiker om wachtwoorden in te zien, toon ze dan eerst gemaskeerd. Maak het wachtwoord pas zichtbaar als een gebruiker daar expliciet opdracht toe geeft.

- Het is mogelijk om een gebruiker uit te loggen, bijvoorbeeld als die gebruiker een kwaadaardige website open heeft staan. Hierdoor is het mogelijk, zolang die kwaadaardige pagina open staat, DigiD onbruikbaar te maken voor de gebruiker. Zie bevinding 3.

  Aanbeveling: Verifieer altijd voor alle acties die worden uitgevoerd of ze van de eigen site afkomstig zijn, door een unieke token mee te sturen.

Punten ter verbetering terugkerende bevindingen (overgenomen uit het vorige rapport):

- De bevinding uit de voorgaande test die als 'opgelost' aangemerkt was is slechts voor een deel van de domeinen in de scope opgelost. Bevinding 5.4.2 (laag).

  Aanbeveling: los de bevinding ook voor de resterende domeinen op.

- Een aantal headers die de gebruiker beschermen tijdens het gebruiken van de applicatie worden door de server niet standaard meegestuurd. Bevinding 5.7.3 (laag), Bevinding 5.7.4 (laag).

  Aanbeveling: Stuur deze headers mee vanuit de server om de gebruiker beter te beschermen tijdens het gebruik van de applicatie.

- De mogelijkheid bestaat dat een aanvaller bepaalde waardes in meegestuurde headers kan veranderen, zodat er cookies voor het verkeerde domein worden aangeleverd door de server. Bevinding 5.7.6 (laag).

  Aanbeveling: Zorg ervoor dat de invoer van een gebruiker nooit zonder controle gereflecteerd wordt als de server de invoer terugstuurt.

Aanvullingen Logius

Deze paragraaf is gereserveerd voor eventuele aanvullingen vanuit Logius.

1 Inleiding

1.1 Opdrachtformulering

DigID Release 5.9 is een release waarin veel kleine aanpassingen en uitbreidingen zijn gedaan. De scope van deze securitytest was de gehele DigID-applicatie, waarbij de nadruk lag op de risico's door de wijzigingen en/of uitbreidingen die in release 5.9 worden doorgevoerd.

In brede zin wordt in R5.9 gerealiseerd:

JIRA-ID	Omschrijving
DD-991	Gebruikersnaam bij midden/substantieel vervangen door koppelcode bij inloggen
DD-973	Faciliteren app2app authenticatie via koppelvlak
DD-1057	Piwik (Matomo)
DD-1030	Enrollment van en verhogen via kiosk
DD-1026	Beheer versies servicezuil
DD-1025	Beheer servicezuilen

In scope waren:

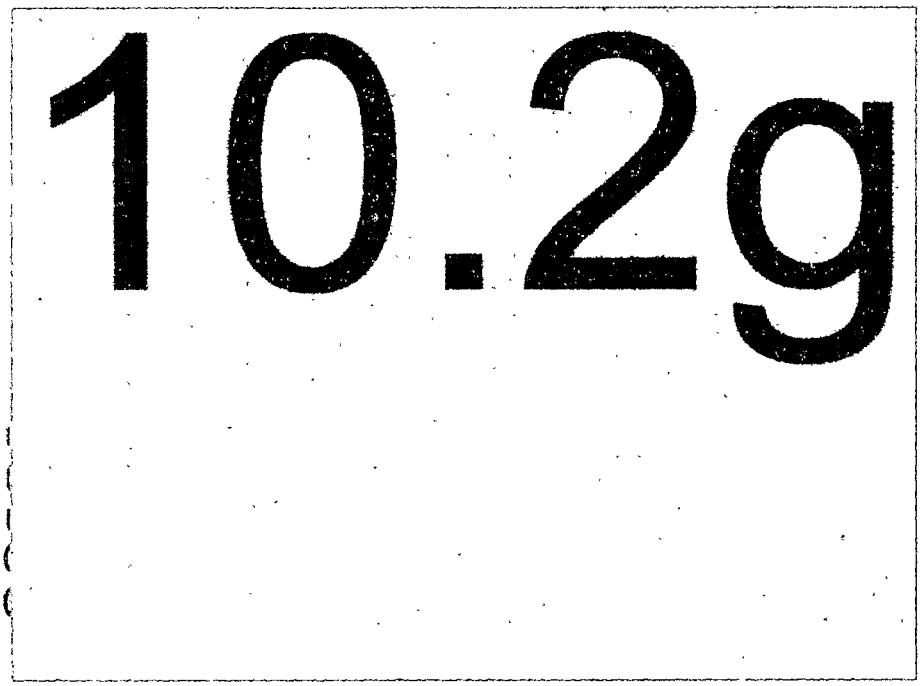
- Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
- Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
- Het verkeer tussen systemen buiten Kern (RDA-server, Status Controller, eID server) en DigID kern voor zover zichtbaar.

Onderstaande schematische weergave geeft een visuele representatie van wat wel en wat niet getest wordt binnen de scope van de securitytest[1]:

Onderdeel	Omranding / vulling	Omschrijving
Functioneel	Oranje / grijs	Binnen scope (voor zover extern benaderbaar)
DigiD Hoog (nieuw)	Oranje / geel	Binnen scope (voor zover extern benaderbaar)
DigiD Kern	Paars	Binnen scope (voor zover extern benaderbaar)
DigiD-Hoog/Substantieel/App	Groen	Alleen functioneel en berichtenverkeer
Infrastructuur	Blauw	Buiten scope, valt niet extern te testen
Certificaten (nieuw)	Geen / geel	Buiten scope, valt niet extern te testen
DigiD Extern	Geen / paars	Buiten scope, valt niet extern te testen

[1] *NB de scope van deze securitytest was dus niet gelijk aan de scope van de release*

derubricering



Er waren ook bevindingen aanwezig die geaccepteerd zijn of bekend zijn en niet opgelost.

IB bevindingen die geaccepteerd zijn

5.4.3 Gelijktijdige sessies
5.5.3 Wachtwoordsterkte onvoldoende
5.5.5 BEAST (Browser Exploit Against SSL/TLS)
5.5.1 Content-Security-Policy header implementatiefout
5.6.1 Cookie-domein te breed
5.6.2 Onvoldoende invoervalidatie Daring Fireball markup

IB bevindingen die bekend zijn en niet opgelost

5.7.3 Anti-Cross-Site-Scripting-header ontbreekt
5.7.4 X-Content-Type-Options header ontbreekt
5.7.6 Reflectie in header
5.6.3 SSL/TLS downgrade

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. De securitytest bestond uit een vulnerability-assessment met een diepgang greybox (hierbij krijgen de testers beschikking over documentatie en gebruikersrechten op het systeem, zodat het systeem met enige diepgang kan worden onderzocht) en betrof een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A4-omgeving.

derubricering

2 Resultaten

2.1 Cumulatief overzicht

Hieronder staat een totaaloverzicht van de bevindingen in dit rapport. Zie paragraaf 5.1 voor een toelichting op de risicoclassificatie.

In de tabel hieronder zijn zowel nieuwe bevindingen opgenomen als terugkerende bevindingen die nog niet opgelost zijn.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Sessiemanagement				1		**1**
Servers			1 & 1	2	1 & 1	**6**
Client-side controls					2	**2**
Totaal	**0**	**0**	**2**	**3**	**4**	**9**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	

[2] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Buiten scope voor deze test.

B.05 Contractmanagement

Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Oordeel

Buiten scope voor deze test.

B.06 ICT-landschap

Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Oordeel

Buiten scope voor deze test.

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel

Geen bevindingen.

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope voor deze test.

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope voor deze test.

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Bevinding 8

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Bevindingen 1, 2, 5, 6 en 7

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Bevinding 9

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

Bevinding 4

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen.

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Bevinding 3

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen.

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope voor deze test.

U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Geen bevindingen.

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de bevelliging.

Oordeel

Geen bevindingen.

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Geen bevindingen.

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Buiten scope voor deze test.

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Buiten scope voor deze test.

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen.

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope voor deze test.

U/NW.02 Beschikbaarheid van netwerken

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel

Buiten scope voor deze test.

U/NW.03 Netwerkzonering

Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Oordeel

Buiten scope voor deze test.

U/NW.04 Protectie- en detectiefunctie

Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Oordeel

Buiten scope voor deze test.

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buiten scope voor deze test.

U/NW.06 Hardening van netwerken

Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/NW.07 Netwerktoegang tot webapplicatie

Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Oordeel

Geen bevindingen.

U/NW.08 Netwerkarchitectuur

Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope voor deze test.

Beheersingsdomein

C.01 Servicemanagementbeleid

Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Oordeel

Buiten scope voor deze test.

C.02 Compliancemanagement

Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Oordeel

Buiten scope voor deze test.

C.03 Vulnerability-assessments

Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Oordeel

Buiten scope voor deze test.

C.04 Penetratietestproces

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Oordeel	

Geen bevindingen.

C.05 Technische controlefunctie

Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Oordeel	

Buiten scope voor deze test.

C.06 Logging

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Oordeel	

Buiten scope voor deze test.

C.07 Monitoring

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	

Buiten scope voor deze test.

C.08 Wijzigingenbeheer

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Oordeel	

Buiten scope voor deze test.

C.09 Patchmanagement

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Oordeel	

Buiten scope voor deze test.

C.10 Beschikbaarheidbeheer

Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Oordeel	

Buiten scope voor deze test.

C.11 Configuratiebeheer

Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Oordeel	

Geen bevindingen.

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Content-Security-Policy (CSP) header ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	5.4.2	Zeer Laag	Zeer Laag	Laag

Betreffende hosts
eid-a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP-header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Een voorbeeld waarbij geen externe scripts worden geladen en "inline-scripts" niet worden uitgevoerd:
Content-Security-Policy: default-src 'self'

Details for Client-side controls
De CSP-header is nu wel aanwezig op de volgende hosts:

- balie-a4.digid.nl
- cis-a4.digid.nl
- digidbeheer-a4.digid.nl (nieuw sinds vorige test)
- mijn.a4.digid.nl

Maar ontbreekt nog steeds op de volgende hosts:

- eid-a4.digid.nl

Voorbeeld antwoord:

```
HTTP/1.1 403 Forbidden
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Date: Mon, 12 Nov 2018 09:18:21 GMT
Connection: close
X-Content-Type-Options: nosniff
Content-Type: text/html
Content-Language: en-US
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html>
    <head>
        <title>Forbidden</title>
    </head>
    <body>
        <h1>Forbidden</h1>
    </body>
</html>
```

- rda-a4.digid.nl

Voorbeeld antwoord:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488815858000"
Last-Modified: Mon, 06 Mar 2017 15:57:38 GMT
Content-Type: text/html
Content-Length: 13
Date: Mon, 12 Nov 2018 09:20:50 GMT
Connection: close
Set-Cookie: _persist='HFC[  verwijderd  ];domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

- was-a4.digid.nl

Voorbeeld antwoord:

```
HTTP/1.1 404 Not Found
Date: Mon, 12 Nov 2018 12:38:54 GMT
X-Request-Id: 39be7f31-5c40-4d58-a543-fb801af348cc
X-Runtime: 0.002382
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE html>
<html lang="nl">
[... verwijderd ...]
```

3.1.2 *Content-Security-Policy header implementatiefout*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	5.8.1	Zeer Laag	Zeer Laag	Laag

Betreffende hosts
balie-a4.digid.nl
cis-a4.digid.nl
digidbeheer-a4.digid.nl (nieuw sinds vorige test)
mijn.a4.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven. De policy welke door de server verstuurd wordt is niet correct/veilig.

Bedreiging
Wanneer de CSP-header niet correct is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwen code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-policy zo strak mogelijk, waarbij onveilig gedrag niet toegelaten wordt. Bouw vanuit hier de policy uit met alleen die functionaliteit welke nodig is. Gebruik hierbij voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Details for Client-side controls
De CSP-header die wordt meegestuurd bevat onveilige waarden:

```
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline';
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Een overzicht van deze bevindingen.

3.4.1 Cross-site request forgery

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3		Laag	Zeer Laag	Laag

Betreffende hosts
a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl

Omschrijving
Bij het verwerken van ingevulde formulieren zou gecontroleerd moeten worden of het verzoek van de eigen site afkomstig is.

Bedreiging
Wanneer bij het verwerken van ingevulde formulieren niet wordt gecontroleerd of het verzoek van de eigen site afkomstig is, is het mogelijk om POST acties vanaf een andere site uit te voeren. Indien er gebruik gemaakt wordt van authenticatie, dan wordt deze actie uitgevoerd in dezelfde browser als waarin een gebruiker op de legitieme website is ingelogd.

Aanbeveling
CSRF kan voorkomen worden door het gebruik van een niet te voorspellen token in een formulier of url van elke HTTP request. Zo'n token moet op z'n minst uniek zijn per verzoek. OWASP's CSRF Guard https://www.owasp.org/index.php/CSRFGuard kan gebruikt worden om automatisch tokens toe te voegen in Java EE, .NET, of PHP applicaties. OWASP's ESAPI bevat token generators en validators die door ontwikkelaars gebruikt kunnen worden om transacties te beveiligen.

Details for Sessiemanagement
Het is mogelijk een gebruiker uit te loggen via een CSRF aanval. Hierdoor is het mogelijk om de website ontoegankelijk te maken wanneer een gebruiker een malafide plugin of tabblad heeft open staan. Door de interactie die benodigd is voor de installatie van bijvoorbeeld een plugin door een gebruiker, is de kans op zeer laag ingeschaald.

PoC digibeheer:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://digidbeheer-a4.digid.nl/destroy_session">
      <input type="hidden" name="session&#95;end" value="absolute" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Acc4

Beheer DigiD

Einde beheersessie

U bent uitgelogd of uw sessie is verlopen.
Sluit uw browser en start deze opnieuw om weer in te loggen.

Deze aanval is ook mogelijk op de mijn.digid omgeving:

PoC mijn digid:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://a4.digid.nl/uitloggen">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

DigiD

DigiD

U bent nu uitgelogd bij Mijn DigiD

› Terug naar www.digid.nl

Heeft u vragen of opmerkingen?

Bekijk de veelgestelde vragen (opent in een nieuw venster) of neem contact op (opent in een nieuw venster) met de DigiD helpdesk.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 Information disclosure – Credentials

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Midden	Zeer Laag	Hoog

Betreffende hosts
https://digidbeheer-a4.digid.nl/configurations

Omschrijving
De applicatie of het systeem lekt informatie over credentials. Deze informatie kan bijvoorbeeld in HTTP-headers of foutmeldingen worden getoond.

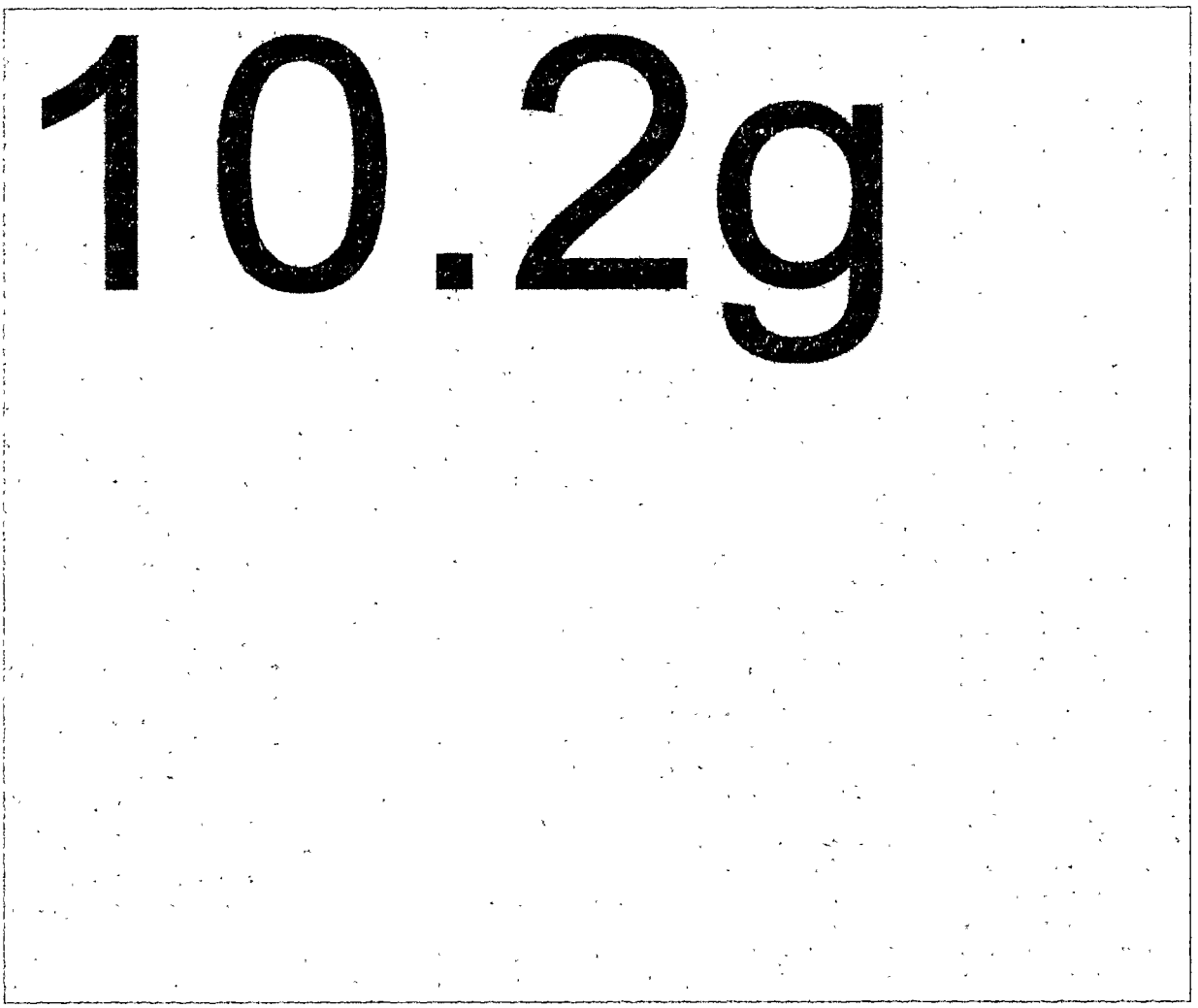
Bedreiging
De gelekte informatie kan door een aanvaller worden gebruikt om direct in te loggen op een applicatie of service of om bestaande gebruikers te kunnen enumereren.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Zorg er nooit credentials op het scherm getoond worden. Indien het echt nodig is om dit mogelijk te maken, toon de credentials dan eerst gemaskeerd en pas na expliciete opdracht van de gebruiker zichtbaar op het scherm.

derubricering

Details for Servers

10.2g



3.9.2 *Dubbele headers*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
digidbeheer-a4.digid.nl
balie-a4.digid.nl
mijn.a4.digid.nl
a4.digid.nl

Omschrijving
Binnen de server, applicatie of het systeem wordt inconsistent gebruik van headers gemaakt.

Bedreiging
Als gevolg hiervan zijn sommige pagina's mogelijk kwetsbaar voor aanvallen.

Aanbeveling
Zorg ervoor dat de headers consistent zijn en toepasselijk zijn voor de applicatie.

Details for Servers
De X-Frame-Options wordt dubbel verstuurd. Zowel met kleine letters als hoofdletters. Het is aanbevolen alleen de kleine letter variant te versturen. Dit om eventuele browser compatibility errors te voorkomen.
Response Headers:

```
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 14:35:20 GMT
Cache-Control: max-age=0, private, must-revalidate
X-XSS-Protection: 1; mode=block
X-Request-Id: fc01[… verwijderd …]
X-Frame-Options: SAMEORIGIN
X-Runtime: 0.121550
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
ETag: W/"4c8d11852a79d24c5565283a303b2b86"
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.9.3 *Anti-Cross-Site-Scripting-header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6	5.7.3	Midden	Laag	Hoog

Betreffende hosts
was-a4.digid.nl
rda-a4.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden standaard bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Gebruikers kunnen de bescherming handmatig uitschakelen, waardoor het voor aanvallers makkelijker wordt om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
"X-XSS-Protection: 1"
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging:
'X-XSS-Protection: 1; mode=block'
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie:
https://blogs.msdn.microsoft.com/ieinternals/2011/01/31/controlling-the-xss-filter/

Details for Servers
Door een aantal hosts wordt deze header niet meegestuurd.

- rda-a4.digid.nl

Voorbeeld antwoord:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488815858000"
Last-Modified: Mon, 06 Mar 2017 15:57:38 GMT
Content-Type: text/html
Content-Length: 13
Date: Mon, 12 Nov 2018 09:20:50 GMT
Connection: close
Set-Cookie: _persist=!HFC[... verwijderd... ];domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

- was-a4.digid.nl

Voorbeeld antwoord:

```
HTTP/1.1 404 Not Found
Date: Mon, 12 Nov 2018 12:38:54 GMT
X-Request-Id: 39be[... verwijderd... ]
X-Runtime: 0.002382
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE html>
<html lang="nl">
[... verwijderd ...]
```

3.9.4 *X-Content-Type-Options header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7	5.7.4	Laag	Laag	Laag

Betreffende hosts
was-a4.digid.nl
rda-a4.digid.nl

Omschrijving
De anti-MIME-sniffing header X-Content-Type-opties is niet ingesteld op 'nosniff'.

Bedreiging
Door het ontbreken van deze header wordt in oudere versies van Internet Explorer en Chrome MIME-sniffing toegepast op de response-body. Dit kan de response-body in een ander formaat weergeven dan het opgegeven content-type. Huidige (sinds begin 2014) versies van Firefox maken altijd gebruik van het opgegeven content-type (als er een is ingesteld).

Aanbeveling
Zorg ervoor dat de webserver de Content-Type header goed meestuurt, en dat de header X-Content-Type-Options is ingesteld op 'nosniff' voor alle webpagina's.

Details for Servers
- rda-a4.digid.nl

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488815858000"
Last-Modified: Mon, 06 Mar 2017 15:57:38 GMT
Content-Type: text/html
Content-Length: 13
Date: Mon, 12 Nov 2018 09:20:50 GMT
Connection: close
Set-Cookie: _persist=!HFC[... verwijderd... ];domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

- was-a4.digid.nl

```
HTTP/1.1 404 Not Found
Date: Mon, 12 Nov 2018 12:38:54 GMT
X-Request-Id: 39be[... verwijderd... ]
X-Runtime: 0.002382
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE html>
<html lang="nl">
[... verwijderd ...]
```

3.9.5 Reflectie in header

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
8	5.7.6	Laag	Laag	Laag

Betreffende hosts
cis-a4.digid.nl
digidbeheer-a4.digid.nl
mijn.a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl
eid-a4.digid.nl
a4.digid.nl

Omschrijving
Gegevens die door de server worden gestuurd naar de gebruiker bevatten veelal instructies voor browsers in de vorm van headers, naast natuurlijk de uiteindelijke content van de pagina. Meestal kunnen de meegestuurde headers niet worden beïnvloed of aangepast door de gebruiker. In dit geval is dit wel mogelijk.

Bedreiging
Door het wijzigen van bepaalde invoer die naar de server wordt gestuurd, kan een aanvaller bijvoorbeeld de inhoud van een teruggestuurde header controleren. De invoer wordt direct gereflecteerd naar de gebruiker in de uitvoer.

Aanbeveling
Filter alle mogelijke invoer van de gebruiker en zorg dat er geen headerwaardes direct gewijzigd kunnen worden door invoer in een web request te veranderen.

Details
De waarde van het cookie *_persist* in headers van de a4.digid.nl site is te beïnvloeden door in de request de Host header aan te passen.

Request:

```
GET / HTTP/1.1
Host: hi;test=true
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _session_id=95bd[... verwijderd ...]; _persist='9Ln[...
verwijderd ...]
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Thu, 15 Nov 2018 14:36:10 GMT
Content-Length: 347
Connection: close
Content-Type: text/html; charset=iso-8859-1
Set-Cookie: _persist='33Z[  verwijderd  ];domain=.hi;test=true;
HttpOnly,secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not
understand.<br />
</p>
<p>Additionally, a 400 Bad Request
error was encountered while trying to use an ErrorDocument to handle
the request.</p>
</body></html>
```

3.9.6 *SSL/TLS downgrade*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
9	5.6.3	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
balie-a4.digid.nl
cis-a4.digid.nl
digidbeheer-a4.digid.nl
mijn.a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl
eid-a4.digid.nl
a4.digid.nl

Omschrijving
De applicatie maakt gebruik van een SSL/TLS tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.
"openssl s_client -connect host:443 -state -fallback_scsv -tls1_1"

Bedreiging
Als een aanvaller kan optreden als "man in the middle" kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 12).
Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details for Servers

Voorbeeld voor a4.digid.nl:

```
sslscan a4.digid.nl
Version: 1.11.12-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 144.43.243.160

Testing SSL server a4.digid.nl on port 443 using SNI name a4.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256
DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256
DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256
DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256
DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  a4.digid.nl
Altnames: DNS:a4.digid.nl, DNS:was-a4.digid.nl, DNS:mijn.a4.digid.nl,
DNS:balie-a4.digid.nl, DNS:digidbeheer-a4.digid.nl, DNS:config-
a4.digid.nl, DNS:www.a4.digid.nl, DNS:stubs-a4.digid.nl, DNS:app-
a4.digid.nl, DNS:cis-a4.digid.nl, DNS:cts-a4.digid.nl
Issuer:   KPN PKIoverheid Organisatie CA - G2

Not valid before: Apr  7 11:03:30 2017 GMT
Not valid after:  Apr  7 11:03:30 2019 GMT
```

4 PAP-eisen

Hieronder wordt van de eisen uit het document aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

ID	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Geen bevindingen		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
5.7.4 Reflectie in header, 5.4.2 CSP-header ontbreekt		
ACC2.2.3	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Geen bevindingen		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en tolerantles Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.	DNSSEC
Geen bevindingen		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is	Ingetrokken certificaten
Geen bevindingen		

5 Bijlagen

5.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD R5.10

Kenmerk: 42100000 2019xx

Datum	31-01-2019
Status	Definitief
Versie	1.0

Rubricering	derubricering
Vaststeller	10.2e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**42100000 2019xx**
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius
	Postbus 96810
	2509 JE Den Haag
	servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
22-01-2019	0.1	Sogeti	Initiële versie
22-01-2019	0.2	Sogeti	Interne review
31-01-2019	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

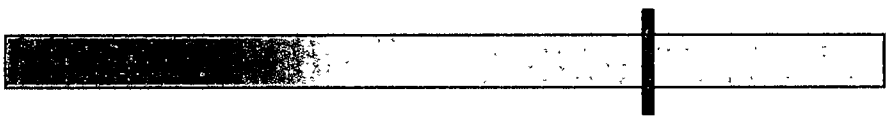
Managementsamenvatting

Inleiding

Dit Plan van Aanpak beschrijft concreet en specifiek de aanpak van deze voorgenomen securitytest op DigiD release 5.10. Dit plan is opgesteld in overleg met alle drie de betrokken partijen: Logius, auditor en auditee. En dit plan maakt onderdeel uit van de vrijwaringsverklaring tussen deze betrokkenen.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.10, zoals getest op de A4-omgeving voldoende is. Er zijn enkele nieuwe bevindingen gedaan met een laag en zeer laag risico. Daarnaast zijn er verschillende bevindingen onopgelost gebleven sinds de vorige test.



Onvoldoende Voldoende

Punten ter verbetering (nieuw):

- Tijdens de test zijn meerdere servers gevonden die een zogenaamde "Incrementeel IP ID" hebben. Dit maakt het mogelijk om informatie die over het internet wordt verstuurd via deze server te sturen. Hierdoor wordt het bijna onmogelijk om te achterhalen wie de aanval heeft uitgevoerd. Ook wordt er meer informatie wordt prijsgegeven over het interne systeem dan nodig. Zie bevinding #8
    - Aanbeveling: Zorg dat de hosts geen gebruik maken van incrementeel IP identiteit.
- Tijdens de test is er gevoelige informatie over de URL's van de DigiD omgeving gevonden op een externe website. Zie bevinding #4
    - Aanbeveling: Zorg dat de informatie niet meer publiekelijk toegankelijk is.

Punten ter verbetering terugkerende bevindingen (overgenomen uit het vorige rapport Rapport securitytest DigiD release 5.9 - v1.0.pdf):

- Een aantal headers die de gebruiker beschermen tijdens het gebruiken van de applicatie worden door de server niet standaard meegestuurd. Bevinding 5.7.3 (laag), Bevinding 5.7.4 (laag).

  Aanbeveling: Stuur deze headers mee vanuit de server om de gebruiker beter te beschermen tijdens het gebruik van de applicatie.
- De applicatie toont wachtwoorden in de beheerinterface. Dit zorgt ervoor dat iemand die op het scherm meekijkt deze wachtwoorden in handen kan krijgen. Zie bevinding 5.9.4.

  Aanbeveling: Toon bij voorkeur nooit wachtwoorden in een applicatie. Indien het echt noodzakelijk is voor de gebruiker om

wachtwoorden in te zien, toon ze dan eerst gemaskeerd. Maak het wachtwoord pas zichtbaar als een gebruiker daar expliciet opdracht toe geeft.

- Het is mogelijk om een gebruiker uit te loggen, bijvoorbeeld als die gebruiker een kwaadaardige website open heeft staan. Hierdoor is het mogelijk, zolang die kwaadaardige pagina open staat, DigiD onbruikbaar te maken voor de gebruiker. Zie bevinding 5.9.3.

  Aanbeveling: Verifieer voor alle acties die worden uitgevoerd of ze van de eigen site afkomstig zijn, door een unieke token mee te sturen.

Aanvullingen Logius

1 Inleiding

1.1 Opdrachtformulering

DigiD Release 5.10 is een release waarin veel kleine aanpassingen en uitbreidingen zijn gedaan. De scope van deze securitytest is de gehele DigiD-applicatie, waarbij de nadruk ligt op de risico's door de wijzingen en/of uitbreidingen die in release 5.10 worden doorgevoerd.

In brede zin wordt in R5.10 gerealiseerd:

JIRA-ID	Omschrijving
DD-1135	Substantieel door authentiseren
DD-1193	Met DigiD basis de DigID app activeren op niveau substantieel (zonder brief)

De scope van deze securitytest is de DigiD-applicatie, gezien vanaf een extern oogpunt, met extra aandacht op de impact als gevolg van aanpassingen die onderdeel zijn van release 5.10.

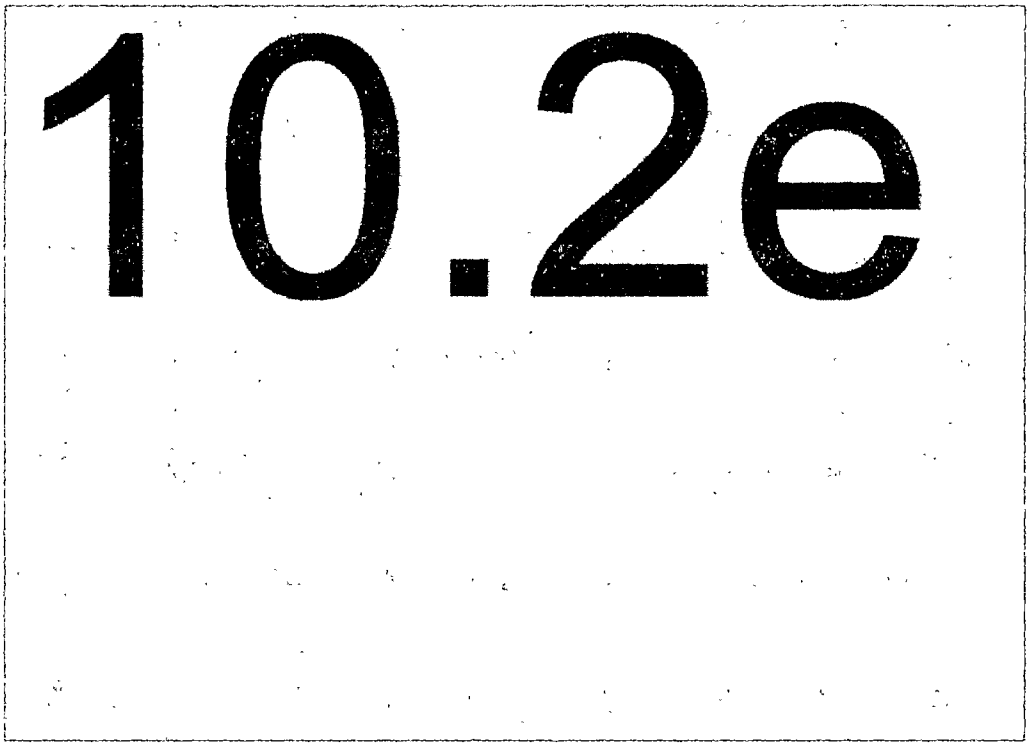
In scope:

- Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
- Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
- Het verkeer tussen systemen buiten Kern (RDA-server, Status Controller, eID server) en DigiD kern voor zover zichtbaar.

Onderstaande schematische weergave geeft een visuele representatie van wat wel en wat niet getest wordt binnen de scope van de securitytest[1]:

Onderdeel	Opvulling / vulling	Omschrijving
Functioneel	Oranje / grijs	Binnen scope (voor zover extern benaderbaar)
DigiD Hoog (nieuw)	Oranje / geel	Binnen scope (voor zover extern benaderbaar)
DigiD Kern	Paars	Binnen scope (voor zover extern benaderbaar)
DigiD-Hoog/Substantieel/App	Groen	Alleen functioneel en berichtenverkeer
Infrastructuur	Blauw	Buiten scope, valt niet extern te testen
Certificaten (nieuw)	Geen / geel	Buiten scope, valt niet extern te testen
DigiD Extern	Geen / paars	Buiten scope, valt niet extern te testen

[1] *NB de scope van de securitytest is dus niet gelijk aan de scope van de release*



IB bevindingen die geaccepteerd zijn

5.4.3 Gelijktijdige sessies
5.5.3 Wachtwoordsterkte onvoldoende
5.5.5 BEAST (Browser Exploit Against SSL/TLS)
5.5.1 Content-Security-Policy header implementatiefout
5.6.1 Cookie-domein te breed
5.6.2 Onvoldoende invoervalidatie Daring Fireball markup

IB bevindingen die bekend zijn en niet opgelost

5.7.3 Anti-Cross-Site-Scripting-header ontbreekt
5.7.4 X-Content-Type-Options header ontbreekt
5.7.6 Reflectie in header
5.6.3 SSL/TLS downgrade

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd.

Bij een vulnerability assessment wordt het domein nauwkeurig onderzocht aan de hand van een in huis ontwikkelde methodiek. Tooling is daarbij ondergeschikt aan de kennis en expertise van de securityconsultants. Weliswaar wordt gestart met een automated test inclusief manual verification, maar aanvullend daarop vindt ook een beoordeling plaats van alles wat een tool alleen niet kan vinden. Een vulnerability assessment levert een overzicht van alle aanwezige technische zwakheden, die binnen een vooraf gestelde 'time box' zijn gevonden.

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Grey box.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

In de tabel hieronder zijn zowel nieuwe bevindingen opgenomen als terugkerende bevindingen die nog niet opgelost zijn.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Sessiemanagement	0	0	0	1	0	1
Servers	0	0	0	1	2 & 2	2 & 3
Client-side controls	0	0	1	0	1	2
Totaal	**0**	**0**	1	2	**2 & 3**	**2 & 6**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope van deze test	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope van deze test	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope van deze test	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	

[2] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Oordeel	
Buiten scope van deze test	

B.05 Contractmanagement

Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Oordeel	
Buiten scope van deze test	

B.06 ICT-landschap

Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Oordeel	
Buiten scope van deze test	

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel	
Geen bevindingen	

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel	
Buiten scope voor deze test.	

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel	
Buiten scope voor deze test.	

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel	
Geen bevindingen.	

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel	
Zie bevinding 1, 5, 6	

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel	
Zie bevinding 7	

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel	
Zie bevinding 3	

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Zie bevinding 2

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen.

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope voor deze test.

U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Geen bevindingen.

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel

Zie bevinding 4

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Geen bevindingen.

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Buiten scope voor deze test.

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Buiten scope voor deze test.

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Zie bevinding 8

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope voor deze test.

U/NW.02 Beschikbaarheid van netwerken

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel

Buiten scope voor deze test.

U/NW.03 Netwerkzonering

Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Oordeel

Buiten scope voor deze test.

U/NW.04 Protectie- en detectiefunctie

Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Oordeel

Buiten scope voor deze test.

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buten scope voor deze test.

U/NW.06 Hardening van netwerken

Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/NW.07 Netwerktoegang tot webapplicatie

Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Oordeel

Geen bevindingen.

U/NW.08 Netwerkarchitectuur

Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope voor deze test.

Beheersingsdomein

C.01 Servicemanagementbeleid

Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Oordeel

Buiten scope voor deze test.

C.02 Compliancemanagement

Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Oordeel

Buiten scope voor deze test.

C.03 Vulnerability-assessments

Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Oordeel

Buiten scope voor deze test.

C.04 Penetratietestproces

derubricering

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Oordeel	

Geen bevindingen.

C.05	**Technische controlefunctie**

Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Oordeel	

Buiten scope voor deze test.

C.06	**Logging**

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Oordeel	

Buiten scope voor deze test.

C.07	**Monitoring**

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	

Buiten scope voor deze test.

C.08	**Wijzigingenbeheer**

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Oordeel	

Buiten scope voor deze test.

C.09	**Patchmanagement**

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Oordeel	

Buiten scope voor deze test.

C.10	**Beschikbaarheidbeheer**

Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Oordeel	

Buiten scope voor deze test.

C.11	**Configuratiebeheer**

Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Oordeel	

Geen bevindingen.

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Content-Security-Policy (CSP) header ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1		Laag	Zeer Laag	Laag

Betreffende hosts
eid-a4.digid.nl
was-a4.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP-header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en "inline-scripts" niet worden uitgevoerd:
Content-Security-Policy: default-src 'self'

Details
De CSP-header ontbreken nog op de volgende hosts:
- eid-a4.digid.nl

```
HTTP/1.1 403 Forbidden
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Date: Mon, 21 Jan 2019 10:55:22 GMT
Connection: close
X-Content-Type-Options: nosniff
Content-Type: text/html
Content-Language: en-US
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html>
    <head>
        <title>Forbidden</title>
    </head>
    <body>
        <h1>Forbidden</h1>
    </body>
</html>
```

- was-a4.digid.nl

```
HTTP/1.1 404 Not Found
Date: Mon, 21 Jan 2019 11:07:17 GMT
X-Request-Id: 0ca728ba-f787-4b75-8ad7-53914ad66986
X-Runtime: 0.004565
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter

genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Een overzicht van deze bevindingen.

3.4.1 *Cross-site request forgery*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2		Laag	Zeer Laag	Laag

Betreffende hosts
a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl

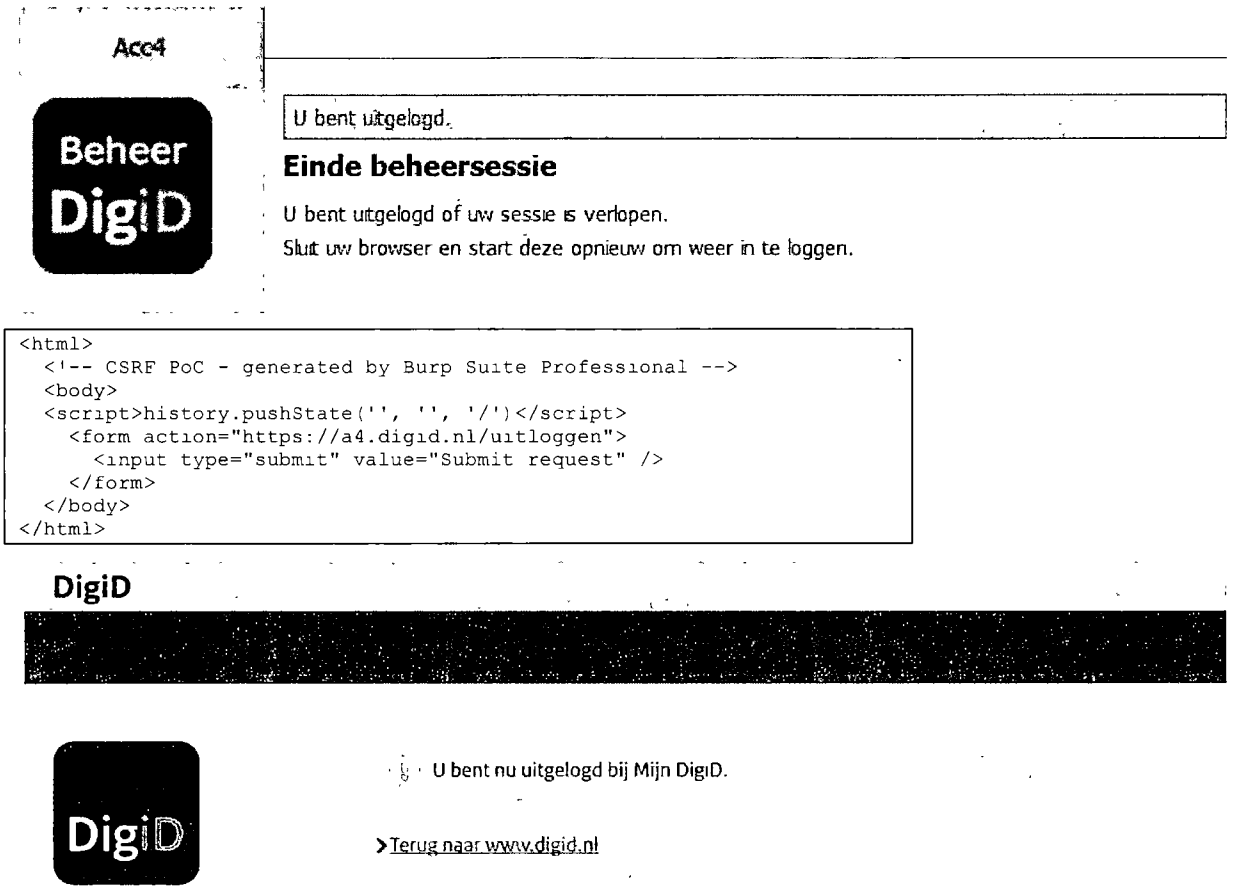
Omschrijving
Bij het verwerken van ingevulde formulieren zou gecontroleerd moeten worden of het verzoek van de eigen site afkomstig is.

Bedreiging
Wanneer bij het verwerken van ingevulde formulieren niet wordt gecontroleerd of het verzoek van de eigen site afkomstig is, is het mogelijk om POST acties vanaf een andere site uit te voeren. Indien er gebruik gemaakt wordt van authenticatie, dan wordt deze actie uitgevoerd in dezelfde browser als waarin een gebruiker op de legitieme website is ingelogd.

Aanbeveling
CSRF kan voorkomen worden door het gebruik van een niet te voorspellen token in een formulier of url van elke HTTP request. Zo'n token moet op z'n minst uniek zijn per verzoek. OWASP's CSRF Guard https://www.owasp.org/index.php/CSRFGuard kan gebruikt worden om automatisch tokens toe te voegen in Java EE, .NET, of PHP applicaties. OWASP's ESAPI bevat token generators en validators die door ontwikkelaars gebruikt kunnen worden om transacties te beveiligen.

Details
Het is mogelijk een gebruiker uit te loggen via een CSRF aanval. Hierdoor is het mogelijk om de website ontoegankelijk te maken wanneer een gebruiker een malafide plug-in of tabblad heeft open staan. Door de interactie die benodigd is voor de installatie van bijvoorbeeld een plug-in door een gebruiker, is de kans op zeer laag ingeschaald.

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://digidbeheer-a4.digid.nl/destroy_session">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 Information disclosure – Credentials

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3		Midden	Zeer Laag	Hoog

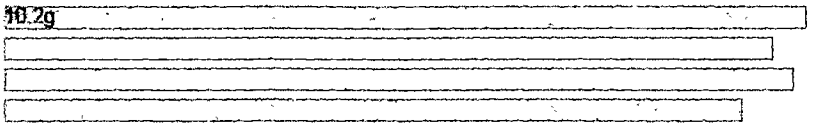
Betreffende hosts
digidbeheer-a4.digid.nl

Omschrijving
De applicatie of het systeem lekt informatie over credentials. Deze informatie kan bijvoorbeeld in HTTP-headers of foutmeldingen worden getoond.

Bedreiging
De gelekte informatie kan door een aanvaller worden gebruikt om direct in te loggen op een applicatie of service of om bestaande gebruikers te kunnen enumereren.

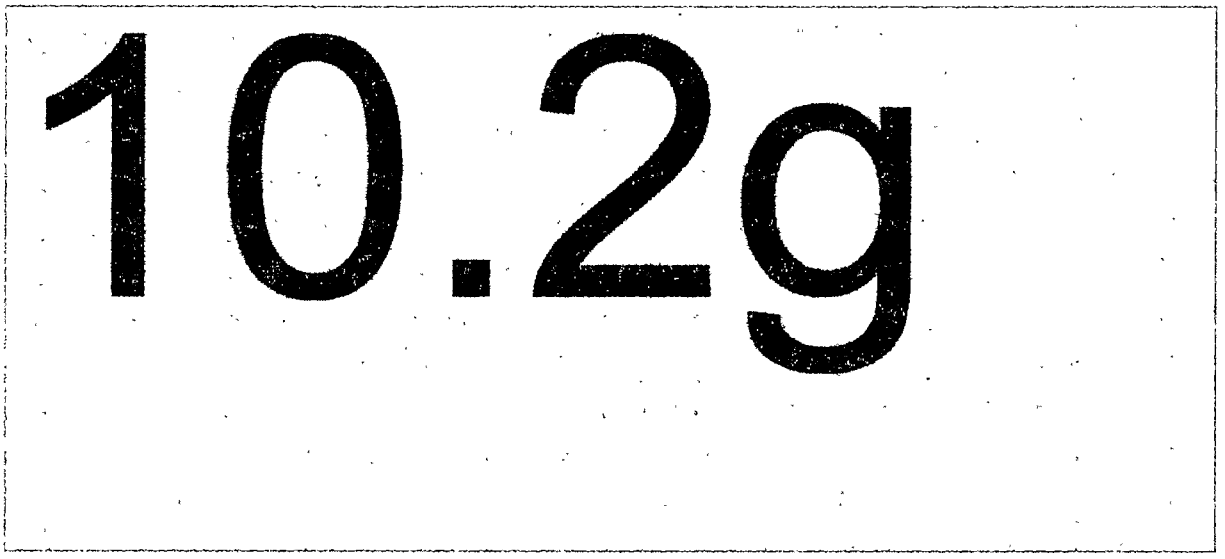
Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Zorg er nooit credentials op het scherm getoond worden. Indien het echt nodig is om dit mogelijk te maken, toon de credentials dan eerst gemaskeerd en pas na expliciete opdracht van de gebruiker zichtbaar op het scherm.

Details



derubricering

10.2g



3.9.2 *Information disclosure – Gevoelige informatie publiekelijk toegankelijk*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Zeer Laag	Zeer Laag	Laag

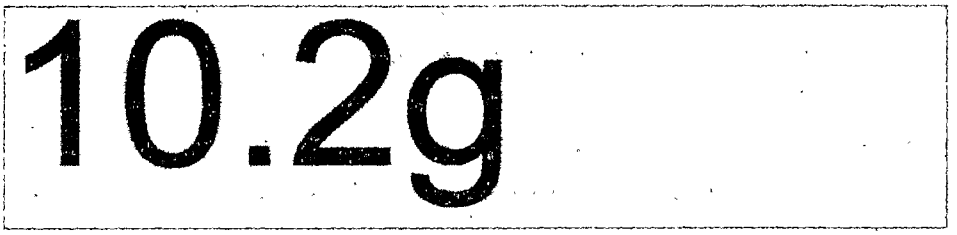
Betreffende hosts
*.digid.nl

Omschrijving
Informatie over de (interne) werking/logica van het systeem zelf, de (onderliggende) infrastructuur, privacygevoelige data of gerelateerd aan toegangsmanagement is publiekelijk toegankelijk.

Bedreiging
De informatie kan een aanvaller inzicht geven over gebruikte technologieën, omgevingen en software. Dit vergroot de kans dat er een aanval kan worden uitgevoerd op een systeem.

Aanbeveling
Zorg ervoor dat de informatie niet meer publiekelijk toegankelijk is, door bijvoorbeeld contact op te nemen met de externe partij waar de informatie te vinden is.

10.2g



3.9.3 *Dubbele Headers*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
digidbeheer-a4.digid.nl
balie-a4.digid.nl
mijn.a4.digid.nl
a4.digid.nl

Omschrijving
Binnen de server, applicatie of het systeem wordt inconsistent gebruik van headers gemaakt.

Bedreiging
Als gevolg hiervan zijn sommige pagina's mogelijk kwetsbaar voor aanvallen.

Aanbeveling
Zorg ervoor dat de headers consistent en toepasselijk zijn voor de oplossing.

Details
De X-Frame-Options wordt dubbel verstuurd. Zowel met kleine letters als hoofdletters. Het is aanbevolen alleen de kleine letter variant te versturen. Dit om eventuele browser compatibility errors te voorkomen.

Response Headers:

```
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 14:35:20 GMT
Cache-Control: max-age=0, private, must-revalidate
X-XSS-Protection: 1; mode=block
X-Request-Id: fc01[… verwijderd …]
X-Frame-Options: SAMEORIGIN
X-Runtime: 0.121550
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
ETag: W/"4c8d11852a79d24c5565283a303b2b86"
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.9.4 *Anti-Cross-Site-Scripting-header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6		Midden	Laag	Hoog

Betreffende hosts

rda-a4.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden standaard bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Gebruikers kunnen de bescherming handmatig uitschakelen, waardoor het voor aanvallers makkelijker wordt om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
"X-XSS-Protection: 1"
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging:
'X-XSS-Protection: 1; mode=block'
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie:
https://blogs.msdn.microsoft.com/ieinternals/2011/01/31/controlling-the-xss-filter/

Details
Door een aantal hosts wordt deze header niet meegestuurd.
- rda-a4.digid.nl
Voorbeeld antwoord:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488815858000"
Last-Modified: Mon, 06 Mar 2017 15:57:38 GMT
Content-Type: text/html
Content-Length: 13
Date: Mon, 12 Nov 2018 09:20:50 GMT
Connection: close
Set-Cookie: _persist=!HFC[... verwijderd... ];domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

3.9.5 *SSL/TLS downgrade*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
balie-a4.digid.nl
cis-a4.digid.nl
digidbeheer-a4.digid.nl
mijn.a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl
eid-a4.digid.nl
a4.digid.nl

Omschrijving
De applicatie maakt gebruik van een SSL/TLS tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.
"openssl s_client -connect host:443 -state -fallback_scsv -tls1_1"

Bedreiging
Als een aanvaller kan optreden als "man in the middle" kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 12).
Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details
Voorbeeld voor a4.digid.nl

```
root@kali:~# sslscan a4.digid.nl
Version: 1.11.12-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 144.43.243.160

Testing SSL server a4.digid.nl on port 443 using SNI name a4.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported
```

```
  TLS Compression:
Compression disabled
[..snip..]
```

3.9.6 *Serverconfiguratie fout – Zombie machine*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
8		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
144.43.243.145
144.43.243.144
144.43.243.146
144.43.243.148
144.43.243.147
144.43.243.150
144.43.243.152
144.43.243.155
144.43.243.154
144.43.243.149

Omschrijving
Een of meerdere machines heeft een incrementeel IP ID. Deze machines worden "zombies" genoemd. Een zombie machine staat tussen de aanvaller en het doelwit in en geeft alle pakketjes tussen beide partijen door. Er is geen interactie tussen de machine van de aanvaller en het doel: de aanvaller heeft uitsluitend interactie met de zombie machine. Hierdoor is (bijna) niet te achterhalen wie een scan heeft uitgevoerd. Tevens denkt het doelwit dat een bekende machine verbinding probeert te maken, waardoor meer informatie over open poorten bekend kan raken bij de aanvaller.

Bedreiging
Het wordt mogelijk een idle-scan uit te voeren, waar een zombie machine voor vereist is. De werking van een idle-scan is gebaseerd op de FragmentationId-headers (een unieke identificatiecode, maakt deel uit van elk IP-pakket en zit in de IP-header). Bij een idle-scan wordt de identiteit van een zombie machine waargenomen. Het doelwit denkt dat een interne computer (de zombie) verbinding probeert te maken en kan verbindingen accepteren. Hierdoor worden open poorten inzichtelijk die met een normale scan niet inzichtelijk kunnen zijn.

Aanbeveling
Zorg dat de machines geen incrementeel IP ID in de IP-header bevat.

Details
Er zijn meerdere zombie machines aangetroffen. In de onderstaande output is dit zichtbaar voor een specifiek IP-adres. Alle IP-adressen binnen scope zijn nagelopen.

```
root@kali:~# nmap 144.43.243.145 --script ipidseq -v
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-21 13:17 CET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
```

```
Initiating NSE at 13:17
[...]

Host script results:
|_ipidseq: Incremental!

[...]
```

4 PAP-eisen

Hieronder wordt van de eisen uit het document aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

ID	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Geen bevindingen		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
5.4.2 CSP-header ontbreekt		
ACC2.2.3	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Geen bevindingen		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en tolerantles Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.	DNSSEC
Geen bevindingen		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is	Ingetrokken certificaten
Geen bevindingen		

5 Bijlagen

5.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-around' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD release 5.11

Kenmerk: 2019DigiD5.11

Datum	25-04-2019
Status	Definitief
Versie	1.0

Rubricering	derubricering
Vaststeller	10.2 e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**2019DigiD5.11**
Versienummer	1.0
Contactpersoon	[redacted]
Organisatie	Logius
	Postbus 96810
	2509 JE Den Haag
	servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
18-04-2019	0.1	Sogeti Nederland BV	Initiële versie
18-04-2019	0.2	Sogeti Nederland BV	Interne review
25-04-2019	1.0	Sogeti Nederland BV	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
[redacted]	[redacted]	[redacted]	[redacted]

Inhoud

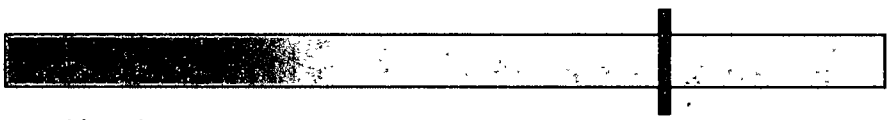
Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest was de aanstaande release 5.11 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is gedurende de test extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook zijn er voorstellen gedaan hoe de gevonden kwetsbaarheden gemitigeerd kunnen worden.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.11, zoals getest op de A4-omgeving voldoende is. Er zijn geen nieuwe bevindingen gedaan maar er zijn wel verschillende bevindingen onopgelost gebleven sinds de vorige test.



Onvoldoende Voldoende

Belangrijkste bevindingen ter verbetering:

A. De applicatie toont nog steeds wachtwoorden in de beheerinterface. Dit zorgt ervoor dat iemand die op het scherm meekijkt die wachtwoorden in handen kan krijgen. Zie bevinding 6 (Mantis nnb).
Aanbeveling: Toon bij voorkeur nooit wachtwoorden in een applicatie. Indien het echt noodzakelijk is voor de gebruiker om wachtwoorden in te zien, toon ze dan eerst gemaskeerd. Maak het wachtwoord pas zichtbaar als een gebruiker daar expliciet opdracht toe geeft.

B. Het is nog steeds mogelijk om een gebruiker uit te loggen, bijvoorbeeld als die gebruiker een kwaadaardige website open heeft staan. Hierdoor is het mogelijk, zolang die kwaadaardige pagina open staat, DigiD onbruikbaar te maken voor de gebruiker. Zie bevinding 4 (Mantis nnb).
Aanbeveling: Verifieer altijd voor alle acties die worden uitgevoerd of ze van de eigen site afkomstig zijn, door een unieke token mee te sturen.

C. In sommige gevallen wordt niet optimaal gebruikgemaakt van de beschikbare beveiligingsmechanismen. Zie bevinding 1 (Mantis 5.7.3), 2 (Mantis 5.4.2) en 3 (Mantis 5.7.4).
Aanbeveling: pas de beveiligingsmechanismen alsnog toe.

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

DigiD Release 5.11 is een release met als belangrijkste wijzigingen de toevoeging van DigiD Hoog eNIK-functionaliteit, een nieuw design en de mogelijkheid om van interfacetaal te wisselen. 10.2g
10.2g De scope van deze securitytest was de gehele DigiD-applicatie, waarbij de nadruk lag op de risico's door de wijzingen en/of uitbreidingen die in release 5.11 worden doorgevoerd.

In brede zin wordt in R5.11 gerealiseerd:

JIRA-ID	Omschrijving
DGDC-210	Tekstueel "Controle rijbewijs" veranderen in "inloggen met Rijbewijs"
DGDC-219	Pilot DigiD Kiosk Zuil
DGDC-220	Promotie DigiD app in notificatie emails en sms berichten
10.2g	[redacted]
DGDC-262	Toevoegen zoeken/uitvragen accountgegevens op basis van gebruikersnaam. (DigiD beheer)
DGDC-314	App2app: URL check in subdomein afnemer
DGDC-328	DigiD Hoog eNIK: Inloggen met identiteitskaart
DGDC-331	DigiD Hoog eNIK: Blokkeren identiteitskaart via Servicecentrum
DGDC-332	DigiD Hoog eNIK: Aanvragen PIN/PUK brief identiteitskaart via Servicecentrum
DGDC-335	DigiD Hoog eNIK: Deblokkeren identiteitskaart (incl aanvragen deblokkeringscode per brief)
DGDC-337	DigiD Hoog eNIK: Gegevens identiteitskaart inzien door beheerder
DGDC-389	Content-Security-Policy (CSP) header ontbreekt (5.9.1)
DGDC-399	Information disclosure - Credentials (5.9.4)
DGDC-617	Beheer PDF Activeringsbrieven van SVB-burger niet correct
DGDC-428	Verleiden tot verhogen account na te lage authenticatie

In de PRA zijn de onderdelen bepaald die tijdens de securitytest niet onderzocht kunnen of hoeven te worden. Deze zijn in de tabel hierboven grijs gemarkeerd.

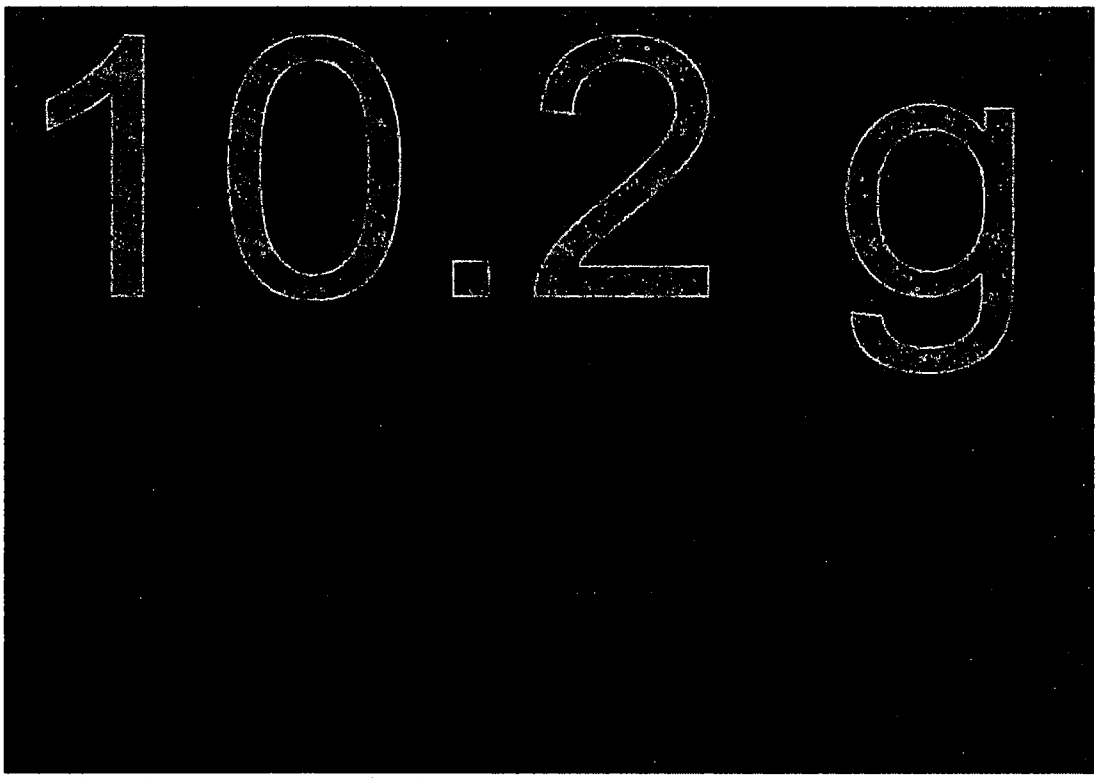
De scope van deze securitytest was de DigiD-applicatie, gezien vanaf een extern oogpunt, met extra aandacht op de impact als gevolg van aanpassingen die onderdeel zijn van release 5.11.

In scope:

- Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
- Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
- Het verkeer tussen systemen buiten Kern (RDA-server, Status Controller, eID server) en DigiD kern voor zover zichtbaar.

Onderstaande schematische weergave geeft een visuele representatie van wat wel en wat niet getest wordt binnen de scope van de securitytest[1]:

Onderdeel	Omranding / vulling	Omschrijving
Functioneel	Oranje / grijs	Binnen scope (voor zover extern benaderbaar)
DigiD Hoog (nieuw)	Oranje / geel	Binnen scope (voor zover extern benaderbaar)
DigiD Kern	Paars	Binnen scope (voor zover extern benaderbaar)
DigiD-Hoog/Substantieel/App	Groen	Alleen functioneel en berichtenverkeer
Infrastructuur	Blauw	Buiten scope, valt niet extern te testen
Certificaten (nieuw)	Geen / geel	Buiten scope, valt niet extern te testen
DigiD Extern	Geen / paars	Buiten scope, valt niet extern te testen



Tijdens de securitytest is ook gelet op eventuele regressie dan wel ongeautoriseerde of onbedoelde veranderingen.

Tijdens eerdere tests op DigiD is een aantal bevindingen gedaan welke in release 5.11 zijn opgelost en daarom specifiek opnieuw moesten worden getest of waarvan bekend is dat het risico is geaccepteerd. Deze bevindingen zijn:

Opgeloste bevindingen
Geen

IB bevindingen die geaccepteerd zijn
5.4.3 Gelijktijdige sessies
5.5.3 Wachtwoordsterkte onvoldoende
5.5.5 BEAST (Browser Exploit Against SSL/TLS)
5.5.1 Content-Security-Policy header implementatiefout
5.6.1 Cookie-domein te breed

[1] *NB de scope van de securitytest is dus niet gelijk aan de scope van de release*

5.6.2 Onvoldoende invoervalidatie Daring Fireball markup

IB bevindingen die bekend zijn en niet opgelost

5.7.3 Anti-Cross-Site-Scripting-header ontbreekt
5.7.4 X-Content-Type-Options header ontbreekt
5.7.6 Reflectie in header
5.6.3 SSL/TLS downgrade

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. De securitytest bestond uit een vulnerability-assessment met een diepgang greybox (hierbij krijgen de testers beschikking over documentatie en gebruikersrechten op het systeem, zodat het systeem met enige diepgang kan worden onderzocht) en betrof een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A4-omgeving.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 5.1 voor een toelichting op de risicoclassificatie.

In de tabel hieronder zijn zowel nieuwe bevindingen opgenomen als terugkerende bevindingen die nog niet opgelost zijn.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Client-Side Controls			1	1	1	3
Servers			1		1	2
Invoerafhandeling				2		2
Totaal			2	3	2	7

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test	
B.04	**Cryptografiebeleid**

[2] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).

Oordeel

Buiten scope voor deze test

B.05 Contractmanagement

Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Oordeel

Buiten scope voor deze test

B.06 ICT-landschap

Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Oordeel

Buiten scope voor deze test

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel

Geen bevindingen

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope voor deze test

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope voor deze test

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Bevinding: 1, 2, 4, 5

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Bevinding: 1, 2, 3, 5

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Bevinding: 7

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

derubricering

Bevinding 6

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Bevinding: 4

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope voor deze test

U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Geen bevindingen

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel

Geen bevindingen

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Geen bevindingen

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Buiten scope voor deze test

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Buiten scope voor deze test

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope voor deze test

U/NW.02 Beschikbaarheid van netwerken
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.
Oordeel
Buiten scope voor deze test
U/NW.03 Netwerkzonering
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.
Oordeel
Buiten scope voor deze test
U/NW.04 Protectie- en detectiefunctie
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.
Oordeel
Buiten scope voor deze test
U/NW.05 Beheer- en productieomgeving
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.
Oordeel
Buiten scope voor deze test
U/NW.06 Hardening van netwerken
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Oordeel
Geen bevindingen
U/NW.07 Netwerktoegang tot webapplicatie
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.
Oordeel
Geen bevindingen
U/NW.08 Netwerkarchitectuur
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.
Oordeel
Buiten scope voor deze test

Beheersingsdomein

C.01 Servicemanagementbeleid
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
Oordeel
Buiten scope voor deze test
C.02 Compliancemanagement
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.
Oordeel
Buiten scope voor deze test
C.03 Vulnerability-assessments
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.
Oordeel
Buiten scope voor deze test

derubricering

C.04	Penetratietestproces
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Geen bevindingen	

C.05	Technische controlefunctie
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Buiten scope voor deze test	

C.06	Logging
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Buiten scope voor deze test	

C.07	Monitoring
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Buiten scope voor deze test	

C.08	Wijzigingenbeheer
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Buiten scope voor deze test	

C.09	Patchmanagement
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Buiten scope voor deze test	

C.10	Beschikbaarheidbeheer
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope voor deze test	

C.11	Configuratiebeheer
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Geen bevindingen	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Anti-Cross-Site-Scripting-header ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	5.7.3	Midden	Laag	Hoog

Betreffende hosts
was-a4.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Wanneer de cross-site-scripting bescherming niet is ingeschakeld, wordt het voor aanvallers makkelijker om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
"X-XSS-Protection: 1"
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging:
'X-XSS-Protection: 1; mode=block'
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Details for ClientSideControls
Eén van de hosts uit de scope stuurt de header niet naar de browser.

Voorbeeld responseheaders was-a4.digid.nl:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 01 Apr 2019 15:38:53 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=99
Content-Type: image/svg+xml
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 15 Apr 2019 13:29:09 GMT
Expires: Tue, 14 Apr 2020 13:29:09 GMT
Age: 0
Content-Length: 21493
```

3.1.2 *Content-Security-Policy (CSP) header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	5.4.2	Zeer Laag	Zeer Laag	Laag

Omschrijving
Content Security Policy (CSP) is een beveiligingsmechanisme in moderne browsers dat is ontwikkeld om te voorkomen dat inhoud vanaf een niet vertrouwde bron ingeladen of uitgevoerd wordt. De server initieert dit door een header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt deze header heeft ontvangen, dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer inhoud inlaadt die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP-header niet is geïmplementeerd kan, een aanvaller inhoud inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld kwaadaardige code (XSS) uitgevoerd worden, of ongewilde inhoud getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en *inline-scripts* niet worden uitgevoerd:
Content-Security-Policy: default-src 'self'

Details for ClientSideControls
Er zijn nog vier hosts die de CSP-header niet meesturen naar de browser.

Voorbeeld responseheaders was-a4.digid.nl:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 01 Apr 2019 15:38:53 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=99
Content-Type: image/svg+xml
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 15 Apr 2019 13:29:09 GMT
Expires: Tue, 14 Apr 2020 13:29:09 GMT
Age: 0
Content-Length: 21493
```

3.1.3 *X-Content-Type-Options header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3	5.7.4	Laag	Laag	Laag

Betreffende hosts
was-a4.digid.nl

Omschrijving
De anti-MIME-sniffing header X-Content-Type-opties is niet ingesteld op 'nosniff'.

Bedreiging
Door het ontbreken van deze header wordt in oudere versies van Internet Explorer en Chrome MIME-sniffing toegepast op de response-body. Dit kan de response-body in een ander formaat weergeven dan het opgegeven content-type. Huidige (sinds begin 2014) versies van Firefox maken altijd gebruik van het opgegeven content-type (als er een is ingesteld).

Aanbeveling
Zorg ervoor dat de webserver de Content-Type header goed meestuurt, en dat de header X-Content-Type-Options is ingesteld op 'nosniff' voor alle webpagina's.

Details for ClientSideControls
Eén van de hosts uit de scope stuurt de header niet naar de browser.

Voorbeeldresponse:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 01 Apr 2019 15:38:53 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=99
Content-Type: image/svg+xml
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 15 Apr 2019 13:29:09 GMT
Expires: Tue, 14 Apr 2020 13:29:09 GMT
Age: 0
Content-Length: 21493
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 *Cross-site request forgery*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Laag	Zeer Laag	Laag

Betreffende hosts
a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl

Omschrijving
Bij het verwerken van ingevulde formulieren zou gecontroleerd moeten worden of het verzoek van de eigen site afkomstig is.

Bedreiging
Wanneer bij het verwerken van ingevulde formulieren niet wordt gecontroleerd of het verzoek van de eigen site afkomstig is, is het mogelijk om POST acties vanaf een andere site uit te voeren. Indien er gebruik gemaakt wordt van authenticatie, dan wordt deze actie uitgevoerd in dezelfde browser als waarin een gebruiker op de legitieme website is ingelogd.

Aanbeveling
CSRF kan voorkomen worden door het gebruik van een niet te voorspellen token in een formulier of URL van elke HTTP request. Zo'n token moet op z'n minst uniek zijn per verzoek. OWASP's CSRF Guard: https://www.owasp.org/index.php/CSRFGuard kan gebruikt worden om automatisch tokens toe te voegen in Java EE, .NET, of PHP-applicaties. OWASP's ESAPI bevat token generators en validators die door ontwikkelaars gebruikt kunnen worden om transacties te beveiligen.

Details for Invoerafhandeling
Het is mogelijk een gebruiker uit te loggen via een CSRF-aanval. Hierdoor is het mogelijk om de website ontoegankelijk te maken wanneer een gebruiker een malafide plugin of tabblad heeft open staan. Door de interactie die benodigd is voor de installatie van bijvoorbeeld een plugin door een gebruiker, is de kans op zeer laag ingeschaald.

Proof-of-Concept CSRF-uitlogknop:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://a4.digid.nl/uitloggen">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3.7.2 *Reflectie in header*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5	5.7.6	Laag	Laag	Laag

Betreffende hosts
a4.digid.nl
cis-a4.digid.nl
digidbeheer-a4.digid.nl
eid-a4.digid.nl
mijn.a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl

Omschrijving
Gegevens die door de server worden gestuurd naar de gebruiker bevatten veelal instructies voor browsers in de vorm van headers, naast natuurlijk de uiteindelijke content van de pagina. Meestal kunnen de meegestuurde headers niet worden beïnvloed of aangepast door de gebruiker. In dit geval is dit wel mogelijk.

Bedreiging
Door het wijzigen van bepaalde invoer die naar de server wordt gestuurd, kan een aanvaller bijvoorbeeld de inhoud van een teruggestuurde header controleren. De invoer wordt direct gereflecteerd naar de gebruiker in de uitvoer.

Aanbeveling
Filter alle mogelijke invoer van de gebruiker en zorg dat er geen headerwaardes direct gewijzigd kunnen worden door invoer in een web request te veranderen.

Details for Invoerafhandeling
De waarde van het cookie *_persist* in de response headers van verschillende hosts is te beïnvloeden door in de request de *Host*-header aan te passen.

Request:

```
GET / HTTP/1.1
Host: a4.digid.nl;INJECTIE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 400 Bad Request
Date: Wed, 17 Apr 2019 11:07:29 GMT
Content-Length: 347
Connection: close
Content-Type: text/html; charset=iso-8859-1
Set-Cookie:
_persist=!oyaWc8tUeljwq+XsW2TPUSuPJujzzAnbJENGIIXVmHLArZOZFbpDaTbBv2tH
ZypIbTbb0J4LclenZuydvSXJnk8gvaj3HIw8ZYpHfm4=;domain=.digid.nl;INJECTIE
```

```
; HttpOnly; secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Een overzicht van deze bevindingen.
Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.
Er zijn geen nieuwe bevindingen in deze categorie.

3.9.1 Information disclosure - Inloggegevens

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6		Midden	Zeer Laag	Hoog

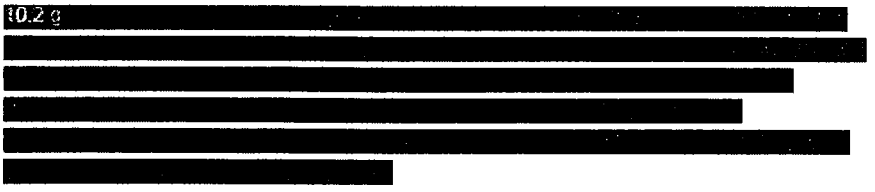
Betreffende hosts
digidbeheer-a4.digid.nl

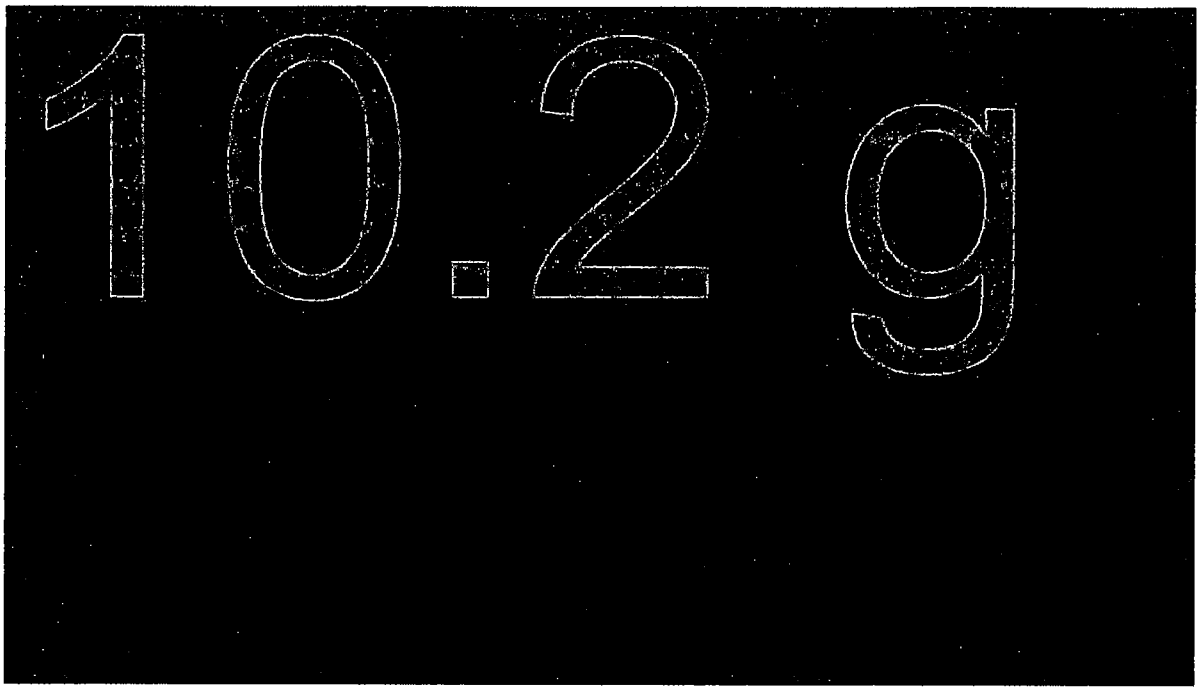
Omschrijving
De applicatie of het systeem lekt informatie over inloggegevens. Deze informatie kan bijvoorbeeld in HTTP-headers of foutmeldingen worden getoond.

Bedreiging
De gelekte informatie kan door een aanvaller worden gebruikt om direct in te loggen op een applicatie of service of om bestaande gebruikers te kunnen enumereren.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Zorg dat foutmeldingen zonder gebruikte inloggegevens getoond worden.

Details for Servers





3.9.2 SSL/TLS downgrade

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7	5.6.3	Zeer Laag	Zeer Laag	Zeer Laag

Omschrijving
De applicatie maakt gebruik van een SSL/TLS-tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.
"openssl s_client -connect host:443 -state -fallback_scsv -tls1_1"

Bedreiging
Als een aanvaller kan optreden als "man in the middle" kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS-tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 11.0.20). Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details for Servers
Voorbeeld voor a4.digid.nl:

```
root@not-a-hacker:~# sslscan a4.digid.nl
Version: 1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 144.43.243.160

Testing SSL server a4.digid.nl on port 443 using SNI name a4.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
[...]
```

4 PAP-eisen

Hieronder wordt van de eisen uit het document aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

ID	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Bevinding 6: Information disclosure - Inloggegevens		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
Bevinding 1, 2, 3, 4, 5: Security headers, reflectie in response header, CSRF		
ACC2.2.3	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Geen bevindingen		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en toleranties Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.	DNSSEC
Geen bevindingen		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is	Ingetrokken certificaten
Geen bevindingen		

5 Bijlagen

5.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD R5.12

Kenmerk: 2019DD5.12

Datum	16-08-2019
Status	Concept
Versie	0.2

Rubricering	derubricering
Vaststeller	10.2e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**2019DD5.12**
Versienummer	0.2
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
15-08-2019	0.1	Sogeti	Initiële versie
16-08-2019	0.2	Sogeti	Interne review

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

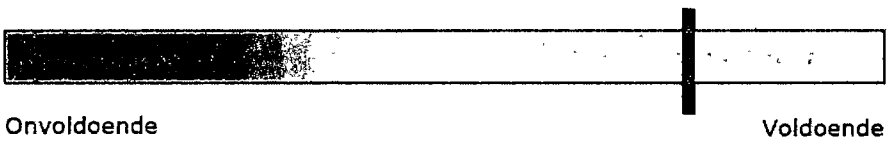
Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest betrof de aanstaande release 5.12 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Het verzoek was om een "generieke" greybox security test uit te voeren op de gehele DigiD-applicatie. Hierbij waren geen specifieke punten doorgegeven waar extra aandacht naar uit moet gaan gedurende deze security test.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.12 zoals getest op de A4-omgeving, voldoende is. Er zijn geen nieuwe bevindingen gedaan maar er zijn wel verschillende bevindingen onopgelost gebleven sinds de vorige test.



Onvoldoende Voldoende

Belangrijkste bevindingen ter verbetering:

A. De applicatie toont nog steeds wachtwoorden in de beheerinterface. Dit zorgt ervoor dat iemand die op het scherm meekijkt die wachtwoorden in handen kan krijgen. Zie bevinding 5 (Mantis 5.9.4).

   Aanbeveling: Toon bij voorkeur nooit wachtwoorden in een applicatie. Indien het echt noodzakelijk is voor de gebruiker om wachtwoorden in te zien, toon ze dan eerst gemaskeerd. Maak het wachtwoord pas zichtbaar als een gebruiker daar expliciet opdracht toe geeft.

B. Het is nog steeds mogelijk om een gebruiker uit te loggen, bijvoorbeeld als die gebruiker een kwaadaardige website open heeft staan. Hierdoor is het mogelijk, zolang die kwaadaardige pagina open staat, DigiD onbruikbaar te maken voor de gebruiker. Zie bevinding 3 (Mantis 5.9.3).

   Aanbeveling: Verifieer altijd voor alle acties die worden uitgevoerd of ze van de eigen site afkomstig zijn, door een unieke token mee te sturen.

C. In sommige gevallen wordt niet optimaal gebruikgemaakt van de beschikbare beveiligingsmechanismen. Zie bevinding 1 (Mantis 5.7.3) en 2 (Mantis 5.7.4).

   Aanbeveling: pas de beveiligingsmechanismen alsnog toe.

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

DigiD Release 5.12 betreft een release waarvan, op basis van een risicoanalyse uitgevoerd door Logius, is geconcludeerd dat de bijbehorende wijzigingen en aanvullingen op het systeem niet kritiek of relevant zijn vanuit een security perspectief. Het verzoek vanuit Logius was dan ook om een "generieke" greybox security test uit te voeren op de gehele DigiD-applicatie. Hierbij waren geen specifieke punten doorgegeven waar extra aandacht naar uit moet gaan gedurende deze security test.

Wel heeft Logius aangegeven een aantal bestaande bevindingen te hebben opgelost. Deze zijn gehertest tijdens deze security test op DigiD release 5.12.

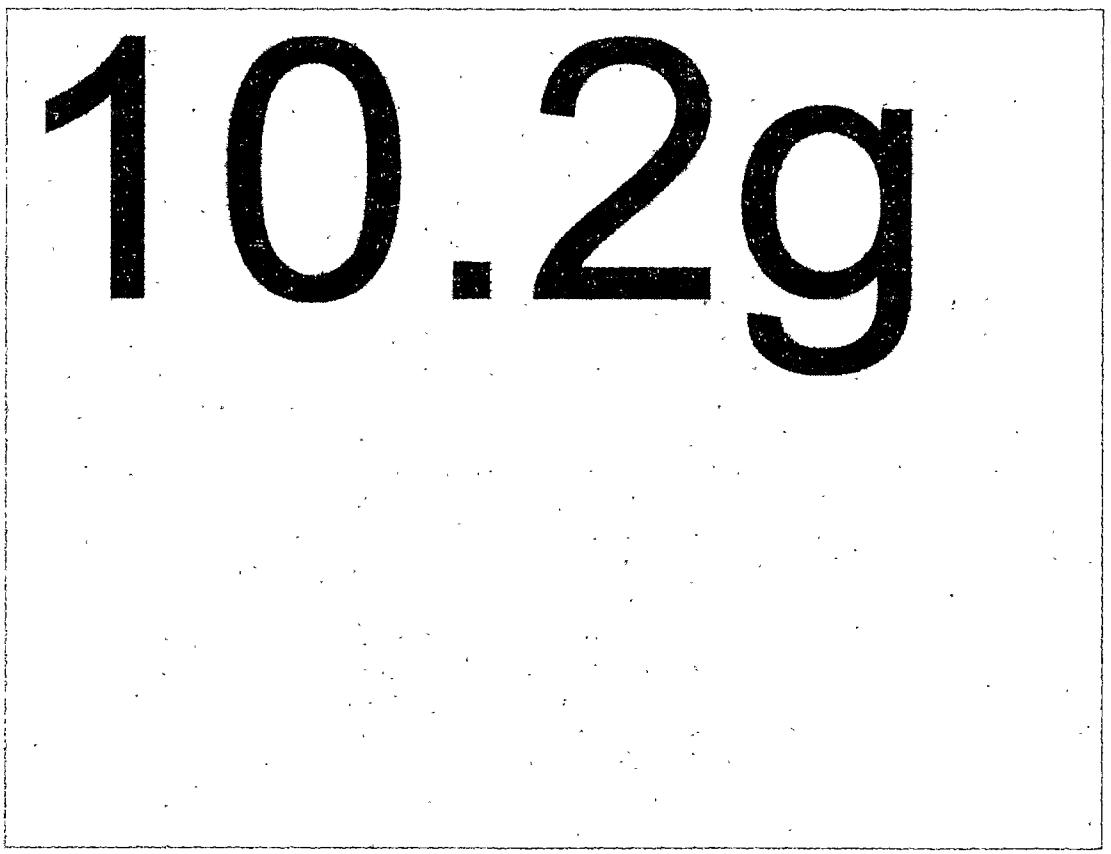
De scope van deze securitytest was de DigiD-applicatie, gezien vanaf een extern oogpunt.

In scope:

- Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
- Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
- Het verkeer tussen systemen buiten Kern (RDA-server, Status Controller, eID server) en DigiD kern voor zover zichtbaar.

Onderstaande schematische weergave geeft een visuele representatie van wat wel en wat niet getest werd binnen de scope van deze securitytest[1]:

Onderdeel	Omranding / vulling	Omschrijving
Functioneel	Oranje / grijs	Binnen scope (voor zover extern benaderbaar)
DigiD Hoog (nieuw)	Oranje / geel	Binnen scope (voor zover extern benaderbaar)
DigiD Kern	Paars	Binnen scope (voor zover extern benaderbaar)
DigiD-Hoog/Substantieel/App	Groen	Alleen functioneel en berichtenverkeer
Infrastructuur	Blauw	Buiten scope, valt niet extern te testen
Certificaten (nieuw)	Geen / geel	Buiten scope, valt niet extern te testen
DigiD Extern	Geen / paars	Buiten scope, valt niet extern te testen



[1] *NB de scope van de securitytest is dus niet gelijk aan de scope van de release*

In bovenstaande afbeelding zijn ook interacties en koppelvlakken tussen de verschillen actoren weergegevens. In de tabel hieronder is weergegeven op basis van scope bepaling of deze binnen de test vielen:

Nr	Aanvraag vanuit DigiD naar RDW	Zender	Ontvanger	
1	Opvragen DigiD Hoog Middel	DigiD	RDW	Binnen scope
2	Status wijzigingsverzoek DigiD Hoog middel	DigiD	RDW	Binnen scope
3	Heraanvragen PIN/PUK mailer	DigiD	RDW	Binnen scope
20	Aanvragen AT certificaat	DigiD	RDW	Binnen scope
	Aanvragen vanuit RDW			
4	Status wijzigingen door MU	RDW	DigiD	Buiten scope, valt niet extern te testen
5	Levering risicogebieden	DigiD	RDW	Binnen scope
6	Opvragen PP	RDW	BSNk PP	Buiten scope, valt niet extern te testen
8	Doorgeven statuswijziging IR	RDW	BSNk IR	Buiten scope, valt niet extern te testen
	Het koppelvlakken			
7	Opvragen versleuteld Pseudoniem	DigiD	BSNk PP	Binnen scope
9	Opvragen sleutelmateriaal HSM	HSM	BSNk SB	Buiten scope, valt niet extern te testen
11	Opvragen adresgegevens	Beheer	BRP	Binnen scope
12	Opvragen persoongegevens	Beheer	BRP	Binnen scope
13	Print en verzend opdracht	DS	BS	Buiten scope, valt niet extern te testen
14	Authenticatie aanvraag	AK	MK	Buiten scope, valt niet extern te testen
18	Opvragen status	DigiD	SC	Binnen scope
	PCA			
16	PCA eIDAS protocol	eIDsrv	eIDclt	Binnen scope
17	Registeren aanvraag, uitreiking, intrekking	AS	MU	Buiten scope, valt niet extern te testen
19	Controleren WID (BAC/BAP)	DigiD	WID	Binnen scope

Tijdens de securitytest is ook gelet op eventuele regressie dan wel ongeautoriseerde of onbedoelde veranderingen.

Tijdens eerdere tests op DigiD is een aantal bevindingen gedaan welke in release 5.12 zijn opgelost en daarom specifiek opnieuw moesten worden getest of waarvan bekend is dat het risico is geaccepteerd. Deze bevindingen zijn:

Opgeloste bevindingen
5.9.6 Anti-Cross-Site-Scripting-header ontbreekt
5.9.5 Dubbele Headers (X-Frame-Options)
5.9.4 Information Disclosure - Credentials
5.9.3 Cross-Site Request Forgery
5.9.1 Content-Security-Policy-header ontbreekt
7.1.0 Lekken van gevoelige informatie

IB-bevindingen die geaccepteerd zijn
5.4.3 Gelijktijdige sessies
5.5.3 Wachtwoordsterkte onvoldoende
5.5.5 BEAST (Browser Exploit Against SSL/TLS)
5.5.1 Content-Security-Policy header implementatiefout
5.6.1 Cookie-domein te breed
5.6.2 Onvoldoende invoervalidatie Daring Fireball markup

IB-bevindingen die bekend zijn en niet opgelost
5.7.4 X-Content-Type-Options header ontbreekt
5.7.6 Reflectie in header
5.6.3 SSL/TLS downgrade

1.2 Aanpak

De test is geheel conform het Security Testplan uitgevoerd. Zie 'PVA securitytest - DigiD R5.12.pdf', hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'.
Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Grey box test.

derubricering

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Nieuwe bevindingen
Er zijn gedurende deze test geen nieuwe bevindingen gedaan.

Hertest bevindingen
Onderstaand overzicht betreft opnieuw geteste bevindingen die nog steeds bestaan.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Client-side Controls	0	0	1	1	0	**2**
Servers	0	0	1	0	2	**3**
Invoerafhandeling	0	0	0	2	0	**2**
Totaal	**0**	**0**	**2**	**3**	**2**	**7**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	

[2] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Buiten scope voor deze test

B.05 Contractmanagement

Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Oordeel

Buiten scope voor deze test

B.06 ICT-landschap

Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Oordeel

Buiten scope voor deze test

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel

Geen bevindingen

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope voor deze test

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope voor deze test

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Bevinding: 3, 1

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Bevinding: 1, 2, 4

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Bevinding: 7

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

Bevinding: 5, 6

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel	

Geen bevindingen

U/WA.08	**Webapplicatiesessie**

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel	

Bevinding:

U/WA.09	**Webapplicatiearchitectuur**

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel	

Buiten scope voor deze test

U/PW.01	**Operationeel beleid voor platformen en webservers**

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel	

Buiten scope voor deze test

U/PW.02	**Webprotocollen**

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel	

Geen bevindingen

U/PW.03	**Webserver**

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel	

Geen bevindingen

U/PW.04	**Isolatie van processen/bestanden**

Beperk de impact bij misbruik van processen.

Oordeel	

Buiten scope voor deze test

U/PW.05	**Toegang tot beheermechanismen**

Voorkomen van misbruik van beheervoorzieningen.

Oordeel	

Geen bevindingen

U/PW.06	**Platform-netwerkkoppeling**

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel	

Geen bevindingen

U/PW.07	**Hardening van platformen**

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel	

Buiten scope voor deze test

U/PW.08	**Platform- en webserverarchitectuur**

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel	

Buiten scope voor deze test

U/NW.01	**Operationeel beleid voor netwerken**

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel	

Buiten scope voor deze test

U/NW.02	**Beschikbaarheid van netwerken**

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel	
Buiten scope voor deze test	

U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Buiten scope voor deze test	

U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Buiten scope voor deze test	

U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Buiten scope voor deze test	

U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Geen bevindingen	

U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Buiten scope voor deze test	

U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Buiten scope voor deze test	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Buiten scope voor deze test	

C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Buiten scope voor deze test	

C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Buiten scope voor deze test	

C.04	**Penetratietestproces**

derubricering

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).
Oordeel
Buiten scope voor deze test
C.05 Technische controlefunctie
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.
Oordeel
Buiten scope voor deze test
C.06 Logging
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.
Oordeel
Buiten scope voor deze test
C.07 Monitoring
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.
Oordeel
Buiten scope voor deze test
C.08 Wijzigingenbeheer
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.
Oordeel
Buiten scope voor deze test
C.09 Patchmanagement
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.
Oordeel
Buiten scope voor deze test
C.10 Beschikbaarheidbeheer
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.
Oordeel
Buiten scope voor deze test
C.11 Configuratiebeheer
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.
Oordeel
Buiten scope voor deze test

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Anti-Cross-Site-Scripting-header ontbreekt

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	5.7.3	Midden	Laag	Hoog

Betreffende hosts
was-a4.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Wanneer de cross-site-scripting bescherming niet is ingeschakeld, wordt het voor aanvallers makkelijker om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
"X-XSS-Protection: 1"
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging: 'X-XSS-Protection: 1; mode=block'
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Details for ClientSideControls
Eén van de hosts uit de scope stuurt de header niet naar de browser.

Voorbeeld responseheaders was-a4.digid.nl:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 01 Apr 2019 15:38:53 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Content-Type: image/svg+xml
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 12 Aug 2019 12:28:56 GMT
Expires: Tue, 11 Aug 2020 12:28:56 GMT
Age: 0
Content-Length: 21493
```

3.1.2 *X-Content-Type-Options header ontbreekt*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	5.7.4	Laag	Laag	Laag

Betreffende hosts
was-a4.digid.nl

Omschrijving
De anti-MIME-sniffing header X-Content-Type-opties is niet ingesteld op 'nosniff'.

Bedreiging
Door het ontbreken van deze header wordt in oudere versies van Internet Explorer en Chrome MIME-sniffing toegepast op de response-body. Dit kan de response-body in een ander formaat weergeven dan het opgegeven content-type. Huidige (sinds begin 2014) versies van Firefox maken altijd gebruik van het opgegeven content-type (als er een is ingesteld).

Aanbeveling
Zorg ervoor dat de webserver de Content-Type header goed meestuurt, en dat de header X-Content-Type-Options is ingesteld op 'nosniff' voor alle webpagina's.

Details for ClientSideControls
Eén van de hosts uit de scope stuurt de header niet naar de browser.

Voorbeeld response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 01 Apr 2019 15:38:53 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Content-Type: image/svg+xml
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 12 Aug 2019 12:28:56 GMT
Expires: Tue, 11 Aug 2020 12:28:56 GMT
Age: 0
Content-Length: 21493

<?xml version="1.0" encoding="UTF-8"?>
<svg width="44px" height="77px" viewBox="0 0 44 77" version="1.1"
xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink">
[… snip …]
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 Cross-site request forgery

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3	5.9.3	Laag	Zeer Laag	Laag

Betreffende hosts
a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl

Omschrijving
Bij het verwerken van ingevulde formulieren zou gecontroleerd moeten worden of het verzoek van de eigen site afkomstig is.

Bedreiging
Wanneer bij het verwerken van ingevulde formulieren niet wordt gecontroleerd of het verzoek van de eigen site afkomstig is, is het mogelijk om POST acties vanaf een andere site uit te voeren. Indien er gebruik gemaakt wordt van authenticatie, dan wordt deze actie uitgevoerd in dezelfde browser als waarin een gebruiker op de legitieme website is ingelogd.

Aanbeveling
CSRF kan voorkomen worden door het gebruik van een niet te voorspellen token in een formulier of URL van elke HTTP request. Zo'n token moet op z'n minst uniek zijn per verzoek. OWASP's CSRF Guard: https://www.owasp.org/index.php/CSRFGuard kan gebruikt worden om automatisch tokens toe te voegen in Java EE, .NET, of PHP-applicaties. OWASP's ESAPI bevat token generators en validators die door ontwikkelaars gebruikt kunnen worden om transacties te beveiligen.

Details for Invoerafhandeling

Het is nog steeds mogelijk een gebruiker uit te loggen via een CSRF-aanval. Hierdoor is het mogelijk om de website ontoegankelijk te maken wanneer een gebruiker een malafide plugin of tabblad heeft open staan. Door de interactie die benodigd is voor de installatie van bijvoorbeeld een plugin door een gebruiker, is de kans op zeer laag ingeschaald.

Proof-of-Concept CSRF-uitlogknop:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://a4.digid.nl/uitloggen">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3.7.2 *Reflectie in header*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4	5.7.6	Laag	Laag	Laag

Betreffende hosts
a4.digid.nl
cis-a4.digid.nl
digidbeheer-a4.digid.nl
eid-a4.digid.nl
mijn.a4.digid.nl
rda-a4.digid.nl
was-a4.digid.nl

Omschrijving
Gegevens die door de server worden gestuurd naar de gebruiker bevatten veelal instructies voor browsers in de vorm van headers, naast natuurlijk de uiteindelijke content van de pagina. Meestal kunnen de meegestuurde headers niet worden beïnvloed of aangepast door de gebruiker. In dit geval is dit wel mogelijk.

Bedreiging
Door het wijzigen van bepaalde invoer die naar de server wordt gestuurd, kan een aanvaller bijvoorbeeld de inhoud van een teruggestuurde header controleren. De invoer wordt direct gereflecteerd naar de gebruiker in de uitvoer.

Aanbeveling
Filter alle mogelijke invoer van de gebruiker en zorg dat er geen headerwaardes direct gewijzigd kunnen worden door invoer in een web request te veranderen.

Details for Invoerafhandeling
De waarde van het cookie *_persist* in de response headers van verschillende hosts is te beïnvloeden door in de request de *Host*-header aan te passen.

Request:

```
GET / HTTP/1.1
Host: a4.digid.nl;XYZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Wed, 14 Aug 2019 11:24:07 GMT
Content-Length: 347
Connection: close
Content-Type: text/html; charset=iso-8859-1
Set-Cookie: _persist='Jpb0[... snip ...]Nk=;domain=.digid.nl;XYZ;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
[... snip ...]
```

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

derubricering

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 Information disclosure - Inloggegevens

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5	5.9.4	Midden	Zeer Laag	Hoog

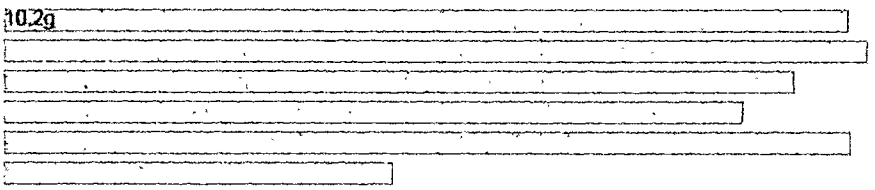
Betreffende hosts
digidbeheer-a4.digid.nl

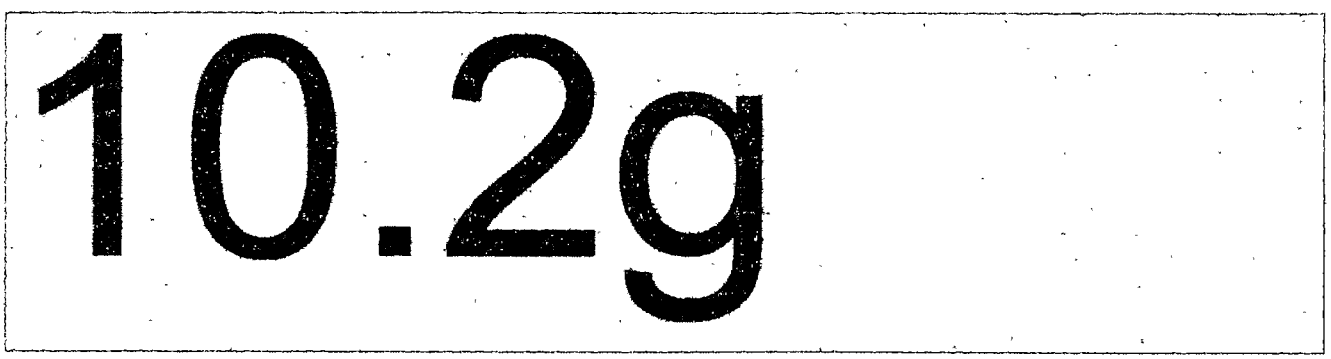
Omschrijving
De applicatie of het systeem lekt informatie over inloggegevens. Deze informatie kan bijvoorbeeld in HTTP-headers of foutmeldingen worden getoond.

Bedreiging
De gelekte informatie kan door een aanvaller worden gebruikt om direct in te loggen op een applicatie of service of om bestaande gebruikers te kunnen enumereren.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Zorg dat foutmeldingen zonder gebruikte inloggegevens getoond worden.

Details for Servers





derubricering

3.9.2 *Information disclosure*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6	7.1.0	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
*.digid.nl

Omschrijving
Het systeem geeft informatie vrij over de (interne) werking of logica van het systeem zelf, de onderliggende infrastructuur, privacygevoelige data of informatie gerelateerd aan toegangsmanagement.

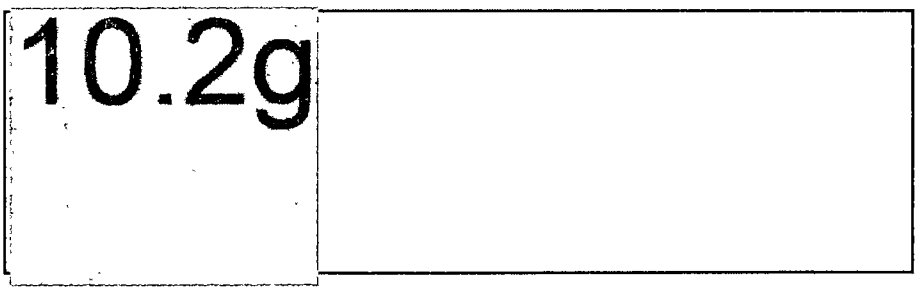
Bedreiging
De informatie kan een aanvaller inzicht verlenen dat als een springplank kan dienen voor aanvallen op het systeem: gelekte sessietokens kunnen het toegangsbeheer ondermijnen, versie-informatie ontsluit het patchlevel, stacktraces geven inzicht in interne logica en gebruikte technologie, open directories over het onderliggende besturingssysteem, hostnames en IP-adressen geven inzicht in de netwerkimplementatie, etc.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie en zorg dat foutmeldingen aan eindgebruikers zonder systeeminformatie getoond worden.

Details for Servers
Tijdens eerdere tests op DigiD is een aantal bevindingen gedaan welke in release 5.12 aangemeld zijn als opgelost, echter is het document nog steeds beschikbaar via onderstaande URL

10.2g

Deze pagina bevat een lijst met subdomeinen op digid.nl:



De volledige lijst is opgenomen in bijlage 5.2.

3.9.3 SSL/TLS downgrade

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7	5.6.3	Zeer Laag	Zeer Laag	Zeer Laag

Omschrijving
De applicatie maakt gebruik van een SSL/TLS-tunnel, bijvoorbeeld door de toepassing van het https-protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.
"openssl s_client -connect host:443 -state -fallback_scsv -tls1_1"

Bedreiging
Als een aanvaller kan optreden als "man in the middle" kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS-tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS-verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 11.0.20). Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details for Servers
Voorbeeld voor a4.digid.nl:

```
cyber:~$ sslscan a4.digid.nl
Version: 1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 144.43.243.160

Testing SSL server a4.digid.nl on port 443 using SNI name a4.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
```

4 PAP-eisen

Hieronder wordt van de PAP-eisen aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

ID	Omschrijving	Criterium
ACC2.1.2	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.	Lekken van informatie
Bevinding 5: Information disclosure - Inloggegevens		
ACC2.2.1	Het systeem moet bestand zijn tegen veelvoorkomende aanvallen zoals benoemd door OWASP in de category Attack. (https://www.owasp.org/index.php/Category:Attack)	Aanvallen
Bevinding 1: CSRF		
ACC2.2.3	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)	Zwakheden
Bevinding 2, 3, 4: Security headers, reflectie in response header		
ACC2.3.1	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en toleranties Als privacy gevoelige gegevens	Persoonsgegevens
Geen bevindingen.		
ACC2.5.1	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC-standaard.	DNSSEC
Geen bevindingen.		
ACC2.5.2	Cookies zijn veilig, betekenisloos, uniek en tijdelijk	Cookies
Geen bevindingen.		
ACC2.5.4	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is	Ingetrokken certificaten
Geen bevindingen.		

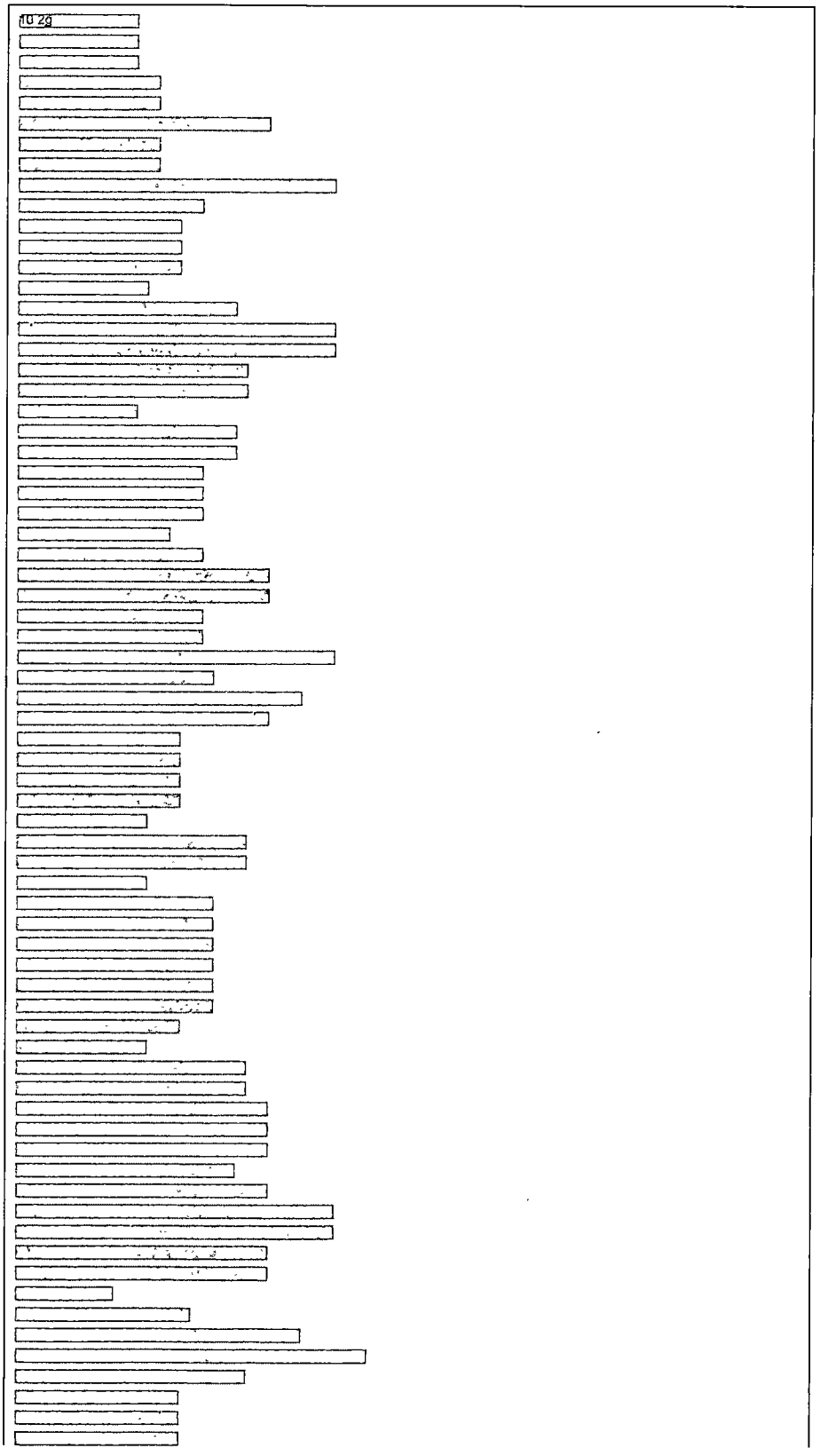
5 Bijlagen

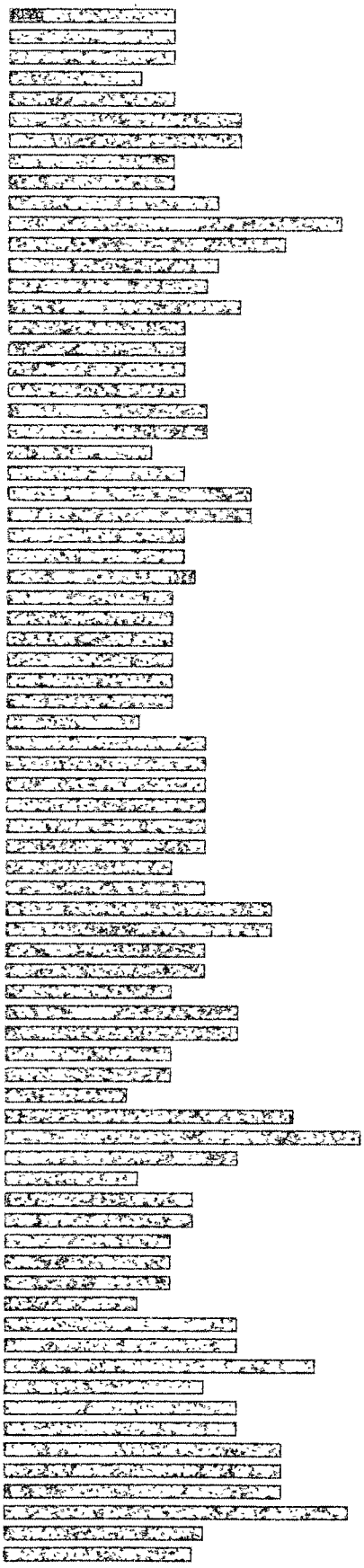
5.1 Risicoclassificatie

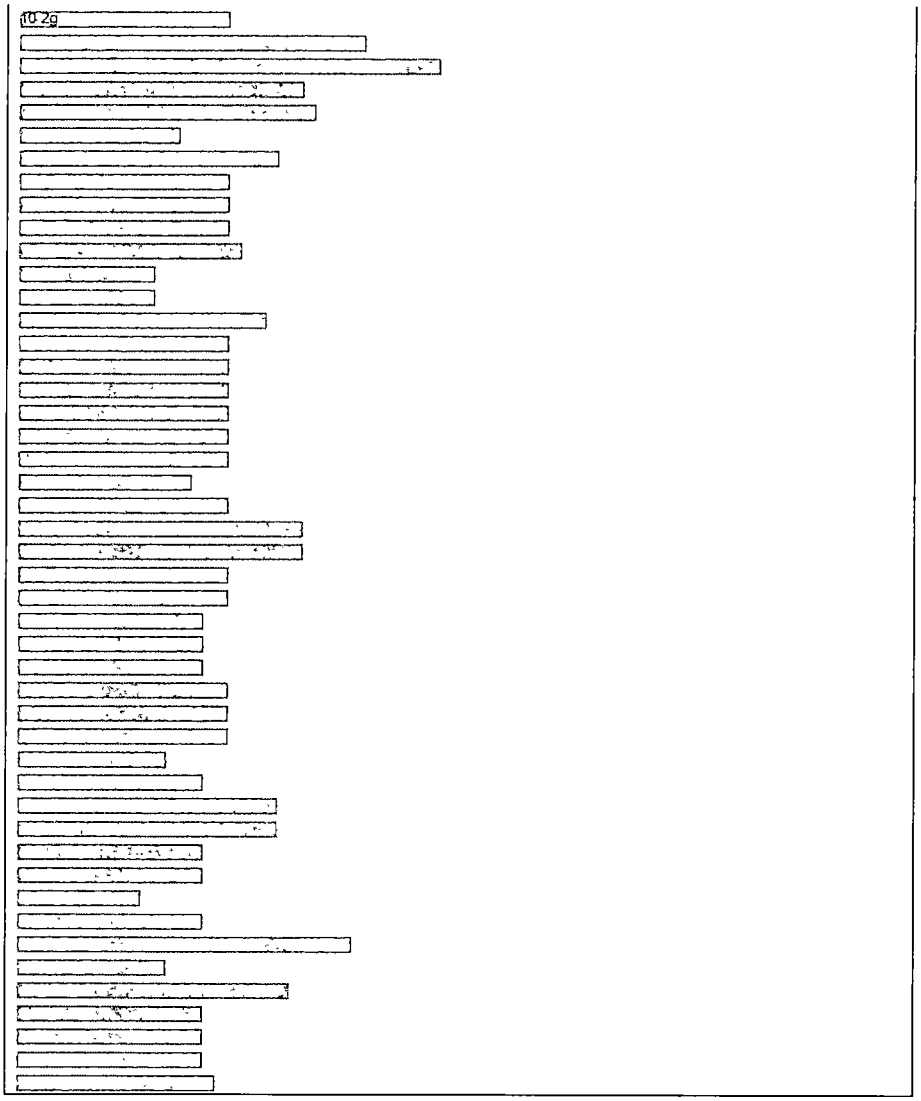
Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

5.2 Lijst subdomeinen

Hieronder is de volledige lijst subdomeinen uit bevinding 6 opgenomen.






10.2g

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
Securitytest DigiD R5.13

Kenmerk: 42100000

Datum	28-11-2019
Status	Definitieve versie
Versie	1.0

Rubricering	derubricering
Vaststeller	10.2e
Functie	Ketenbeheerder voorziening

Colofon

Kenmerk	**42100000**
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
22-11-2019	0.1	Sogeti	Initiële versie
22-11-2019	0.2	Sogeti	Interne review
26-11-2019	0.3	Sogeti	Aanvullingen Logius
28-11-2019	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest betrof de aanstaande release 5.13 van DigiD. De test is bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook zijn er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Conclusies en aanbevelingen

- De config stub is kwetsbaar voor een aanval op de onderliggende database. Het is mogelijk om informatie uit de database buit te maken en de database te manipuleren. Zie bevinding #1.
  Aanbeveling: deze kwetsbaarheid is ontstaan doordat de input van de gebruiker wordt geïnterpreteerd als onderdeel van de code. Het is aanbevolen om de gebruikersinput apart te versturen door middel van zogenaamde prepared statements.
- Het is mogelijk om bezoekers door te sturen naar externe domeinen. Dit kan gebruikt worden bij phishing aanvallen. Zie bevindingen #5 en #6.
  Aanbeveling: bepaalde headers zorgen voor dit probleem. Negeer deze headers bij verzoeken richting de server.
- De server geeft informatie vrij over de gebruikte software en onderliggende logica. Zie bevinding #2 en #3.
  Aanbeveling: toon alleen informatie die strict noodzakelijk is voor het functioneren van de applicaties. Door het verminderen van de vrijgave van informatie over de gebruikte software en logica, wordt de kans op een succesvolle aanval kleiner.

Aanvullingen Logius

Vanuit Logius zijn er aanvullingen op het rapport aangaande de SQL injectie bevinding. Deze aanvullingen zijn hieronder beschreven.

De door een gebruiker opgegeven invoer wordt gebruikt in of als commando's (queries) die door de achterliggende SQL database rechtstreeks uitgevoerd worden. Bevinding is gedaan op de host 'config-a4.digid.nl'.

Deze constatering is in eerdere security testen ook gedaan en het klopt dat deze configuratie informatie via de interne Logius infrastructuur is te benaderen. Logius heeft hier nader onderzoek naar gedaan en de voors- en tegens- tegenover elkaar afgewogen. Daarbij is het volgende meegenomen:
1) Het configuratie scherm is alleen via de interne Logius infrastructuur te benaderen. Wel zijn de configuratie gegevens voor de A omgeving zichtbaar voor Logius medewerkers (die weten hoe te benaderen)
2) Het configuratie scherm is alleen beschikbaar voor de Acceptatie omgeving. **En dus niet voor Productie!**
3) De A omgeving bevat geen burger gegevens;

4) Het afschermen van de pagina heeft andere nadelige gevolgen voor het intern kunnen testen en is derhalve als ongewenst aangemerkt;
5) Als mitigerende maatregel worden steeds voor het starten van een test de configuratie gegevens gereset naar hun default waarden.

1 Inleiding

1.1 Opdrachtformulering

De opdracht is geheel conform het Security Testplan uitgevoerd.
Aan de securitytest is als volgt invulling gegeven:

- Volledig geautomatiseerde scans zijn uitgevoerd op de applicatie, met behulp van tooling.
- De resultaten van de test zijn handmatig geverifieerd.
- Er is een handmatige vulnerability assessment uitgevoerd op de systemen en de applicatie.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. Zie Security Testplan DigiD R5.13 v1.2.pdf, hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'.
Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Grey box test.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Servers	0	0	0	2	3	5
Invoerafhandeling	0	0	1	0	0	1
Totaal	**0**	**0**	1	2	3	6

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Buiten scope	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope	

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

derubricering

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel

Geen bevindingen.

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

SQL injectie is mogelijk, wat tenminste de beschikbaarheid kan aantasten.

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Geen bevindingen.

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Geen bevindingen.

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

De server geeft informatie over de gebruikte software vrij + de API documentatie is te vinden op de server.

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen.

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Geen bevindingen.

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Geen bevindingen.

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope

derubricering

U/PW.02 Webprotocollen
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.
Oordeel
Er is SQL injectie mogelijk en bezoekers kunnen d.m.v. header injecties worden doorgestuurd naar externe hosts. Tevens geeft de gevonden API documentatie inzage in de logica van de webapplicatie.
U/PW.03 Webserver
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.
Oordeel
De sever geeft informatie vrij over de gebruikte sofware. Ook is de API documentatie inzichtelijk, waardoor inzicht wordt gegeven in de opbouw van de beveiliging (authenticatie proces is in de API beschreven).
U/PW.04 Isolatie van processen/bestanden
Beperk de impact bij misbruik van processen.
Oordeel
Buiten scope
U/PW.05 Toegang tot beheermechanismen
Voorkomen van misbruik van beheervoorzieningen.
Oordeel
De config stub is alleen vanaf het interne netwerk bereikbaar.
U/PW.06 Platform-netwerkkoppeling
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.
Oordeel
Geen bevinding.
U/PW.07 Hardening van platformen
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Oordeel
Buiten scope
U/PW.08 Platform- en webserverarchitectuur
Een platform bieden dat een betrouwbare verwerking garandeert.
Oordeel
Buiten scope
U/NW.01 Operationeel beleid voor netwerken
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.
Oordeel
Buiten scope
U/NW.02 Beschikbaarheid van netwerken
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.
Oordeel
Buiten scope
U/NW.03 Netwerkzonering
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.
Oordeel
Buiten scope
U/NW.04 Protectie- en detectiefunctie
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.
Oordeel

Buiten scope

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buiten scope.

U/NW.06 Hardening van netwerken

Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/NW.07 Netwerktoegang tot webapplicatie

Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Oordeel

Buiten scope

U/NW.08 Netwerkarchitectuur

Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope

Beheersingsdomein

C.01 Servicemanagementbeleid

Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Oordeel

Buiten scope

C.02 Compliancemanagement

Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Oordeel

Buiten scope

C.03 Vulnerability-assessments

Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Oordeel

Buiten scope

C.04 Penetratietestproces

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Oordeel

Buiten scope

C.05 Technische controlefunctie

Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Oordeel

Buiten scope

C.06 Logging

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Oordeel
Buiten scope
C.07 Monitoring
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.
Oordeel
Buiten scope
C.08 Wijzigingenbeheer
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.
Oordeel
Buiten scope
C.09 Patchmanagement
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.
Oordeel
Geen bevindingen.
C.10 Beschikbaarheidbeheer
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.
Oordeel
Buiten scope
C.11 Configuratiebeheer
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.
Oordeel
Buiten scope

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Er zijn geen nieuwe bevindingen in deze categorie.

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 SQL injection

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1		Midden	Laag	Hoog

Betreffende hosts
config-a4.digid.nl

Omschrijving
De door een gebruiker opgegeven invoer wordt gebruikt in of als commando's (queries) die door de achterliggende SQL database rechtstreeks uitgevoerd worden.

Bedreiging
Door de invoer uit te breiden met, of aan te passen naar, database commando's kan een gebruiker de database manipuleren zonder dat dit de bedoeling van de ontwikkelaar is. Dit kan ertoe leiden dat ongewenst informatie wordt vrijgegeven, dan wel gegevens worden gemanipuleerd of verwijderd

Aanbeveling
Vertrouw invoer van gebruikers niet wanneer deze direct als invoer op een ander systeem gebruikt kan worden.
Om SQL injection te voorkomen is het aan te raden de vraagstelling van de applicatie aan de database in twee delen aan te leveren. Maak gebruik van geparameteriseerde queries met placeholders. Op deze manier worden logica en data gescheiden en zal de applicatie deze twee niet met elkaar verwarren en per ongeluk informatie van de gebruiker als commando uitvoeren.

Zie ook
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet.
Daarnaast is het aan te raden aangeleverde invoer te valideren op het verwachte type, zoals bijvoorbeeld tekst en datum, alsook op lengte en formaat zoals bij een postcode of een telefoonnummer. Dit is een mitigerende maatregel die als aanvullend voordeel heeft dat ook andere problemen zoals bijvoorbeeld type mismatches worden voorkomen.

Details
De webapplicatie op de host communiceert met de [redacted] database door het uitvoeren van zogeheten query's. Input van gebruikers wat in database query's wordt verwerkt, dient altijd gevalideerd te worden om te voorkomen dat SQL injectie mogelijk is. Tijdens de securitytest op de host is gebleken dat de host kwetsbaar is voor SQL injectie. Dit zou betekenen dat aanvallers de complete database inhoud buit kunnen maken + mogelijk directe toegang tot (alle) bestanden op de host kunnen krijgen. Er is niet met zekerheid te stellen dat de onderstaande request de daadwerkelijke request is die de SQL error heeft veroorzaakt. De ongefilterde data is namelijk in de database opgeslagen, waardoor de webapplicatie crasht. Deze bevinding is niet aanwezig in de productie omgeving.

Request:

```
POST /jobs HTTP/1.1
Host: config-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv.70.0)
Gecko/20100101 Firefox/70.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 210
Origin: https.//config-a4.digid.nl
Connection: close
Referer: https://config-a4.digid.nl/jobs
Cookie: [.. truncated ..]
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=XdugdpT1PZoocGWRheg3Ai4NCI1C2zB45sWj
QQj0%2BxTRDVsUBCRMgxD9FPrGWe1OTGeJpfoaLKY1vC3j0CLAJg%3D%3D&job=CreateA
ccountsJob&type=midden_actief&from=test&to=test'&commit=Create+account
s
```

Response:

```
HTTP/1.1 200 OK
Date: Wed, 20 Nov 2019 10:15:19 GMT
[redacted]

[.. truncated ..]
```

In de request is de volgende input te zien:

```
test'&commit=Create+accounts
```

Vermoedelijk is de quote (') de veroorzaker van de SQL error.

De technische scoring van deze bevinding is ingeschat op:
- Kans: laag, omdat de omgeving alleen vanaf het interne netwerk te benaderen is.
- Impact: hoog, omdat de omgeving te verstoren is, (gevoelige) informatie kan worden buitgemaakt en wellicht toegang tot de server te verkrijgen is
- Risico: midden, want de kans is laag, het betreft een hoge impact en het is slechts op de acceptatie server aanwezig die alleen vanaf het interne netwerk bereikbaar is

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 X-Forwarded-For-header aanval

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
a4.digid.nl

Omschrijving
Een aanvaller kan een X-Forwarded-For-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de X-Forwarded-For-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de X-Forwarded-For-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende X-Forwarded-For header verstuurd.

Details
De X-Forwarded-For header wordt vaak gebruikt als een request naar de server via een proxy verloopt. De aanwezigheid van een malafide X-Forwarded-For header is niet geblokkeerd vanuit de server. Indien een bepaalde waarde aan de X-Forwarded-For header wordt meegegeven, komt dit terug op de webpagina. Zie de onderstaande request en

response, waarin de X-Forwarded-For header wordt meegegeven met als waarde "Sogeti.nl".

Request:

```
POST /activeringscode?k0svdsvnid=1 HTTP/1.1
Host: a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0)
Gecko/20100101 Firefox/70.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 206
Origin: https://a4.digid.nl
Connection: close
Referer: https://a4.digid.nl/activeringscode
Cookie: [.. truncated ..]
Upgrade-Insecure-Requests: 1
X-Forwarded-Host: sogeti.nl

[.. truncated ..]
```

Response:

```
HTTP/1.1 200 OK
[.. truncated ..]
<!-- Matomo -->
<script>
//<![CDATA[
  var _paq = _paq || [];
  /* tracker methods like "setCustomDimension" should be called before
"trackPageView" */
  _paq.push(['trackPageView']);
  _paq.push(['enableLinkTracking']);
  (function() {
    var u="//statistiek.mijn.overheid.nl/";
    _paq.push(['setTrackerUrl', u+'piwik.php']);
    _paq.push(['setSiteId', '12']);
    var d=document, g=d.createElement('script'),
s=d.getElementsByTagName('script')[0];
    g.type='text/javascript'; g.async=true; g.defer=true;
g.src='https://sogeti.nl/assets/piwik-
88b8824a5f55a9bb5be3b1e48b0fe9e314196870c10116491a478817ac781065.js';
s.parentNode.insertBefore(g,s);
  })();

//]]>
</script><!-- End Matomo Code -->
[.. truncated ..]
```

Normaliter probeert de browser het volgende javascript bestand in te laden:

```
https://a4.digid.nl/assets/piwik-
88b8824a5f55a9bb5be3b1e48b0fe9e314196870c10116491a478817ac781065.js
```

Wanneer de X-Forwarded-For header wordt meegegeven met als waarde "Sogeti.nl", probeert de browser het javascript bestand in te laden vanuit Sogeti.nl in plaats van a4.digid.

```
https://sogeti.nl/assets/piwik-
88b8824a5f55a9bb5be3b1e48b0fe9e314196870c10116491a478817ac781065.js
```

Aanvallers zijn normaliter door dit probleem in staat om externe javascript code op de webpagina in te laden. Dit kan kwaadaardige code zijn, waarbij bijvoorbeeld geprobeerd wordt om malafide software op de computer van een gebruiker te installeren. Echter, doordat de CSP-headers op a4.digid.nl correct zijn ingesteld, wordt een poging om externe javascript code in te laden door de host geblokkeerd. De CSP-headers

geven namelijk aan dat alleen zeer specifieke javascript code mag worden ingeladen, namelijk alleen code die van DigiD zelf afkomstig is. Een aanval door middel van X-Forwarded-For header injectie zou in dit geval dus niet slagen. Een andere manier waarop aanvallers dit probleem zouden kunnen misbruiken, is wanneer er caching problemen zijn aan de kant van de server. De server-side caching lijkt goed geconfigureerd te zijn.
Samengevat is het niet mogelijk de X-Forwarded-For header injectie met succes uit te buiten, aangezien de CSP headers in orde zijn en de server-side caching op orde is.

3.9.2 *Information disclosure – Versie-informatie*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3		Laag	Midden	Zeer Laag

Betreffende hosts
stubs-a4.digid.
app-a4.digid.nl

Omschrijving
Systemen geven vaak zelf onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een default instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details
De hosts geven informatie vrij over de gebruikte software inclusief versienummers. Kwaadwillenden kunnen deze informatie gebruiken in een (toekomstige) aanval. Zo kunnen kwaadwillende gebruikers wachten op een bepaald moment dat er een zero-day kwetsbaarheid voor de specifieke gebruikte software bekend wordt.
In de response op de volgende request is de gebruikte software inzichtelijk:

Request:

```
GET /app_stub/[object%20Event] HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0)
Gecko/20100101 Firefox/70.0
Accept: image/webp,*/*
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://stubs-a4.digid.nl/app_stub/old_app
Cookie: _[.. truncated ..]
```

Response:

```
HTTP/1.1 404 Not Found
Date: Tue, 19 Nov 2019 07:50:36 GMT
[illegible]
X-Permitted-Cross-Domain-Policies: none
[.. truncated ..]
```

Ook als de volgende URL wordt opgevraagd, is de versie informatie inzichtelijk:

```
https://app-a4.digid.nl/
```

Aanbevolen wordt om de vrijgave van informatie te beperken tot het absolute minimum, om aanvallers zodoende geen inzicht te geven in de gebruikte software en de kans op een succesvolle aanval te verkleinen.

3.9.3 *Information disclosure – API documentatie*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Laag	Zeer Laag	Midden

Betreffende hosts
eid-a4.digid.nl

Omschrijving
De server geeft informatie vrij over zowel de interne als externe versie van de API.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om gevoelige informatie uit de API op te vragen. Tevens biedt het een aanvaller informatie over de interne werking van een systeem.

Aanbeveling
Verwijder de API documentatie op de server, zodat aanvallers geen informatie krijgen over de interne werking van het systeem.

Details

```
[illegible]
```

Hier is te zien hoe zowel de externe als interne API er uit ziet. Hierdoor zien aanvallers welke API calls mogelijk zijn, hoe het authenticatie proces verloopt en wat de interne werking van het systeem is. Dit biedt kansen voor aanvallers om gericht te gaan zoeken naar kwetsbaarheden in de API.

Externe API:

```
https://eid-a4.digid.nl/v2/api-docs?group=extern
```

Interne API:

```
https://eid-a4.digid.nl/v2/api-docs?group=intern
```

Het is aanbevolen om 10.2g en bovengenoemde URL's niet publiekelijk beschikbaar te maken.

3.9.4 *X-Forwarded-Host-header aanval*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5		Zeer Laag	Zeer Laag	Laag

Betreffende hosts
balie-a4.digid.nl

Omschrijving
Een aanvaller kan een X-Forwarded-Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de X-Forwarded-Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de X-Forwarded-Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende X-Forwarded-Host header verstuurd.

Details
De host is kwetsbaar voor een X-Forwarded-Host header aanval. Hierbij wordt een X-Forwarded-Host header aan de request meegegeven. Het gevolg is dat een bezoeker vanuit de host direct naar de host wordt gestuurd die in de X-Forwarded-Host header is opgegeven. Een dergelijke aanval kan worden ingezet bij phishing campagnes, waarbij bezoekers naar een malafide inlogpagina worden gestuurd. Het doorsturen van de bezoeker is te zien in de onderstaande request en response.

Request:

```
POST /aanvraag?jhp0gg5k9u=1 HTTP/1.1
Host: balie-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0)
Gecko/20100101 Firefox/70.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 267
Origin: https://balie-a4.digid.nl
Connection: close
Referer: https://balie-a4.digid.nl/aanvraag/ophalen
Cookie: [.. truncated ..]
Upgrade-Insecure-Requests: 1
X-Forwarded-Host: sogeti.nl

utf8=%E2%9C%93&authenticity_token=mea%2BEC9DlvbaF9fY%2ByjRgSudxMZLpCuF
wWojRvjg7Yt5A8KU9rA0TKZPLR6MSACygvfeEyfKPzKGvvstL8DDSw%3D%3D&create_ve
```

```
rification_form%5Bcitizen_service_number%5D=111111111&create_verificat
ion_form%5Bfront_desk_code%5D=B11111111&commit=Volgende
```

Response:

```
HTTP/1.1 302 Found
Date: Thu, 21 Nov 2019 07:13:03 GMT
[.. truncated ..]

<html><body>You are being <a
href="https://sogeti.nl/saml/sp/eherkenning_authentication">redirected
</a>.</body></html>
```

Zoals te zien is in de laatste regel van de response, wordt de bezoeker doorgestuurd naar sogeti.nl

3.9.5 Host-header aanval

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6		Zeer Laag	Zeer Laag	Laag

Betreffende hosts
config-a4.digid.nl

Omschrijving
Een aanvaller kan een Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende host header verstuurd.

Details
Wanneer de host-header wordt aangepast naar een andere host (in dit geval bijv. sogeti.nl), dan wordt de bezoeker naar de malafide host doorgestuurd. Dit kan worden gebruikt bij bijvoorbeeld een phishing aanval. Deze bevinding is niet aanwezig op de productieomgeving, enkel in de acceptatie omgeving. Zie de onderstaande request en response.

Request:

```
POST /jobs?cachebust=1574244671.66 HTTP/1.1
Host: sogeti.nl
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0)
Gecko/20100101 Firefox/70.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 210
Origin: https://config-a4.digid.nl
```

```
Connection: close
Referer: https://config-a4.digid.nl/jobs
Cookie: [.. truncated ..]
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=XdugdpTiPZoocGWRheg3Ai4NCI1C2zB45sWj
QQj0%2BxTRDVsUBCRMgxD9FPrGWe1OTGeJpfoaLKY1vC3j0CLAJg%3D%3D&job=CreateA
ccountsJob&type=midden_actief&from=test&to=test&commit=Create+accounts
```

Response:

```
HTTP/1.1 302 Found
Date: Thu, 21 Nov 2019 14:40:03 GMT
Cache-Control: no-cache
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
X-Request-Id: 3f0b01d0-14f2-4f34-90f4-e2bd30727c3c
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'; form-action 'self'
https:
Location: https://sogeti.nl/jobs
Status: 302 Found
Content-Type: text/html; charset=utf-8
Connection: close
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 88

<html><body>You are being <a
href="https://sogeti.nl/jobs">redirected</a>.</body></html>
```

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
Securitytest DigiD R5.14

Kenmerk: 42100000

Datum	13-01-2020
Status	Definitief
Versie	1.0

Rubricering	derubricering
Vaststeller	10.2e
Functie	Ketenbeheerder voorziening

Colofon

Kenmerk	**42100000**
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
17-01-2020	0.1	Sogeti	Initiële versie
17-01-2020	0.2	Sogeti	Interne review
05-02-2020	1.0	Sogeti	Aanvullingen/reactie Logius

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest betrof de aanstaande release 5.14 van DigiD. De test is bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook zijn er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Conclusies en aanbevelingen

- De config-a4 geeft informatie vrij over de query van de database zodra er een waarde wordt ingevuld geeft de database een syntax fout en laat hierbij de hele database query zien. Zie bevinding #3. *Aanbeveling: Vang de syntax fout van de database op en weergeef het niet aan de eindgebruiker.*

- Het is mogelijk om bezoekers door te sturen naar externe domeinen. Dit kan misbruikt worden door een aanvaller die een gerichte phishing aanval uitvoert. Zie bevindingen #8, en #9. *Aanbeveling: Whitelist alleen de headers die nodig zijn voor de werking van de applicatie.*

- De server geeft informatie vrij over de gebruikte software en onderliggende logica. Zie bevinding #4, #5, en #6. *Aanbeveling: toon alleen informatie die nodig is voor de werking van de applicaties.*

- De server maakt geen gebruik van een header die het downgraden van een veilige verbinding naar een onveilige verbinding voorkomt. Zie bevinding #2 *Aanbeveling: Implementeer de header die het downgraden van een veilige verbinding naar een onveilige verbinding voorkomt.*

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

De opdracht is geheel conform het Security Testplan uitgevoerd.
Aan de securitytest is als volgt invulling gegeven:

- Volledig geautomatiseerde scans zijn uitgevoerd op de applicatie, met behulp van tooling.
- De resultaten van de test zijn handmatig geverifieerd.
- Er is een handmatige vulnerability assessment uitgevoerd op de systemen en de applicatie.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. het is niet gelukt om de DigiD app tijdig functioneel te krijgen waardoor het niet mogelijk is geweest om de functie tot het wijzigen van de DigiD app pincode te testen.

Zie Security Testplan DigiD R5.14 v1.2.pdf, hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'. Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Grey box test.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Invoerafhandeling	0	0	0	1	0	1
Servers	0	0	0	4	2	6
Client-side controls	0	0	0	2	0	2
Totaal	**0**	**0**	**0**	7	**2**	9

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01 Informatiebeveiligingsbeleid
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.
Oordeel
Toelichting
B.02 Toegangsvoorzieningsbeleid
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.
Oordeel
Toelichting
B.03 Risicomanagement
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.
Oordeel
Toelichting
B.04 Cryptografiebeleid
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).
Oordeel
Toelichting
B.05 Contractmanagement
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.
Oordeel
Toelichting
B.06 ICT-landschap
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.
Oordeel
Toelichting

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.
Oordeel

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

derubricering

Toelichting

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Toelichting

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Toelichting

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Toelichting

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Toelichting

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Toelichting

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

Toelichting

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Toelichting

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Toelichting

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Toelichting

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Toelichting

U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Toelichting

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel	
Toelichting	
U/PW.04 Isolatie van processen/bestanden	
Beperk de impact bij misbruik van processen.	
Oordeel	
Toelichting	
U/PW.05 Toegang tot beheermechanismen	
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Toelichting	
U/PW.06 Platform-netwerkkoppeling	
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Toelichting	
U/PW.07 Hardening van platformen	
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting	
U/PW.08 Platform- en webserverarchitectuur	
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting	
U/NW.01 Operationeel beleid voor netwerken	
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting	
U/NW.02 Beschikbaarheid van netwerken	
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Toelichting	
U/NW.03 Netwerkzonering	
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Toelichting	
U/NW.04 Protectie- en detectiefunctie	
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Toelichting	
U/NW.05 Beheer- en productieomgeving	
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Toelichting	
U/NW.06 Hardening van netwerken	
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting	
U/NW.07 Netwerktoegang tot webapplicatie	

Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Oordeel	
Toelichting	

U/NW.08 Netwerkarchitectuur

Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Oordeel	
Toelichting	

Beheersingsdomein

C.01 Servicemanagementbeleid

Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Oordeel	
Toelichting	

C.02 Compliancemanagement

Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Oordeel	
Toelichting	

C.03 Vulnerability-assessments

Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Oordeel	
Toelichting	

C.04 Penetratietestproces

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Oordeel	
Toelichting	

C.05 Technische controlefunctie

Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Oordeel	
Toelichting	

C.06 Logging

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Oordeel	
Toelichting	

C.07 Monitoring

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	
Toelichting	

C.08 Wijzigingenbeheer

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

derubricering

Oordeel	
Toelichting	

C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Toelichting	

C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Toelichting	

C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Toelichting	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 HttpOnly-flag ontbreekt

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1		Laag	Laag	Laag

Betreffende hosts
app-a4.digid.nl
stubs-a4.digid.nl

Omschrijving
De HttpOnly flag zorgt dat er, door de daarvoor geschikte browsers, wordt tegenhouden dat een cookie kan worden ingelezen door een client-side script. Wanneer deze flag door de server wordt verstuurd zal dit ertoe leiden dat de informatie van een cookie niet kan worden ingelezen tijden een Cross-Site-Scripting (XSS) aanval.

Bedreiging
Als een aanvaller code kan uitvoeren in de browser van de gebruiker (bijvoorbeeld middels XSS) heeft hij bij het ontbreken van de HttpOnly flag ook toegang tot de cookies. Hij kan deze dan uitlezen en manipuleren, waardoor het in sommige gevallen mogelijk is om de sessie-ID te stelen en de sessie van de gebruiker over te nemen.

Aanbeveling
Bij het versturen van het cookie naar de gebruiker moet HttpOnly op de volgende manier aan de Set-Cookie-header worden toegevoegd:

- "Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; '"HttpOnly'""

Voor meer informatie over HttpOnly-cookies en hoe deze te implementeren zie:

- https://www.owasp.org/index.php/HttpOnly

derubricering

Details
De HttpOnly flag zorgt ervoor dat cookies niet uitgelezen kunnen worden door bijvoorbeeld een client-side script.
Request:

```
GET /sms_stub HTTP/1.1
Host: stubs-a4.digid.nl
[...truncated...]
```

Response:

```
HTTP/1.1 200 OK
10.2g
[...truncated...]
Content-Type: text/html; charset=utf-8
Set-Cookie: _persist=![...truncated...]d0FXjWKCXPx4UiOQ=; path=/
[...truncated...]
```

3.1.2 *HTTP Strict Transport Security (HSTS) header ontbreekt*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2		Laag	Laag	Laag

Betreffende hosts
stubs-a4.digid.nl

Omschrijving
HTTP Strict Transport Security (HSTS) is een beveiligingsmechanisme in moderne browsers, speciaal ontwikkeld om het downgraden van HTTPS naar HTTP te voorkomen. De server initieert dit door een header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen, dwingt hij het gebruik van HTTPS af. Dit houdt in dat er niet langer HTTP-verzoeken worden toegestaan naar het betreffende domein.

Bedreiging
Wanneer de HSTS-header niet is geïmplementeerd kan een aanvaller in een Man-in-the-Middle situatie een HTTPS-verzoek downgraden naar HTTP. Hierdoor worden gegevens onversleuteld verstuurd waardoor ze voor iedereen met toegang tot het verkeer leesbaar zijn.

Aanbeveling
Implementeer HSTS door de volgende response header toe te voegen:
Strict-Transport-Security: max-age=31536000
De beperking kan ook automatisch voor alle subdomeinen opgelegd worden:
Strict-Transport-Security: max-age=31536000; includeSubDomains
Meer informatie over de HSTS-header vindt u hier:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

Details

Wanneer de HSTS-header niet is geïmplementeerd kan een aanvaller in een Man-in-the-Middle situatie een HTTPS-verzoek downgraden naar HTTP. Hierdoor worden gegevens onversleuteld verstuurd waardoor ze voor iedereen met toegang tot het verkeer leesbaar zijn.

Requests:

```
POST /reporting HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv.72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 172
Origin. https://stubs-a4.digid.nl
Connection: close
Referer: https://stubs-a4.digid.nl/reporting
Cookie: [ truncated ]
```

Response:

```
HTTP/1.1 200 OK
[redacted]
Cache-Control: max-age=0, private, must-revalidate
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
X-Request-Id: edfb8b03-4ff0-4cfb-bd79-574f294834ec
X-Download-Options: noopen
X-Frame-Options. sameorigin
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'; form-action 'self'
[redacted]
ETag: W/"b25a9d9bed251b887e8dec9f2d519905"
Status: 200 OK
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Connection: close
Set-Cookie: [...truncated...]
Content-Length: 4515
[...truncated...]
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er

informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 SQL injection

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3		Laag	Laag	Laag

Betreffende hosts
config-a4.digid.nl/job

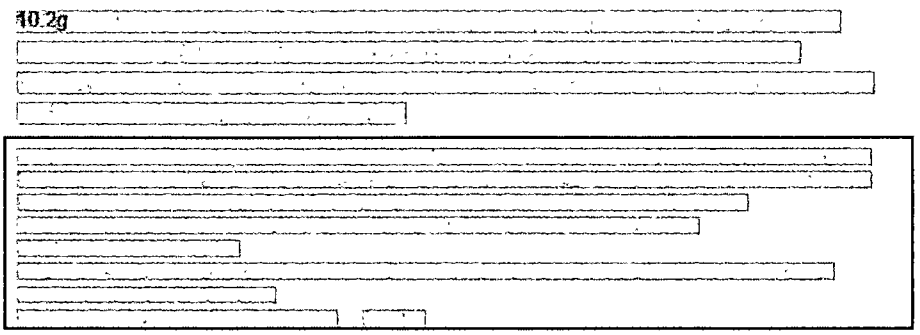
Omschrijving

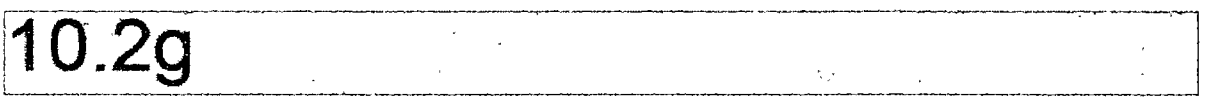
De door een gebruiker opgegeven invoer wordt gebruikt in of als commando's (queries) die door de achterliggende SQL database rechtstreeks uitgevoerd worden.

Bedreiging
Door de invoer uit te breiden met, of aan te passen naar, database commando's kan een gebruiker de database manipuleren zonder dat dit de bedoeling van de ontwikkelaar is. Dit kan ertoe leiden dat ongewenst informatie wordt vrijgegeven, dan wel gegevens worden gemanipuleerd of verwijderd

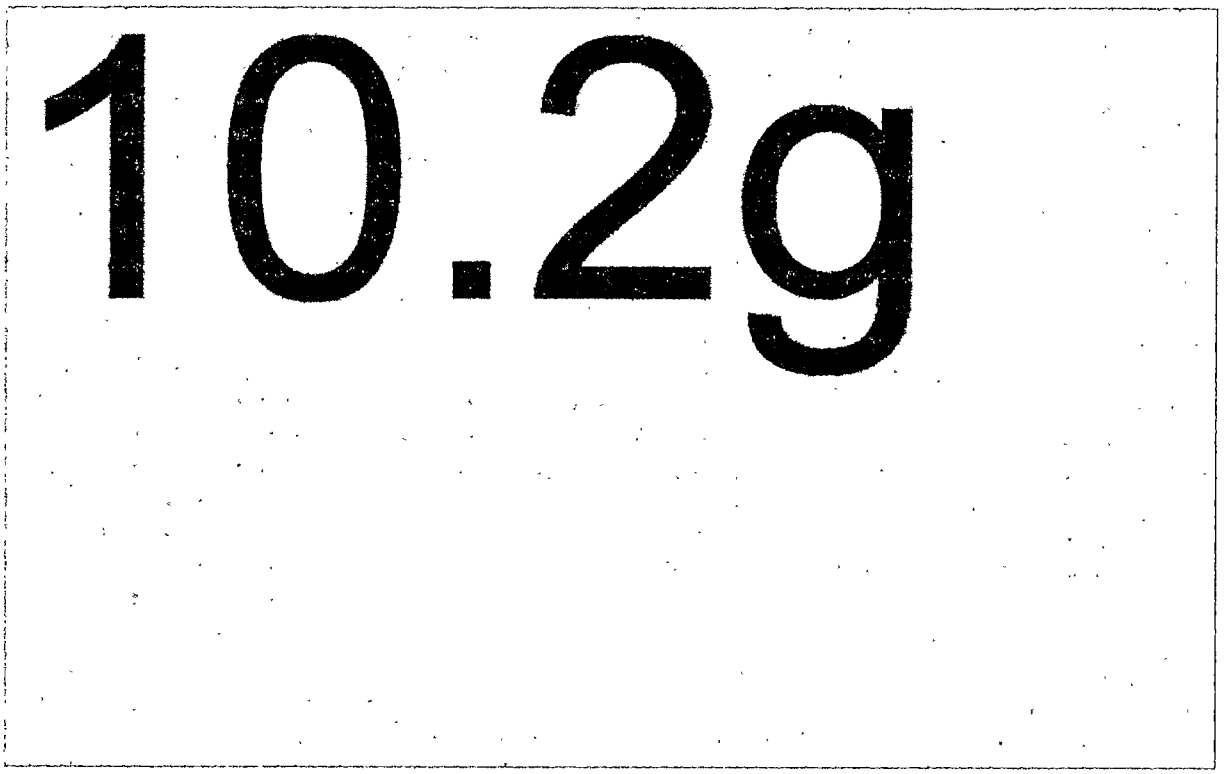
Aanbeveling
Vertrouw invoer van gebruikers niet wanneer deze direct als invoer op een ander systeem gebruikt kan worden.
Om SQL injection te voorkomen is het aan te raden de vraagstelling van de applicatie aan de database in twee delen aan te leveren. Maak gebruik van geparameteriseerde queries met placeholders. Op deze manier worden logica en data gescheiden en zal de applicatie deze twee niet met elkaar verwarren en per ongeluk informatie van de gebruiker als commando uitvoeren.
Zie ook
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet.
Daarnaast is het aan te raden aangeleverde invoer te valideren op het verwachte type, zoals bijvoorbeeld tekst en datum, alsook op lengte en formaat zoals bij een postcode of een telefoonnummer. Dit is een mitigerende maatregel die als aanvullend voordeel heeft dat ook andere problemen zoals bijvoorbeeld type mismatches worden voorkomen.

Details





derubricering



3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 Information disclosure - Versie-informatie

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Laag	Midden	Zeer Laag

Betreffende hosts
app-a4.digid.nl
stubs-a4.digid.nl

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5		Laag	Midden	Zeer Laag

Betreffende hosts

a4.digid.nl

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6		Laag	Midden	Zeer Laag

Betreffende hosts
stubs-a4.digid.nl

Omschrijving
Systemen geven vaak zelf onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een default instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details
De hosts geven informatie vrij over de gebruikte software inclusief versienummers. Kwaadwillende kunnen deze informatie gebruiken in een (toekomstige) aanval. Zo kunnen kwaadwillende gebruikers wachten op een bepaald moment dat er een zero-day kwetsbaarheid voor de specifieke gebruikte software bekend wordt.
In de response op de volgende request is de gebruikte software inzichtelijk:
Request:

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: […truncated…]
```

Response:

```
HTTP/1.1 200 OK
Date: Wed, 15 Jan 2020 08:56:05 GMT
[redacted]
Cache-Control: max-age=0, private, must-revalidate
[...truncated...]
```

Details
De host geeft informatie vrij over de gebruikte software inclusief versienummers. Kwaadwillende kunnen deze informatie gebruiken in een (toekomstige) aanval. Zo kunnen kwaadwillende gebruikers wachten op een bepaald moment dat er een zero-day kwetsbaarheid voor de

specifieke gebruikte software bekend wordt.
In de response op de volgende request is de gebruikte software inzichtelijk:

Request:

```
GET /assets/application-
2bf67cd1a8c2c1febbee201adac040faf651fbdc586bcb7e2f7c2f233f5ec167.js
HTTP/1.1
Host: a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://a4.digid.nl/inloggen
Cookie:
_pk_id.12.0d98=82e3d0d91cb30bfb.1573030080.2.1578901212.1578900959.;
_persist=!/uNRxE3oV4AgV2/8GEo7bK1tTam5S1kFC/gu12f1NHb7IRrkdvQW6Ci1+UdR
CjmMBEYoAhtsRD5rE/72DsJyhxILZCbmpCFzJZgCdZE=;
_session_id=c2bed592fc48c6ce090ef9336a3ba33b
Cache-Control: max-age=0
```

Response:

```
HTTP/1.1 200 OK
Last-Modified: Tue, 12 Nov 2019 09:28:19 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=100
Content-Type: application/javascript
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close
Date: Mon, 13 Jan 2020 08:25:59 GMT
Expires: Mon, 13 Jan 2020 09:25:59 GMT
Age: 0
Content-Length: 257079
```

Details

De host geeft informatie vrij over de gebruikte software inclusief versienummers. Kwaadwillende kunnen deze informatie gebruiken in een (toekomstige) aanval. Zo kunnen kwaadwillende gebruikers wachten op een bepaald moment dat er een zero-day kwetsbaarheid voor de specifieke gebruikte software bekend wordt.

In de response op de volgende request is de gebruikte software inzichtelijk:

Request:

```
GET /feature_docs/js/jquery.js HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://stubs-a4.digid.nl/feature_docs/index.html
[...truncated...]
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 13 Jan 2020 10:07:42 GMT
10.2g
Last-Modified: Tue, 12 Nov 2019 09:54:35 GMT
ETag: "16eac-597233c4eccc0"
Accept-Ranges: bytes
Content-Length: 93868
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript
Set-Cookie:[...truncated...]
102g
(function(a,b){function cy(a){return
[...truncated...]
```

3.9.2 *Information disclosure - API documentatie*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7		Laag	Zeer Laag	Midden

Betreffende hosts
eid-a4.digid.nl

Omschrijving
De server geeft informatie vrij over zowel de interne als externe versie van de API.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om gevoelige informatie uit de API op te vragen. Tevens biedt het een aanvaller informatie over de interne werking van een systeem.

Aanbeveling
Verwijder de API documentatie op de server, zodat aanvallers geen informatie krijgen over de interne werking van het systeem.

Details

```
10.2g
```

Hier is te zien hoe zowel de externe als interne API er uit ziet. Hierdoor zien aanvallers welke API calls mogelijk zijn, hoe het authenticatie proces verloopt en wat de interne werking van het systeem is. Dit biedt kansen voor aanvallers om gericht te gaan zoeken naar kwetsbaarheden in de API.

Interne API:

```
https://eid-a4.digid.nl/v2/api-docs?group=intern
```

Externe API:

```
https://eid-a4.digid.nl/v2/api-docs?group=extern
```

Het is aanbevolen om [redacted] en bovengenoemde URL's niet publiekelijk beschikbaar te maken.

3.9.3 *X-Forwarded-Host-header aanval*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
8		Zeer Laag	Zeer Laag	Laag

Omschrijving
Een aanvaller kan een X-Forwarded-Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de X-Forwarded-Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de X-Forwarded-Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende X-Forwarded-Host header verstuurd.

Details
De host is kwetsbaar voor een X-Forwarded-Host header aanval. Hierbij wordt een X-Forwarded-Host header aan de request meegegeven. Het gevolg is dat een bezoeker vanuit de host direct naar de host wordt gestuurd die in de X-Forwarded-Host header is opgegeven. Een dergelijke aanval kan worden ingezet bij phishing campagnes, waarbij bezoekers naar een malafide inlogpagina worden gestuurd. Het doorsturen van de bezoeker is te zien in de onderstaande request en response.

Request:

```
POST /aanvraag HTTP/1.1
Host: balie-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 261
```

```
Origin: https://balie-a4.digid.nl
Connection: close
Referer: https://balie-a4.digid.nl/
[.. truncated ..]
Upgrade-Insecure-Requests: 1
X-Forwarded-Host: sogeti.nl
utf8=%E2%9C%93&authenticity_token=wbGQdKg8j6B6ZoaBIq8X8QITruj58D1iDa3l
rMsB7UzhxsEpRo2BMz72r5SBFVO3NBKFWnsEvbrCAXiSw8R9Aw%3D%3D&create_verifi
cation_form%5Bcitizen_service_number%5D=000000073&create_verification_
form%5Bfront_desk_code%5D=BFFS3VZN4&commit=Volgende
```

Response:

```
HTTP/1.1 302 Found
Date: Wed, 15 Jan 2020 09:17:04 GMT
[.. truncated ..]
<html><body>You are being <a
href="https://sogeti.nl/aanvraag/110/controle">redirected</a>.</body><
/html>
```

Zoals te zien is in de laatste regel van de response, wordt de bezoeker doorgestuurd naar sogeti.nl

3.9.4 *Host-header aanval*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
9		Zeer Laag	Zeer Laag	Laag

Omschrijving
Een aanvaller kan een Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende host header verstuurd.

Details
Wanneer de host-header wordt aangepast naar een andere host (in dit geval bijv. sogeti.nl), dan wordt de bezoeker naar de malafide host doorgestuurd. Dit kan worden gebruikt bij bijvoorbeeld een phishing aanval. Zie de onderstaande request en response.
Request:

```
POST /jobs HTTP/1.1
Host: sogeti.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 208
Origin: https://config-a4.digid.nl
Connection: close
```

```
Referer: https://config-a4.digid.nl/jobs
[.. truncated ..]
Upgrade-Insecure-Requests: 1
utf8=%E2%9C%93&authenticity_token=UF2K7oA742lqxkcCGVW5AvA%2FPD9hcs06Mm
ePjgdo4cmNKWtWTVn7nMRHnOEQrXXI6PcbWU8e08DrwBvJx0Y1iQ%3D%3D&job=CreateA
ccountsJob&type=midden_actief&from=200&to=200&commit=Create+accounts
```

Response:

```
HTTP/1.1 302 Found
Date: Wed, 15 Jan 2020 09:21:16 GMT
Cache-Control: no-cache
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
X-Request-Id  56b4287f-a86c-45a8-a16b-9bc2b4d0191e
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'; form-action 'self'
https:
Location: https://sogeti.nl/jobs
Status: 302 Found
Content-Type: text/html; charset=utf-8
Connection: close
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 88
<html><body>You are being <a
href="https://sogeti.nl/jobs">redirected</a>.</body></html>
```

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD R5.15

Kenmerk: n.b.

Datum	07-05-2020
Status	Definitief
Versie	1.0

Rubricering	derubricering
Vaststeller	10.2e
Functie	Teamleider

Colofon

Kenmerk	n.b.
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
29-04-2020	0.1	Sogeti	Initiële versie
29-04-2020	0.2	Sogeti	Interne review
29-04-2020	0.3	Sogeti	Revisie
07-05-2020	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

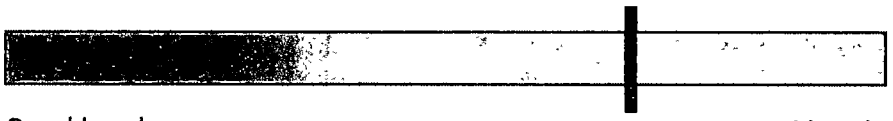
derubricering

Managementsamenvatting

Inleiding

Er is een Nieuwe DigID release ontwikkeld, namelijk DigiD R5.15. Om inzicht te krijgen in het beveiligingsniveau van deze release, is een security test uitgevoerd. Zowel de nieuwe DigiD release als het internetverkeer van de DigiD app zijn onderzocht. In dit rapport treft u de resultaten van de security test aan.

Conclusies en aanbevelingen



Onvoldoende Voldoende

A. 10.2g

B. 10.2g

C. Er wordt geen gebruik gemaakt van best-practises omtrent cookies. Zo is de bescherming tegen het onderscheppen van cookies niet maximaal. Zie bevindingen 2 en 3.
Aanbeveling: implementeer bij het plaatsen van cookies de best-practices zoals beschreven in bevindingen 2 en 3.

D. De servers geven onnodig gedetailleerde informatie vrij over de onderliggende software van het platform. Kwaadwillenden kunnen deze informatie gebruiken in (toekomstige) aanvallen, bijvoorbeeld wanneer zero-day kwetsbaarheden worden ontdekt. Zo is duidelijk geworden dat er gebruik wordt gemaakt van verouderde software die kwetsbaarheden bevat. Zie bevindingen 6 en 7.
Aanbeveling: beperk de vrijgave van informatie tot een minimum en update de kwetsbare software uit bevinding 6 naar een nieuwere versie.

E. Om te navigeren door middel van "app2app" en "app2web" verkeer wordt gebruik gemaakt van universal links, met URL scheme's als een fallback mechanisme. Aanvullend zijn deze zaken onderzocht. Er zijn hierin geen nieuwe kwetsbaarheden aangetroffen.

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

De aanleiding tot deze securitytest betrof de aanstaande release 5.15 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook zijn er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Het doel was om inzicht te krijgen in het beveiligingsniveau van DigiD en de risico's die Logius loopt.

De opdracht is geheel conform het Security Testplan uitgevoerd.
Aan de securitytest is als volgt invulling gegeven:

- Volledig geautomatiseerde scans zijn uitgevoerd op de applicatie, met behulp van tooling.
- De resultaten van de test zijn handmatig geverifieerd.
- Er is een handmatige vulnerability assessment uitgevoerd op de systemen en de applicatie.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. Zie *Security Testplan DigiD R5.15 v1.1.pdf*, hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'.

Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Grey box security test.

1.3 Scope

De scope van deze securitytest is de DigiD-applicatie, gezien vanaf een extern oogpunt.

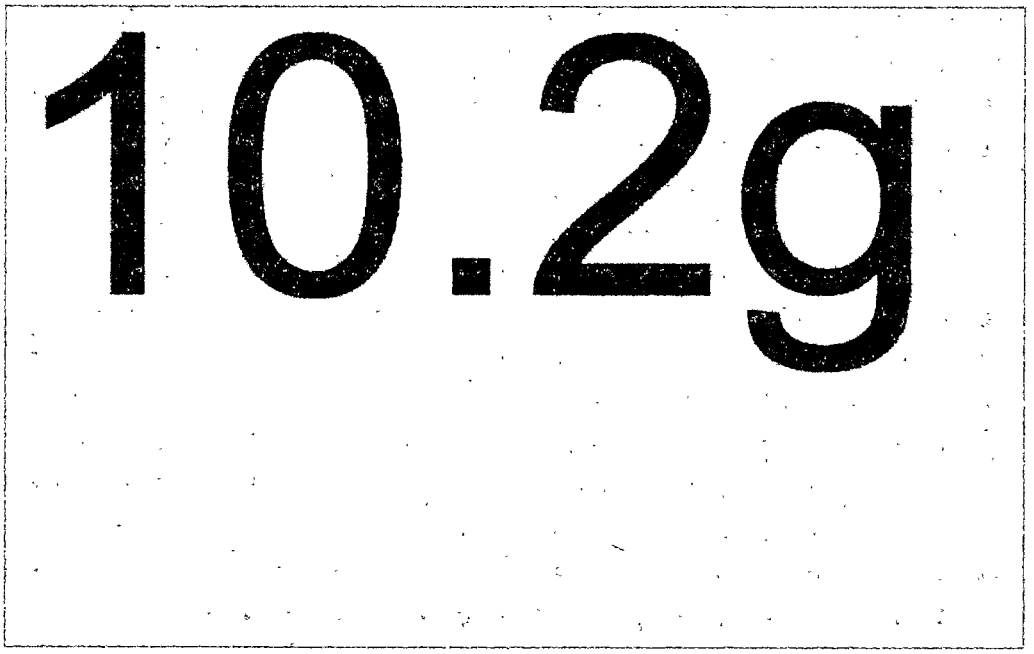
Binnen scope

V Alle services in onderstaande tabel zoals ontsloten naar eindgebruikers en andere services.
V Het verkeer tussen de mobiele en desktopapplicaties voor eindgebruikers en de backend.
V Het verkeer tussen systemen buiten Kern (RDA-server, Status Controller, eID server) en DigiD kern voor zover zichtbaar.

derubricering

Onderstaande schematische weergave geeft een visuele representatie van wat wel en wat niet getest is binnen de scope van de securitytest[1]:

Onderdeel	Omkadering / vulling	Omschrijving
Functioneel	Oranje / grijs	Binnen scope (voor zover extern benaderbaar)
DigID Hoog (nieuw)	Oranje / geel	Binnen scope (voor zover extern benaderbaar)
DigID Kern	Paars	Binnen scope (voor zover extern benaderbaar)
DigID-Hoog/Substantieel/App	Groen	Alleen functioneel en berichtenverkeer
Infrastructuur	Blauw	Buiten scope, valt niet extern te testen
Certificaten (nieuw)	Geen / geel	Buiten scope, valt niet extern te testen
DigID Extern	Geen / paars	Buiten scope, valt niet extern te testen



In bovenstaande afbeelding zijn interacties en koppelvlakken tussen de verschillen actoren weergegeven.

In de tabel hieronder is weergegeven op basis van scopebepaling of deze binnen de test vielen:

Nr	Aanvraag vanuit DigID aan RDW	Van	Ontvanger	
1	Opvragen DigID Hoog Middel	DigID	RDW	Binnen scope
2	Status wijzigingsverzoek DigID Hoog middel	DigiD	RDW	Binnen scope
3	Heraanvragen PIN/PUK mailer	DigiD	RDW	Binnen scope
20	Aanvragen AT certificaat	DigiD	RDW	Binnen scope
	Aanvragen vanuit RDW			
4	Status wijzigingen door MU	RDW	DigiD	Buiten scope, valt niet extern te testen
5	Levering risicogebieden	DigiD	RDW	Binnen scope
6	Opvragen PP	RDW	BSNk PP	Buiten scope, valt niet extern te testen
8	Doorgeven statuswijziging IR	RDW	BSNk IR	Buiten scope, valt niet extern te testen

[1] *NB de scope van de securitytest is dus niet gelijk aan de scope van de release*

	Koppelvlakken			
7	Opvragen vercijferd Pseudoniem	DigID	BSNk PP	Binnen scope
9	Opvragen sleutelmateriaal HSM	HSM	BSNk SB	Buiten scope, valt niet extern te testen
11	Opvragen adresgegevens	Beheer	BRP	Binnen scope
12	Opvragen persoongegevens	Beheer	BRP	Binnen scope
13	Print en verzend opdracht	DS	BS	Buiten scope, valt niet extern te testen
14	Authenticatie aanvraag	AK	MK	Buiten scope, valt niet extern te testen
18	Opvragen status	DigID	SC	Binnen scope
	PCA			
16	PCA eIDAS protocol	eIDsrv	eIDclt	Binnen scope
17	Registeren aanvraag, uitreiking, intrekking	AS	MU	Buiten scope, valt niet extern te testen
19	Controleren WID (BAC/BAP)	DigID	WID	Binnen scope

Tijdens de securitytest is ook gelet op eventuele regressie danwel ongeautoriseerde of onbedoelde veranderingen.

De securitytest richtte zich op de volgende componenten in de *A4* omgeving:

Onderwerp	URL	IP-adres
Mijn DigiD	https://mijn.a4.digid.nl	144.43.243.145
Aanvragen	https://a4.digid.nl/aanvragen	144.43.243.144
Activeren	https://a4.digid.nl/activeer_digid	144.43.243.144
Herstellen	https://a4.digid.nl/herstellen	144.43.243.144
Koppelvlakken	https://was-a4.digid.nl	144.43.243.146
Beheermodule	https://digidbeheer-a4.digid.nl	144.43.243.148
Balie	https://balie-a4.digid.nl	144.43.243.147
DIgiD app	https://app-a4.digid.nl	144.43.243.170
Status Controler	msc-a4.digid.nl	145.21.253.99
eid server	eid-a4.digid.nl	144.43.243.155
stub	stubs-a4.digid.nl	144.43.243.154
config	config-a4.digid.nl	144.43.243.149

Buiten scope

In het kader van deze opdracht worden door de auditor de volgende werkzaamheden niet uitgevoerd.

- Alle websites en referenties die niet op het onderliggende systeem aanwezig zijn.
- De organisatie, fysieke ruimten en documentatie.
- DOS aanvallen of andere performance gerelateerde testen vallen buiten de scope, wel dient er naar beschikbaarheid gekeken te worden.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Authenticatie	0	0	1	1	0	**2**
Servers	0	0	0	1	1	**2**
Client-side controls	0	0	0	0	3	**3**
Totaal	**0**	**0**	**1**	**2**	**4**	**7**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01 Informatiebeveiligingsbeleid	
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope.	

B.02 Toegangsvoorzieningsbeleid	
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope.	

B.03 Risicomanagement	
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope.	

B.04 Cryptografiebeleid	
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Buiten scope.	

B.05 Contractmanagement	
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope.	

B.06 ICT-landschap	
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope.	

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen	
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	

[2] Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Geen bevindingen.

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope.

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope.

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Zie bevindingen 4 en 5.

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Geen bevindingen.

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Geen bevindingen.

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

Zie bevindingen 6 en 7.

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen.

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Zie bevindingen 1, 2 en 3.

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Buiten scope.

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope.

U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Geen bevindingen.

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel

Zie bevindingen 6 en 7.

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Buiten scope.

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Geen bevindingen.

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Geen bevindingen.

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Buiten scope.

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope.

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope.

U/NW.02 Beschikbaarheid van netwerken

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel

Buiten scope.

U/NW.03 Netwerkzonering

Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Oordeel

Buiten scope.

U/NW.04 Protectie- en detectiefunctie

Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Oordeel

Buiten scope.

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buiten scope.

U/NW.06 Hardening van netwerken

Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Geen bevindingen.

U/NW.07 Netwerktoegang tot webapplicatie

Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Oordeel	

Buiten scope.

U/NW.08 Netwerkarchitectuur

Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Oordeel	

Buiten scope.

Beheersingsdomein

C.01 Servicemanagementbeleid

Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Oordeel	

Buiten scope.

C.02 Compliancemanagement

Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Oordeel	

Buiten scope.

C.03 Vulnerability-assessments

Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Oordeel	

Buiten scope.

C.04 Penetratietestproces

Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Oordeel	

Buiten scope.

C.05 Technische controlefunctie

Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Oordeel	

Buiten scope.

C.06 Logging

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Oordeel	

Buiten scope.

C.07 Monitoring

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	

Buiten scope.

C.08 Wijzigingenbeheer

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

derubricering

Oordeel	
Buiten scope.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Zie bevinding 6. De Yarn versie is niet up-to-date en bevat kwetsbaarheden.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Buiten scope.	

derubricering

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 HTTP Strict Transport Security (HSTS) header ontbreekt

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
app-a4.digid.nl
digidbeheer-a4.digid.nl
stubs-a4.digid.nl
was-a4.digid.nl

Omschrijving
HTTP Strict Transport Security (HSTS) is een beveiligingsmechanisme in moderne browsers, speciaal ontwikkeld om het downgraden van HTTPS naar HTTP te voorkomen. De server initieert dit door een header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen, dwingt hij het gebruik van HTTPS af. Dit houdt in dat er niet langer HTTP-verzoeken worden toegestaan naar het betreffende domein.

Bedreiging
Wanneer de HSTS-header niet is geïmplementeerd kan een aanvaller in een Man-in-the-Middle situatie een HTTPS-verzoek downgraden naar HTTP. Hierdoor worden gegevens onversleuteld verstuurd waardoor ze voor iedereen met toegang tot het verkeer leesbaar zijn.

Aanbeveling
Implementeer HSTS door de volgende response header toe te voegen:
Strict-Transport-Security: max-age=31536000
De beperking kan ook automatisch voor alle subdomeinen opgelegd worden:
Strict-Transport-Security: max-age=31536000; includeSubDomains

Meer informatie over de HSTS-header vindt u hier:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

Details
In de onderstaande request en response is te zien dat de HSTS-header niet in de response terug komt.

Request:

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 200 OK
Date: Fri, 24 Apr 2020 12:30:49 GMT
[redacted]
Cache-Control: max-age=0, private, must-revalidate
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
X-Request-Id: 8328283f-fa90-40ca-8fe3-d0e3d1c9f1ee
X-Download-Options: noopen
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'
[redacted]
Set-Cookie: _digid_stubs_session=b91385[.. truncated ..]aed64a;
path=/; HttpOnly; secure; SameSite=Lax
ETag: W/"4834630b235b1006efec368186dfbcd1"
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie: _persist='lPfKRylLra[.. truncated
..]O7epxownzPH2K9DmmG4UQ=; path=/
```

Zoals te zien is, ontbreekt de HSTS-header, ofwel "Strict-Transport-Security: max-age=<seconden>; includeSubDomains" in de response.

Het is aanbevolen deze header te implementeren, zodat gebruik van een TLS verbinding wordt geforceerd door de browser van de gebruiker.

3.1.2 *HttpOnly-flag ontbreekt*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
app-a4.digid.nl
stubs-a4.digid.nl

Omschrijving
De HttpOnly flag zorgt ervoor dat er, door de daarvoor geschikte browsers, wordt tegenhouden dat een cookie kan worden ingelezen door een client-side script. Wanneer deze flag door de server wordt verstuurd zal dit ertoe leiden dat de informatie van een cookie niet kan worden ingelezen tijden een Cross-Site-Scripting (XSS) aanval.

Bedreiging
Als een aanvaller code kan uitvoeren in de browser van de gebruiker (bijvoorbeeld middels XSS) heeft hij bij het ontbreken van de HttpOnly flag ook toegang tot de cookies. Hij kan deze dan uitlezen en manipuleren, waardoor het in sommige gevallen mogelijk is om de sessie-ID te stelen en de sessie van de gebruiker over te nemen.

Aanbeveling
Bij het versturen van het cookie naar de gebruiker moet HttpOnly op de volgende manier aan de Set-Cookie-header worden toegevoegd:

- Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; HttpOnly
  Voor meer informatie over HttpOnly-cookies en hoe deze te implementeren zie:
- https://www.owasp.org/index.php/HttpOnly

Details
De *persist* cookie wordt niet gezet met de HttpOnly flag. Dit is te zien in de onderstaande request en response:

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Het betreft de tweede cookie in de onderstaande response:

```
HTTP/1.1 200 OK
[... truncated ..]
Set-Cookie: _digid_stubs_session=b913852fc6f5f657f16f9e331daed64a;
path=/; HttpOnly; secure; SameSite=Lax
[... truncated ..]
Set-Cookie: _persist=[lPfKRylLr[... truncated
..]UJLkq87Dd+5SerTguO7epxownzPH2K9DmmG4UQ=; path=/
```

3.1.3 *Secure-flag ontbreekt*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3		Zeer Laag	Zeer Laag	Zeer Laag

Betreffende hosts
app-a4.digid.nl
stubs-a4.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de Secure-flag mee te geven in de Set-cookie-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruikmaakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker een onbeveiligde HTTP-verbinding op te laten zetten. Tenzij er gebruikgemaakt wordt van de HTTP Strict Transport Security-header, zal de browser de cookies over de niet-beveiligde verbinding versturen, waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van het cookie naar de gebruiker moet de Secure flag op de volgende manier aan de Set-Cookie-header worden toegevoegd:
"Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; Secure"
Let wel: Als het cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan het cookie op dat moment nog onderschept worden.

Details
Niet alle cookies worden geplaatst met de Secure flag bij het versturen van onderstaande request:

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Zie de tweede cookie die wordt geplaatst, onderaan de response:

```
HTTP/1.1 200 OK
[... truncated ..]
Set-Cookie: _digid_stubs_session=b913852fc[... truncated ..]; path=/;
HttpOnly; secure; SameSite=Lax
ETag: W/"4834630b235b1006efec368186dfbcd1"
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie: persist=!lPfKRylLraYDh[... truncated
..]+5SerTguO7epxownzPH2K9DmmG4UQ=; path=/
[... truncated ..]
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Een overzicht van deze bevindingen.

3.3.1 Denial-of-Service - Inlogpogingen

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4		Midden	Midden	Midden

Betreffende hosts
a4.digid.nl

Omschrijving
10.2g

Bedreiging
10.2g

10.2g

Aanbeveling

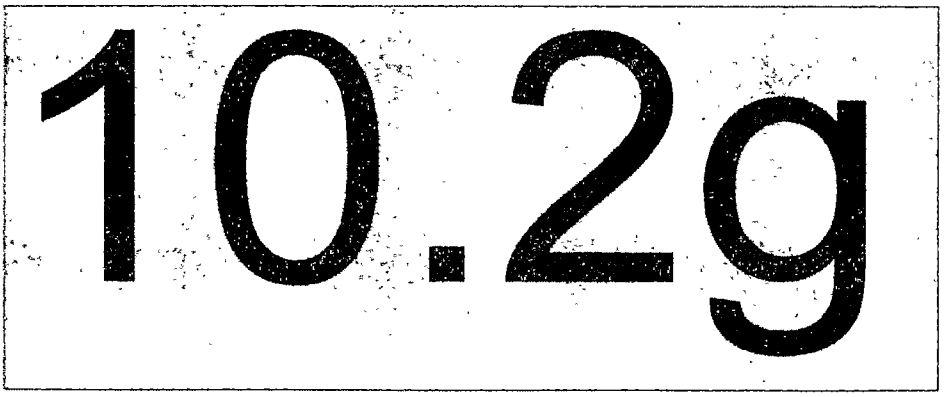
10.2g

Details

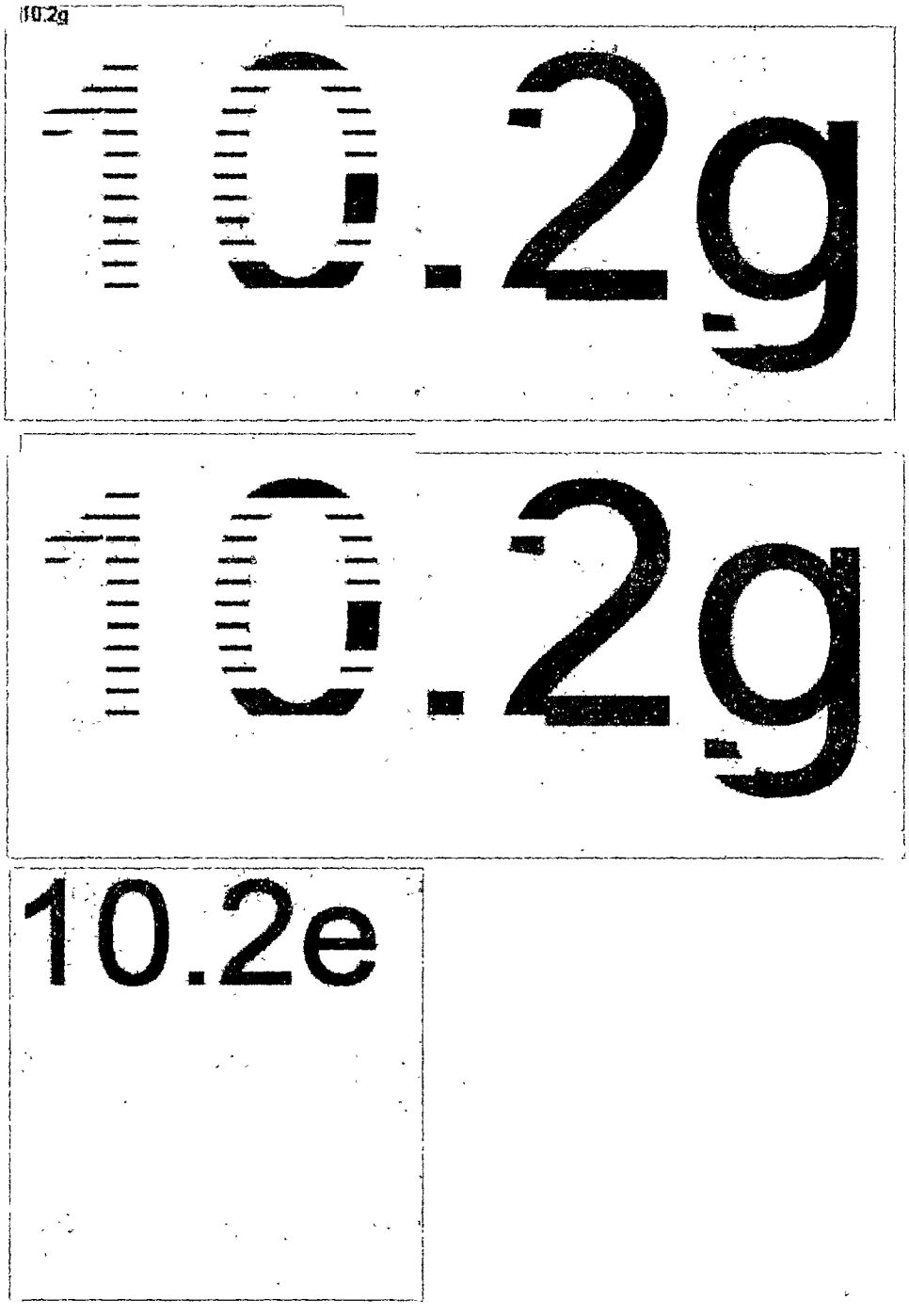
10.2g

10.2g

Login request:



derubricering



3.3.2 *Authenticatie bruteforce*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5		Laag	Laag	Midden

Betreffende hosts
a4.digid.nl

Omschrijving

10.2g

Bedreiging

10.2g

Aanbeveling

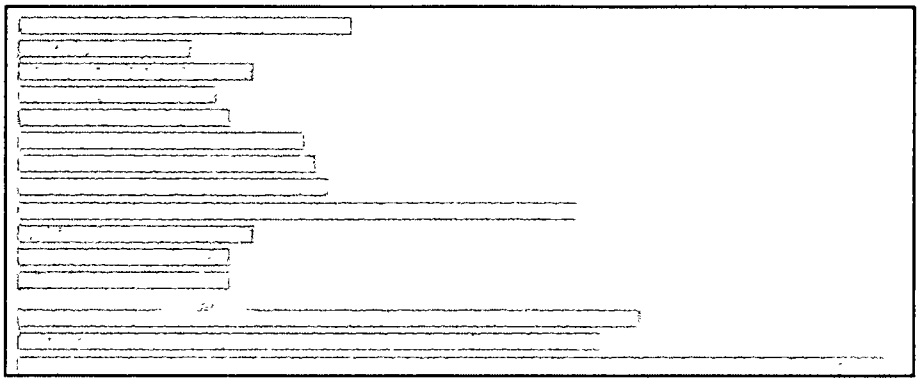
10.2g

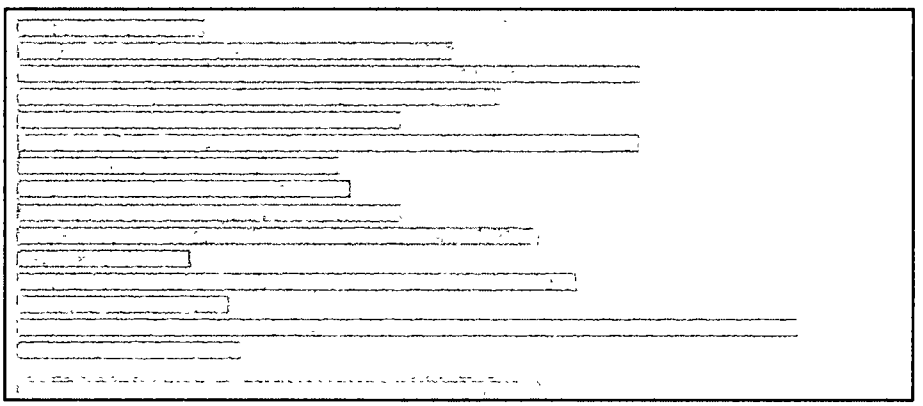
Details

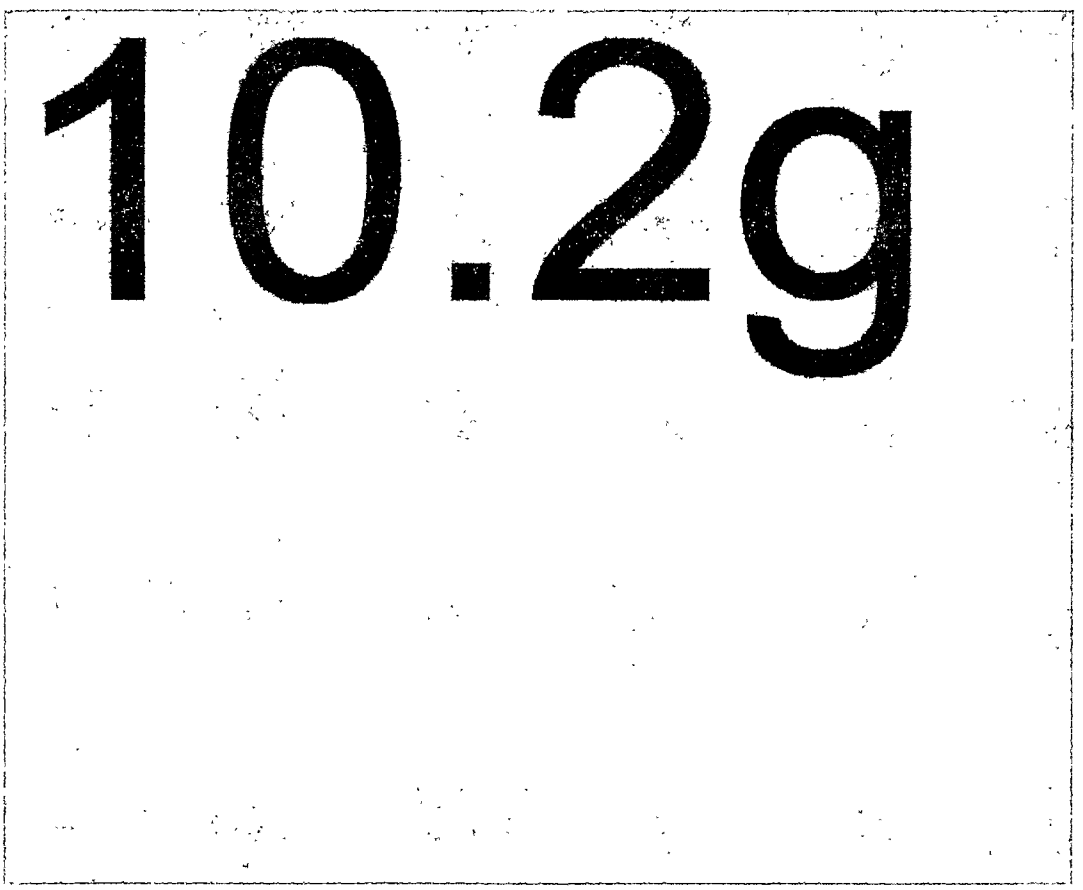
10.2g

derubricering

10.2g







3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 *Information disclosure – Versie informatie*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6		Laag	Zeer Laag	Midden

Betreffende hosts
stubs-a4.digid.nl

Omschrijving
Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details
De server geeft informatie vrij over de gebruikte software. Zo is te zien dat de server gebruik maakt van 10.2g en 10.1c Deze versie is kwetsbaar voor een path traversal aanval, zoals te zien is op:
10.2g en 10.1c

Het is de testers niet gelukt deze path traversal kwetsbaarheid uit te buiten. Desalniettemin is aanbevolen de configuratie te updaten naar een recentere versie.

De versie-informatie is onderaan de webpagina te zien van de volgende URL:

```
https://stubs-a4.digid.nl/feature_docs
```

3.9.2 *Information disclosure - Versie informatie*

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7		Zeer Laag	ZeerLaag	ZeerLaag

Betreffende hosts
stubs-a4.digid.nl

Omschrijving
Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details
10.2g

Request

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 24 Apr 2020 12:30:49 GMT
10.2g en 10.1c
[.. truncated ..]
```

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD R5.16

Kenmerk: -

Datum	24 augustus 2020
Status	Concept
Versie	0.3
Rubricering	derubricering
Vaststeller	Logius

Colofon

Kenmerk	-
Versienummer	0.3
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
21 augustus 2020	0.1	Sogeti	Initiële versie
24 augustus 2020	0.2	Sogeti	Interne review
24 augustus 2020	0.3	Sogeti	Review verwerkt

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

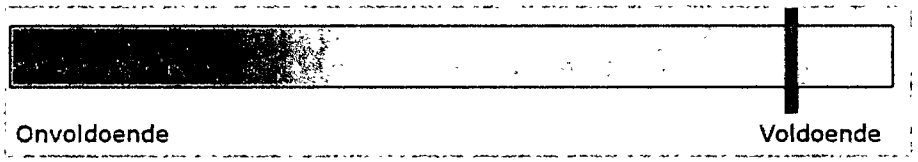
Inhoud

Managementsamenvatting

Inleiding

De aanleiding tot deze securitytest betreft de aanstaande release 5.16 van DigiD. De test is bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen. Er is extra aandacht geschonken aan de mogelijke risico's die de wijzigingen en uitbreidingen die in deze release zijn opgenomen met zich meebrengen. Ook worden er voorstellen gedaan hoe deze risico's gemitigeerd kunnen worden.

Conclusies en aanbevelingen



Moderne browsers beschikken over ingebouwde beveiligingsmechanismes. Deze kunnen worden aangezet door specifieke waardes mee te sturen vanuit de server. Binnen de DigiD omgeving zijn er servers die deze waardes niet mee sturen. Het is aanbevolen deze waardes mee te sturen zodat deze beveiligingsmechanismes worden geactiveerd, zie bevinding 1, 2, en 3.

Applicaties binnen de DigiD omgeving lijken te reageren bij het versturen van versnipperde data. Dit is een aanvalsmethode waarbij verzoeken van gebruikers kunnen worden aangepast, waardoor het mogelijk is om deze ongewilde acties uit te laten voeren. Het is tijdens de securitytest niet gelukt om dit te exploiteren, mede omdat de server niet het verwachte gedrag vertoonde bij deze aanval. Het is aanbevolen om na te lopen of de versnipperde data anders wordt verwerkt per server. Zie bevinding 4.

Het is mogelijk om gebruikers door te sturen naar een externe website via de DigiD omgeving. Dit betekent dat de gebruiker een URL binnen het DigiD domein kan openen en vervolgens door wordt gestuurd naar een mogelijk malafide website zonder dit door te hebben. Het is aanbevolen om gebruikers nooit naar externe websites te sturen zonder hier een waarschuwing bij te geven. Zie bevinding 5, 6.

Binnen de applicatie wordt er versie informatie getoond van de gebruikte software. Dit kan een aanvaller inzicht geven in mogelijk kwetsbaarheden van de website. Het is aanbevolen om deze informatie niet te tonen. Zie bevinding 7, 8, 9, 10 en 11.

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

De opdracht is geheel conform het Security Testplan uitgevoerd.
Aan de securitytest is als volgt invulling gegeven:

- Volledig geautomatiseerde scans zijn uitgevoerd op de applicatie, met behulp van tooling.
- De resultaten van de test zijn handmatig geverifieerd.
- Er is een handmatige vulnerability assessment uitgevoerd op de systemen en de applicatie.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. Zie Security Testplan Logius DigiD R5.16 v1.1, hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'.

Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Bij een vulnerabilityassessment wordt het domein nauwkeurig onderzocht aan de hand van een in huis ontwikkelde methodiek. Tooling is daarbij ondergeschikt aan de kennis en expertise van de securityconsultants. Weliswaar wordt gestart met een automated test inclusief manual verification, maar aanvullend daarop vindt ook een beoordeling plaats van alles wat een tool alleen niet kan vinden. Een vulnerabilityassessment levert een overzicht van alle aanwezige technische zwakheden, die binnen een vooraf gestelde 'time box' zijn gevonden.

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Greybox.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	**Totaal**
Client-side Controls	0	0	0	0	3	**3**
Invoerafhandeling	0	0	1	1	1	**3**
Servers	0	0	0	0	5	**5**
Totaal	**0**	**0**	**1**	**1**	**9**	**11**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Buiten scope.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope.	

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen

De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Oordeel

Geen bevindingen.

U/WA.01 Operationeel beleid voor webapplicaties

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Oordeel

Buiten scope.

U/WA.02 Webapplicatiebeheer

Effectief en veilig realiseren van de dienstverlening.

Oordeel

Buiten scope.

U/WA.03 Webapplicatie-invoer

Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Oordeel

Zie bevinding 5 en 6.

U/WA.04 Webapplicatie-uitvoer

Voorkom manipulatie van het systeem van andere gebruikers.

Oordeel

Geen bevindingen.

U/WA.05 Betrouwbaarheid van gegevens

Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Oordeel

Geen bevindingen.

U/WA.06 Webapplicatie-informatie

Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Oordeel

Geen bevindingen.

U/WA.07 Webapplicatie-integratie

Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

Oordeel

Geen bevindingen.

U/WA.08 Webapplicatiesessie

Voorkomen dat derden de controle over een sessie kunnen krijgen.

Oordeel

Geen bevindingen.

U/WA.09 Webapplicatiearchitectuur

Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Oordeel

Buiten scope.

U/PW.01 Operationeel beleid voor platformen en webservers

Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Oordeel

Buiten scope.

U/PW.02 Webprotocollen

derubricering

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Zie bevinding 4

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel

Zie bevinding 1, 2, 3, 7, 8, 9, 10 en 11

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Buiten scope.

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Geen bevindingen.

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Geen bevindingen.

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Buiten scope.

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope.

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope.

U/NW.02 Beschikbaarheid van netwerken

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel

Buiten scope.

U/NW.03 Netwerkzonering

Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Oordeel

Buiten scope.

U/NW.04 Protectie- en detectiefunctie

Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Oordeel

Buiten scope.

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buiten scope.

U/NW.06 Hardening van netwerken
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Oordeel
Geen bevindingen.
U/NW.07 Netwerktoegang tot webapplicatie
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.
Oordeel
Buiten scope.
U/NW.08 Netwerkarchitectuur
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.
Oordeel
Buiten scope.

Beheersingsdomein

C.01 Servicemanagementbeleid
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
Oordeel
Buiten scope.
C.02 Compliancemanagement
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.
Oordeel
Buiten scope.
C.03 Vulnerability-assessments
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.
Oordeel
Buiten scope.
C.04 Penetratietestproces
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).
Oordeel
Buiten scope.
C.05 Technische controlefunctie
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.
Oordeel
Buiten scope.
C.06 Logging
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.
Oordeel
Buiten scope.
C.07 Monitoring

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	

Buiten scope.

C.08	**Wijzigingenbeheer**

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Oordeel	

Buiten scope.

C.09	**Patchmanagement**

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Oordeel	

Geen bevindingen.

C.10	**Beschikbaarheidbeheer**

Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Oordeel	

Buiten scope.

C.11	**Configuratiebeheer**

Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Oordeel	

Buiten scope.

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 HTTP Strict Transport Security (HSTS) header ontbreekt

Omschrijving
HTTP Strict Transport Security (HSTS) is een beveiligingsmechanisme in moderne browsers, speciaal ontwikkeld om het downgraden van HTTPS naar HTTP te voorkomen. De server initieert dit door een header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen, dwingt hij het gebruik van HTTPS af. Dit houdt in dat er niet langer HTTP-verzoeken worden toegestaan naar het betreffende domein.

Bedreiging
Wanneer de HSTS-header niet is geïmplementeerd kan een aanvaller in een Man-in-the-Middle situatie een HTTPS-verzoek downgraden naar HTTP. Hierdoor worden gegevens onversleuteld verstuurd waardoor ze voor iedereen met toegang tot het verkeer leesbaar zijn.

Aanbeveling
Implementeer HSTS door de volgende response header toe te voegen:
Strict-Transport-Security: max-age=31536000
De beperking kan ook automatisch voor alle subdomeinen opgelegd worden:
Strict-Transport-Security: max-age=31536000; includeSubDomains
Meer informatie over de HSTS-header vindt u hier:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
stubs-a4.digid.nl

Details
De applicatie maakt geen gebruik van de HSTS-header.
Request

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
```

Response headers

```
HTTP/1.1 200 OK
10.2g en 10.1c
Date: Tue, 18 Aug 2020 14:04:53 GMT
Content-Type: text/html; charset=utf-8
Connection: close
ETag: W/"5e1eae1bc84fcba064c72fa0b6f27804"
Cache-Control: max-age=0, private, must-revalidate
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'
X-Request-Id: 9fe2ce30-371b-4539-8457-883e12f28659
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Set-Cookie: _persist=deleted; path=/;Domain=digid.nl; expires=Thu, 01
Jan 1970 00:00:00 GMT
```

3.1.2 *HttpOnly-flag ontbreekt*

Omschrijving
De HttpOnly flag zorgt ervoor dat er, door de daarvoor geschikte browsers, wordt tegenhouden dat een cookie kan worden ingelezen door een client-side script. Wanneer deze flag door de server wordt verstuurd zal dit ertoe leiden dat de informatie van een cookie niet kan worden ingelezen tijden een Cross-Site-Scripting (XSS) aanval.

Bedreiging
Als een aanvaller code kan uitvoeren in de browser van de gebruiker (bijvoorbeeld middels XSS) heeft hij bij het ontbreken van de HttpOnly flag ook toegang tot de cookies. Hij kan deze dan uitlezen en manipuleren, waardoor het in sommige gevallen mogelijk is om de sessie-ID te stelen en de sessie van de gebruiker over te nemen.

Aanbeveling
Bij het versturen van het cookie naar de gebruiker moet HttpOnly op de volgende manier aan de Set-Cookie-header worden toegevoegd:

- Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; HttpOnly
  Voor meer informatie over HttpOnly-cookies en hoe deze te implementeren zie:
- https://www.owasp.org/index.php/HttpOnly

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
stubs-a4.digid.nl

Details
De _persist cookie wordt ingesteld zonder de HttpOnly flag.
Request

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
```

Response Headers

```
HTTP/1.1 200 OK
[redacted]
Date  Tue, 18 Aug 2020 11:40:10 GMT
Content-Type: text/plain
Content-Length: 26
Connection: close
Last-Modified: Sun, 16 Aug 2020 11:56:06 GMT
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Set-Cookie: _persist='PuorEd+MId6H1E71k4[...]gVQ==; path=/;
```

3.1.3 *Secure-flag ontbreekt*

Omschrijving
De server stuurt cookies naar de gebruiker zonder de Secure-flag mee te geven in de Set-cookie-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruikmaakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker een onbeveiligde HTTP-verbinding op te laten zetten. Tenzij er gebruikgemaakt wordt van de HTTP Strict Transport Security-header, zal de browser de cookies over de niet-beveiligde verbinding versturen, waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van het cookie naar de gebruiker moet de Secure flag op de volgende manier aan de Set-Cookie-header worden toegevoegd:
''Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD];
'"Secure'''''
Let wel: Als het cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan het cookie op dat moment nog onderschept worden.

derubricering

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
stubs-a4.digid.nl

Details
De _persist cookie wordt ingesteld zonder de Secure flag.
Request

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
```

Response Headers

```
HTTP/1.1 200 OK
10.2g en 10.1c
Date: Tue, 18 Aug 2020 11:40:10 GMT
Content-Type: text/plain
Content-Length: 26
Connection: close
Last-Modified: Sun, 16 Aug 2020 11:56:06 GMT
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Set-Cookie: _persist=!PuorEd+M1dÉHiE71k4[...]gVQ==; path=/
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 Onverwacht gedrag

Omschrijving

De applicatie of het systeem vertoont onverwacht of onverklaarbaar gedrag op een actie die uitgevoerd wordt door de gebruiker.

Bedreiging

Een aanvaller kan het onverwachte gedrag wellicht gebruiken om de applicatie, het systeem of de gebruikers ervan aan te vallen.

Aanbeveling

Onverwacht of onverklaarbaar gedrag kan het gevolg zijn van programmeer- of configuratiefouten. Probeer te ontdekken wat de precieze oorzaak van het onverwachte gedrag is en pas het gedrag aan.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts

balie-a4.digid.nl
digidbeheer-a4.digid.nl

Details

Binnen de balie en beheer applicatie lijkt "chunked" input anders te worden verwerkt door verschillende servers. Dit kan duiden dat een HTTP Request smuggling aanval mogelijk is.

Bij deze aanval wordt er misbruik gemaakt van het feit dat servers verschillend omgaan met header. Een packet wordt zo aangepast dat de "chunked" informatie wordt uitgevoerd in het volgende verzoek door een willekeurige gebruiker. Voor meer informatie zie: https://portswigger.net/web-security/request-smuggling.

Eerst is er getracht smuggling uit te voeren met de CL.TE smuggling aanval. Hierbij maakt de front-end gebruik van de Content-Length header en de back-end van de Transfer-Encoding header:

```
POST / HTTP/1.1
Host: balie-a4.digid.nl
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 131
Transfer-Encoding : chunked

0
```

```
GET /controle HTTP/1.1
Host: sogetisecuritytest
Content-Length: 3
Connection: close

x=1
```

Na een langere tijd wordt er een lege response teruggestuurd door de server. Echter duit er niks op dat de informatie die verstuurd is terugkomt in het volgende verzoek.

Ook is er getracht een basis TE.CL Request smuggle te doen. Hierbij maakt de front-end gebruik van de Transfer-Encoding header en de back-end van de Content-Length header.

```
POST / HTTP/1.1
Host: balie-a4.digid.nl
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length. 3
Transfer-Encoding : chunked

5c
GPOST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

x=1
0
```

Hier lijkt de server wel anders te reageren. Een 404 melding wordt getoond. Echter wordt er bij het volgende verzoek geen melding getoond dat GPOST niet is toegestaan, wat er op zou duiden dat de server de chunked data meeneemt in de volgende request. Het is aanbevolen dit eventueel nog te verifiëren met toegang tot logs.

NB Voor de beheeromgeving kan het volgende request gebruikt worden voor HTTP smuggling (TE:CL), deze stuurt ook een leeg response naar een wat langere tijd.

```
POST / HTTP/1.1
Host: digidbeheer-a4.digid.nl
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-CSRF-Token:
bHNLtUnsJcDZquY6kZhWGFM9wvxneyesOZTjis7gS1kZ+vya2vo+WI2kZfPj1qxCygDPkJ
UENb8wzg9wKbO9SQ==
X-Requested-With: XMLHttpRequest
Origin: https://digidbeheer-a4.digid.nl
DNT: 1
Connection: close
Referer: https://digidbeheer-a4.digid.nl/bulk_orders
Cookie: _digid_admin_session=d3a4be8847c21bbb00ccf83c46aebaca;
_persist='cbr6Xcz0lnvJCSv1k4RPDFNVOiLPBpBUeFZnpDQlAEWdsIPfr1vdnMIDztK9
nMwZR564T8DklE8Z38gTfHTLbEaEtzD+/myR8T39KtXnbA==
Content-Length: 12
Transfer-Encoding: identity
Transfer-Encoding: chunked

0

X
```

Ook al is het niet gelukt om deze kwetsbaarheid tijdens de doorlooptijd van de security test uit te buiten is het aanbevolen om te controleren of servers iets van de chunked data verwerken. Dit kan bijvoorbeeld worden gedaan door te kijken in de logs of data van de aanval terugkomt.

3.7.2 *Host-header aanval*

Omschrijving
Een aanvaller kan een Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging
Doordat de waarde van de Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling
Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende host header verstuurd.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5	Onbekend	Laag	Laag	Zeer Laag

Betreffende Hosts
balie-a4.digid.nl

Details
De X-Forwarded-Host header wordt door de server verwerkt.
Request

```
GET / HTTP/1.1
Host: balie-a4.digid.nl
X-Forwarded-Host: sogeti.com
```

Response

```
HTTP/1.1 302 Found
Date: Wed, 19 Aug 2020 11:42:33 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Location: https://sogeti.com/saml/sp/eherkenning_authentication
[..truncated..]

<html><body>You are being <a
href="https://sogeti.com/saml/sp/eherkenning_authentication">redirecte
d</a>.</body></html>
```

3.7.3 *Open doorverwijzing*

Omschrijving
De server stuurt de gebruiker door naar een URL die gebaseerd is op ongevalideerde invoer.

Bedreiging
Het is mogelijk gebruikers door te sturen naar een zelfgekozen URL of een URL binnen een ander domein. Een aanvaller kan zo gebruikers naar een kwaadwillende webapplicatie laten doorsturen door de legitieme server. De doorverwijzing wordt door de browser van de gebruiker automatisch gevolgd. Hierdoor kan het voor de eindgebruiker moeilijk zijn de juiste

vertrouwensbeslissing te nemen, zeker als de aanvaller voor zijn kwaadwillende webapplicatie een domeinnaam kiest die lijkt op die van de legitieme applicatie.
Een gebruiker heeft bijvoorbeeld een zekere mate van vertrouwen in Sogeti en ontvangt de volgende link via de mail:
https://www.sogeti.nl?redirect=http://www.sogetti.nl
Deze link wijst naar de website van Sogeti en omdat de gebruiker Sogeti vertrouwt klikt hij deze de link aan. Als deze kwetsbaarheid van toepassing is zal de webapplicatie een doorverwijzing sturen naar de browser van de gebruiker met daarin de opdracht om naar http://www.sogetti.nl (met dubbel 't') te gaan.

Aanbeveling
Sta alleen doorverwijzingen toe naar pagina's binnen het domein van de applicatie of naar pagina's en domeinen die op een whitelist staan.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6	Onbekend	Midden	Laag	Laag

Betreffende Hosts
a4.digid.nl

Details
Het is mogelijk om een open doorverwijzing te doen met volgende URL:

```
https:/a4.digid.nl/cookies_geblokkeerd?url=.sogeti.nl
```

Hierbij wordt de doorverwijzing a4.digid.nl samen met de ingevulde tekst van de url-parameter. Als een gebruiker bijvoorbeeld .sogeti.nl invult. Wordt de gebruiker doorverwezen naar a4.digid.nl.sogeti.nl.
Request:

```
GET /cookies_geblokkeerd?url=.sogeti.nl HTTP/1.1
Host: a4.digid.nl
```

Response:

```
HTTP/1.1 302 Found
Date: Wed, 19 Aug 2020 10:02:01 GMT
[..truncated..]

<html><body>You are being <a
href="https://a4.digid.nl.sogeti.nl">redirected</a>.</body></html>
```

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 Information disclosure - Versie informatie

Omschrijving

Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging

Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling

Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
7	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts

digidbeheer-a4.digid.nl

Details

10.2g

Request:

```
GET /munin/status/dgd-a4-as1.bh.dgd-
a4.easi/diskstats_latency/index.html HTTP/1.1
Host: digidbeheer-a4.digid.nl
```

Response:

```
HTTP/1.1 200 OK
Date: Tue, 18 Aug 2020 14:39:12 GMT
Content-Type: text/html
Content-Length: 11781
Connection: close
Last-Modified: Tue, 18 Aug 2020 14:31:53 GMT
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
```

```
        "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
[...TRUNCATED...]
10.2g
</div>
```

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
8	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
stubs-a4.digid.nl
config-a4.digid.nl
digidbeheer-a4.digid.nl

Details
10.2g

Request

```
GET / HTTP/1.1
Host: stubs-a4.digid.nl
```

Response Headers

```
HTTP/1.1 200 OK
10.2g en 10.1c
Date: Tue, 18 Aug 2020 14:04:53 GMT
Content-Type: text/html; charset=utf-8
Connection: close
ETag: W/"5e1eae1bc84fcba064c72fa0b6f27804"
Cache-Control: max-age=0, private, must-revalidate
Content-Security-Policy: default-src 'self' https:; font-src 'self'
https: data:; img-src 'self' https: data:; object-src 'none'; script-
src 'self' 'unsafe-inline'; style-src 'self' https: 'unsafe-inline';
frame-src 'self' https:; frame-ancestors 'none'
X-Request-Id: 9fe2ce30-371b-4539-8457-883e12f28659
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Set-Cookie: _persist=deleted; path=/;Domain=digid.nl; expires=Thu, 01
Jan 1970 00:00:00 GMT
```

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
9	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
was-a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl
app-a4.digid.nl

Details
10.2g

Request:

```
GET /assets/application-
d09c123275f7008f31ace25f51b9864daf5fcfe00fec59f6c9b7c2c932721e57.js
HTTP/1.1
Host: was-a4.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://was-a4.digid.nl/
Connection: close
Cookie: _session_id=9a25feadde409cde6074009212956Of3;
_persist=!u3oNioBMXq+GPAD1k4RPDFNVOiLPBr1CmIPnGEC1nNkkr88qSzo3PQ/N9g8X
W2wpbGhASqR7yqetnUOqA7xwKxhYkemkv6dDvgWif8k=
```

Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 10 Aug 2020 09:50:45 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=99
Content-Type: application/javascript
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Connection: close

{..TRUNCATED...}
```

[redacted]

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
10	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts

was-a4.digid.nl
mijn.a4.digid.nl
digidbeheer-a4.digid.nl
app-a4.digid.nl

Details

[redacted]

Request:

```
GET /assets/application-
d09c123275f7008f31ace25f51b9864daf5fcfe00fec59f6c9b7c2c93272Ie57.js
HTTP/1.1
Host: was-a4.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://was-a4.digid.nl/
```

```
Connection: close
Cookie: _session_id=9a25feadde409cde60740092129560f3;
_persist=!u3oNioBMXq+GPAD1k4RPDFNVOiLPBr1CmIPnGEC1nNkkr88qSzo3PQ/N9g8X
W2wpbGhASqR7yqetnUOqA7xwKxhYkemkv6dDvgWif8k=
```

Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 10 Aug 2020 09:50:45 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=99
Content-Type: application/javascript
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

{...TRUNCATED...}
3929
[redacted]
*/
```

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
11	Onbekend	Zeer Laag	Zeer Laag	Zeer Laag

Betreffende Hosts
app-a4.digid.nl

Details
[redacted]

Request:

```
GET /assets/digid_eo_rgb-
55f1daa50e8a463ddb0718ad1781c22195c16d3bfee3535b1df04fed763f488a.svg
HTTP/1.1
Host: app-a4.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://app-a4.digid.nl/
Connection: close
Cookie: _session_id=e2d7b6cd7b9d08d267da52e672a9c27b;
_persist=!BzWkrdlcE2n4+cX1k4RPDFNVOiLPBn5XjqkPd0ebG9Ohjzz29OAfJMfS12Pp
Evigyu0DvqNldOLCXpwDAvhhOOq2x4qIgLlDvMCVVAA=
```

Response:

```
HTTP/1.1 200 OK
[redacted]
Last-Modified: Wed, 15 Aug 2018 06:18:31 GMT
Accept-Ranges: bytes
Cache-Control: max-age=31536000
Keep-Alive: timeout=5, max=98
Content-Type: image/svg+xml
Connection: close
```

```
Date: Mon, 17 Aug 2020 08:09:45 GMT
Expires: Tue, 17 Aug 2021 08:09:45 GMT
Age: 0
Content-Length: 1594
```

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD R5.17

Kenmerk: XXXXXX

Datum	2 december 2020
Status	Definitief
Versie	1.0
Rubricering	derubricering
Vaststeller	Logius

Colofon

Kenmerk	XXXXXX
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
20 November 2020	0.1	Sogeti	Initiële versie
20 november 2020	0.2	Sogeti	Interne review
20 november 2020	0.3	Sogeti	Review verwerkt
1 December 2020	1.0	Sogeti	Feedback verwerkt

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

Managementsamenvatting

Inleiding

De scope van een security assessment wordt daarbij bepaald door de voorziening (infrastructuur en software) en de productrisico's.

In de praktijk wordt deze assessment ofwel jaarlijks uitgevoerd voor een voorziening in opdracht van een servicemanager vanuit team 'Levering', ofwel maakt deze assessment onderdeel uit van een testtraject voor een specifieke release in opdracht van een Product Owner.

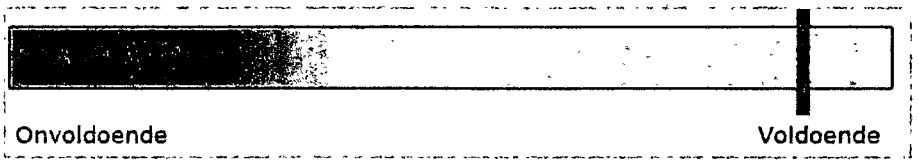
Het doel van deze securitytest uitgevoerd met release 5.17 is inzicht te krijgen in het beveiligingsniveau van het te testen product en de (beveiligings) risico's die Logius loopt.

Securitytesten worden onderscheiden in de mate waarin de tester (in de praktijk een "legale" hacker) vooraf informatie krijgt van het te testen systeem. Hiervoor worden de volgende benamingen gebruikt: blackbox test, greybox test en whitebox test. Whitebox wordt door sommige partijen ook wel crystal box genoemd.

Deze Security Testrapportage beschrijft concreet en specifiek de aanpak van deze voorgenomen securitytest. Deze Testrapportage is opgesteld in overleg met alle vier de betrokken partijen: Logius, de securitytest organisatie als auditor, de leverancier van de voorziening als auditee, en Equinix. En deze Testrapportage maakt onderdeel uit van de vrijwaringsverklaring tussen deze betrokkenen.

Middels het 'kenmerk' op het voorblad is het Testrapportage onlosmakelijk verbonden met de opdracht en daarmee verbonden met de contractueel geregelde vrijwaringsverklaring. Deze Testrapportage mag dan ook niet worden beschouwd als een 'levend' projectplan, maar is scope bepalend en dient een eigen doelgroep. De juridische aspecten zijn opgenomen in de vrijwaringsverklaring, en de inhoudelijke en technische afspraken in deze Security Testrapportage.

Conclusies en aanbevelingen



Het is mogelijk om gebruikers door te sturen naar externe websites. Een aanvaller kan een malifide link naar de gebruiker sturen. Als de gebruiker deze link opent wordt hij vervolgens doorgestuurd naar een website die de aanvaller in zijn beheer kan hebben. Dit zou bijvoorbeeld gebruikt kunnen worden voor phishing aanvallen.
Aanbeveling: zorg ervoor dat gebruikers niet doorgestuurd kunnen worden naar externe websites. Zie bevinding 1 en 2.

De DigID omgeving toont versie informatie van meerdere diensten binnen de omgeving. Dit geeft een aanvaller meer informatie wat in de toekomst misbruikt kan worden als er ontdekt wordt dat er in die bepaalde versies kwetsbaarheden zijn. Deze informatie is dus inherent niet gelijk onveilig maar kan onzekerheden bieden voor de toekomst.
Aanbeveling: zorg ervoor dat deze informatie niet getoond wordt. Zie bevinding 3, 4, 5 en 6.

Aanvullingen Logius

Deze paragraaf biedt Logius de ruimte opmerkingen te plaatsen bij de inhoud van dit rapport.

1 Inleiding

1.1 Opdrachtformulering

De opdracht is geheel conform het Security Testplan uitgevoerd.
Aan de securitytest is als volgt invulling gegeven:

- Volledig geautomatiseerde scans zijn uitgevoerd op de applicatie, met behulp van tooling.
- De resultaten van de test zijn handmatig geverifieerd.
- Er is een handmatige vulnerability assessment uitgevoerd op de systemen en de applicatie.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd. Zie Security_Testplan_Logius_DigiD_R5.17_v1.0, hoofdstuk 4, 'Aanpak' en bijlagen van 'Aanpak securitytest'.

Er is getest met bekende en actuele exploits en daarnaast is getest op de meest voorkomende risico's en fouten (in ieder geval de OWASP top 10 en de SANS top 25).

Bij een vulnerability assessment wordt het domein nauwkeurig onderzocht aan de hand van een in huis ontwikkelde methodiek. Tooling is daarbij ondergeschikt aan de kennis en expertise van de security consultants. Weliswaar wordt gestart met een automated test inclusief manual verification, maar aanvullend daarop vindt ook een beoordeling plaats van alles wat een tool alleen niet kan vinden. Een vulnerability assessment levert een overzicht van alle aanwezige technische zwakheden, die binnen een vooraf gestelde 'time box' zijn gevonden.

Afhankelijk van de aard en hoeveelheid informatie die vooraf beschikbaar is gesteld, vindt een Black box, Grey box of White box test plaats. In het kader van deze securitytest was er sprake van een Greybox.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	**Totaal**
Servers	0	0	2	0	4	**6**
Totaal	**0**	**0**	**2**	**0**	**4**	**6**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2 (2015)[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01 Informatiebeveiligingsbeleid
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.
Oordeel
Buiten scope.
B.02 Toegangsvoorzieningsbeleid
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.
Oordeel
Buiten scope.
B.03 Risicomanagement
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.
Oordeel
Buiten scope.
B.04 Cryptografiebeleid
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).
Oordeel
Buiten scope.
B.05 Contractmanagement
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.
Oordeel
Buiten scope.
B.06 ICT-landschap
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.
Oordeel
Buiten scope.

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Uitvoeringsdomein

U/TV.01 Toegangsvoorzieningsmiddelen
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.
Oordeel
Geen bevindingen.
U/WA.01 Operationeel beleid voor webapplicaties
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.
Oordeel
Buiten scope.
U/WA.02 Webapplicatiebeheer
Effectief en veilig realiseren van de dienstverlening.
Oordeel
Buiten scope.
U/WA.03 Webapplicatie-invoer
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.
Oordeel
Zie bevinding 1 en 2.
U/WA.04 Webapplicatie-uitvoer
Voorkom manipulatie van het systeem van andere gebruikers.
Oordeel
Geen bevindingen.
U/WA.05 Betrouwbaarheid van gegevens
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.
Oordeel
Geen bevindingen.
U/WA.06 Webapplicatie-informatie
Beperk het (onnodig) vrijgeven van informatie tot een minimum.
Oordeel
Geen bevindingen.
U/WA.07 Webapplicatie-integratie
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.
Oordeel
Geen bevindingen.
U/WA.08 Webapplicatiesessie
Voorkomen dat derden de controle over een sessie kunnen krijgen.
Oordeel
Geen bevindingen.
U/WA.09 Webapplicatiearchitectuur
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.
Oordeel
Buiten scope.
U/PW.01 Operationeel beleid voor platformen en webservers
Betrouwbare ondersteuning van de programmatuur die op het platform draait.
Oordeel
Buiten scope.
U/PW.02 Webprotocollen

Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Oordeel

Geen bevindingen.

U/PW.03 Webserver

Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Oordeel

Zie bevindingen 3, 4, 5 en 6.

U/PW.04 Isolatie van processen/bestanden

Beperk de impact bij misbruik van processen.

Oordeel

Buiten scope.

U/PW.05 Toegang tot beheermechanismen

Voorkomen van misbruik van beheervoorzieningen.

Oordeel

Geen bevindingen.

U/PW.06 Platform-netwerkkoppeling

Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Oordeel

Geen bevindingen.

U/PW.07 Hardening van platformen

Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Oordeel

Buiten scope.

U/PW.08 Platform- en webserverarchitectuur

Een platform bieden dat een betrouwbare verwerking garandeert.

Oordeel

Buiten scope.

U/NW.01 Operationeel beleid voor netwerken

Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Oordeel

Buiten scope.

U/NW.02 Beschikbaarheid van netwerken

Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Oordeel

Buiten scope.

U/NW.03 Netwerkzonering

Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Oordeel

Buiten scope.

U/NW.04 Protectie- en detectiefunctie

Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Oordeel

Buiten scope.

U/NW.05 Beheer- en productieomgeving

Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Oordeel

Buiten scope.

U/NW.06 Hardening van netwerken
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.
Oordeel
Geen bevindingen.
U/NW.07 Netwerktoegang tot webapplicatie
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.
Oordeel
Buiten scope.
U/NW.08 Netwerkarchitectuur
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.
Oordeel
Buiten scope.

Beheersingsdomein

C.01 Servicemanagementbeleid
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
Oordeel
Buiten scope.
C.02 Compliancemanagement
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.
Oordeel
Buiten scope.
C.03 Vulnerability-assessments
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.
Oordeel
Buiten scope.
C.04 Penetratietestproces
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).
Oordeel
Buiten scope.
C.05 Technische controlefunctie
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.
Oordeel
Buiten scope.
C.06 Logging
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.
Oordeel
Buiten scope.
C.07 Monitoring

Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Oordeel	

Buiten scope.

C.08	**Wijzigingenbeheer**

Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Oordeel	

Buiten scope.

C.09	**Patchmanagement**

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Oordeel	

Geen bevindingen.

C.10	**Beschikbaarheidbeheer**

Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Oordeel	

Buiten scope.

C.11	**Configuratiebeheer**

Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Oordeel	

Buiten scope.

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Er zijn geen nieuwe bevindingen in deze categorie.

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie-specifieke Invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beinvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 *Open doorverwijzing*

Omschrijving
De server stuurt de gebruiker door naar een URL die gebaseerd is op ongevalideerde invoer.

Bedreiging
Het is mogelijk gebruikers door te sturen naar een zelfgekozen URL of een URL binnen een ander domein. Een aanvaller kan zo gebruikers naar een kwaadwillende webapplicatie laten doorsturen door de legitieme server. De doorverwijzing wordt door de browser van de gebruiker automatisch gevolgd. Hierdoor kan het voor de eindgebruiker moeilijk zijn de juiste vertrouwensbeslissing te nemen, zeker als de aanvaller voor zijn kwaadwillende webapplicatie een domeinnaam kiest die lijkt op die van de legitieme applicatie.
Een gebruiker heeft bijvoorbeeld een zekere mate van vertrouwen in Sogeti en ontvangt de volgende link via de mail:
https://www.sogeti.nl?redirect=http://www.sogetti.nl
Deze link wijst naar de website van Sogeti en omdat de gebruiker Sogeti vertrouwt klikt hij deze de link aan. Als deze kwetsbaarheid van toepassing is zal de webapplicatie een doorverwijzing sturen naar de browser van de gebruiker met daarin de opdracht om naar http://www.sogetti.nl (met dubbel 't') te gaan.

Aanbeveling
Sta alleen doorverwijzingen toe naar pagina's binnen het domein van de applicatie of naar pagina's en domeinen die op een whitelist staan.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
1	Onbekend	Midden	Midden	Laag

Betreffende Hosts
balie-a4.digid.nl

Details

Het is mogelijk om de x-forwarded-host waarde aan te passen naar sogeti.nl waardoor we vervolgens geredirect worden naar sogeti.nl zie highlight, request en reponse.

Request:

```
GET / HTTP/1.1
Host: balie-a4.digid.nl
X-Forwarded-Host: sogeti.nl
Content-Length: 8
```

Response:

```
HTTP/1.1 302 Found
Date: Wed, 18 Nov 2020 13:07:19 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Location: https://sogeti.nl/saml/sp/eherkenning_authentication
Cache-Control: no-cache
{...TRUNCATED...}
<html><body>You are being <a
href="https://sogeti.nl/saml/sp/eherkenning_authentication">redirected
</a>.</body></html>
```

3.9.2 *Host-header aanval*

Omschrijving

Een aanvaller kan een Host-header manipuleren en versturen. De waarde van de header wordt vervolgens gebruikt door de applicatie.

Bedreiging

Doordat de waarde van de Host-header wordt overgenomen door de applicatie kan een aanvaller bijvoorbeeld links op een pagina aanpassen of externe scripts laden.

Aanbeveling

Zorg ervoor dat de applicatie een vaste waarde gebruikt in plaats van de Host-header. Daarnaast zou er een foutmelding moeten worden getoond als de client een onbekende host header verstuurd.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
2	Onbekend	Midden	Midden	Laag

Betreffende Hosts

digidbeheer-a4.digid.nl

Details

Het is mogelijk om de host waarde aan te passen naar sogeti.nl waardoor we vervolgens geredirect worden naar sogeti.nl zie highlight, request en reponse.

Request:

```
GET /?cachebust=1605709516.21 HTTP/1.1
Host: sogeti.nl
Cache-Control: no-cache
[.. truncated ..]
```

Response:

```
HTTP/1.0 302 Found
Location: https://sogeti.nl/?cachebust=1605709516.21
Connection: close
Content-Length: 0
```

3.9.3 *Information disclosure – Versie informatie*

Omschrijving
Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
3	Onbekend	Zeer Laag	Zeer Hoog	Zeer Laag

Betreffende Hosts
app-a4.digid.nl
mijn.a4.digid.nl
was-a4.digid.nl

Details
De host geeft informatie vrij over de gebruikte software. Kwaadwillenden kunnen deze informatie
gebruiken in (toekomstige) aanvallen, bijvoorbeeld wanneer zero-day kwetsbaarheden bekend worden.
Request:

```
GET /assets/application-
128ced700935dadda60639e1ba5cd0ef9b835faa853f1bd2a749246a142a6a1b.js
HTTP/1.1
Host: app-a4.digid.nl
```

Response:

```
HTTP/1.1 200 OK
Date: Tue, 17 Nov 2020 13:46:27 GMT
{...TRUNCATED...}
1024
[redacted]

TRUNCATED...}
```

3.9.4 *Information disclosure - Versie informatie*

Omschrijving
Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
4	Onbekend	Zeer Laag	Zeer Hoog	Zeer Laag

Betreffende Hosts
app-a4.digid.nl
mijn.a4.digid.nl
was-a4.digid.nl

Details
De host geeft informatie vrij over de gebruikte software. Kwaadwillenden kunnen deze informatie
gebruiken in (toekomstige) aanvallen, bijvoorbeeld wanneer zero-day kwetsbaarheden bekend worden.
Request:

```
GET /assets/application-
128ced700935dadda60639e1ba5cd0ef9b835faa853f1bd2a749246a142a6a1b.js
HTTP/1.1
Host: app-a4.digid.nl
```

Response:

```
HTTP/1.1 200 OK
Date: Tue, 17 Nov 2020 13:46:27 GMT
{...TRUNCATED...}
102g
{...TRUNCATED...}
```

3.9.5 *Information disclosure – Versie informatie*

Omschrijving
Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5	Onbekend	Zeer Laag	Zeer Hoog	Zeer Laag

Betreffende Hosts
digidbeheer-a4.digid.nl

Details
De host geeft informatie vrij over de gebruikte software. Kwaadwillenden kunnen deze informatie
gebruiken in (toekomstige) aanvallen, bijvoorbeeld wanneer zero-day kwetsbaarheden bekend worden.
Request:

```
GET /assets/application-
b868d877c357f7a28eabbb872f4d272131eb31cf00a5dda3b9e7f42cbde64dc1.js
HTTP/1.1
Host: digidbeheer-a4.digid.nl
```

Response:

```
HTTP/1.1 200 OK
102g
[redacted]
(...TRUNCATED...)
```

3.9.6 *Information disclosure – Versie informatie*

Omschrijving

Systemen geven zelf vaak onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaard instelling van de software.

Bedreiging

Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling

Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versie-informatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

ID	Jira nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
6	Onbekend	Zeer Laag	Zeer Hoog	Zeer Laag

Betreffende Hosts

digidbeheer-a4.digid.nl

Details

De host geeft informatie vrij over de gebruikte software. Kwaadwillenden kunnen deze informatie
gebruiken in (toekomstige) aanvallen, bijvoorbeeld wanneer zero-day kwetsbaarheden bekend worden.

Request:

```
POST /admin_reports?jpYo={...TRUNCATED...} HTTP/1.1
Host: digidbeheer-a4.digid.nl
Accept-Encoding: gzip, deflate
```

Response:

```
HTTP/1.1 400 Bad Request
{...TRUNCATED...}>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
</body>
</html>
{...TRUNCATED...}
```

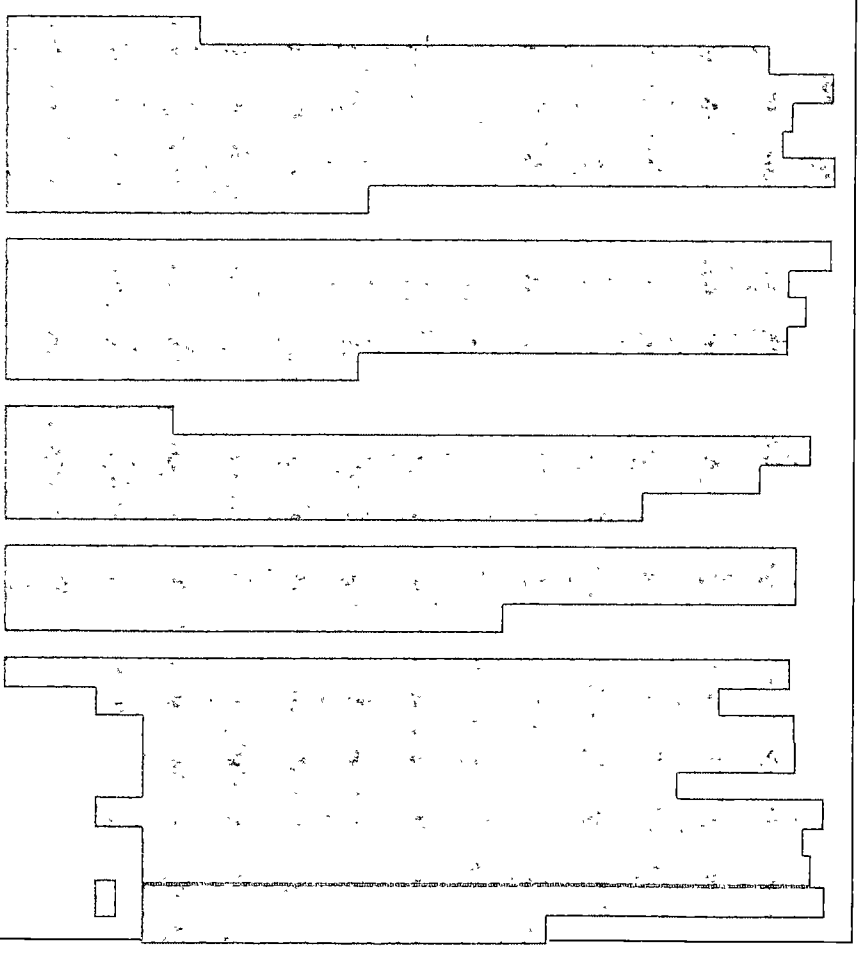
4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Cyberregistratie

Datum	7 januari 2016	Stand-by manager	10.2e
Tijd van	8.55	Tijd tot	9.03
Tijd van	9.03	Tijd tot	9.07
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	■ Calamiteitenmanager ■ Juridische zaken / IB ■ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Maatregelen	■ 10.2g ☐ Anders.....		
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		



Opslaan als document met prefix:

Call nummer - Registratie Datum.doc

Cyberregistratie

Datum	4-2-2016	Stand-by manager	10.2e
Tijd van	23:00	Tijd tot	23:10
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC	
Onbeschikbaarheid	☐ Ja ■ Nee	☐ Taskforce Ddos ☐ Taskforce DigiStorm	
Primair doel aanval	■ DigiD ☐ MijnOverheid DigiD machtigen ☐ Weet niet / onduidelijk	☐ Anders	
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

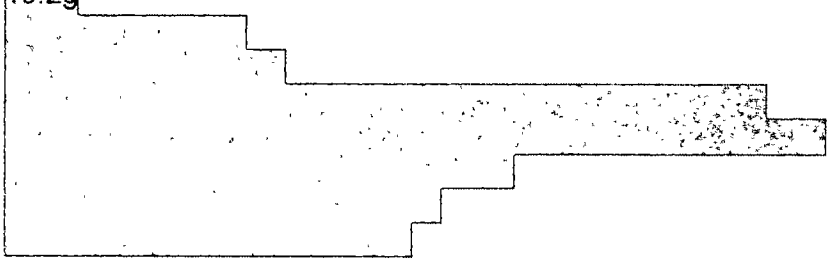
Cyberregistratie

Datum	17-2-2016	Stand-by manager	10.2e
Tijd van	13:20	Tijd tot	13:45
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		■ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ DigiD Machtigen ☐ MijnOverheid ☐ Digipoort ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	13042016	Stand-by manager	10.2e
Tijd van	11:49	Tijd tot	12:13
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		**X Calamiteitenmanager** **X Juridische zaken** **X NCSC** ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	☐ DigiD ☐ MijnOverheid ☐ --Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g 		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	14-5-2016	Stand-by manager	10.2e
Tijd van	12:31	Tijd tot	12:43
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders Deze melding kwam 3 dagen later pas binnen. Niet het standaard proces gevolgd. Alleen registratie van DDos gedaan	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	X DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	16-9-2016	Stand-by manager	10.2e
Tijd van	17:55	Tijd tot	18:28
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		■ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	13-10-2016	Stand-by manager	10.2e
Tijd van	16:05	Tijd tot	
Tijd van		Tijd tot	
Geïnformeerd door	☐ 10.2g ☐ Leverancier ..... ☐ Intern Logius ■ 10.2g	Geïnformeerd	
Maatregelen	☐ 10.2g ☐ Anders.....	■ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ■ Anders : Fraude Team	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	☐ DigiD ☐ MijnOverheid ☐ Anders ..... ■ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Cyberregistratie

Datum	31.10.2016	Stand-by manager	10.2e
Tijd van	28/10 – 17.41	Tijd tot	28/10 – 17.43
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	31.10.2016	Stand-by manager	10.2e
Tijd van	31-10-2016 17:29	Tijd tot	31-10-2016 17:47
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

	10.2g

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	04.11.2016	Stand-by manager	10.2e
Tijd van	04.11.2016 11.42	Tijd tot	04.11.2016 11.43
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

	10.2g

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ○ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
29-12-2016 om 11:00 uur	◉ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☒ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☒ Overig:	Fraudeteam

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
405883	10.2g	Nee	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
16-11-2016 om 17:19 uur	16-11-2016 om		18-11-2016 om 12:54 uur
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☒ Communicatie ☒ JZ ☒ SM	
☒ Anders:	Fraudeteam		

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:
Beveiligingsincident

Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ○ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ○ Nee	
Extern gecommuniceerd?	○ Ja ○ Nee	
Incidentproces gevolgd?	○ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ○ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	○ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Actiepunten:

10.2g

Opmerkingen algemeen:

10.2g

Verzenden via e-mail

Cyberregistratie

Datum	24-1-2017	Stand-by manager	10.2e
Tijd van	21:37u	Tijd tot	21:39u
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	29-1-2017	Stand-by manager	10.2e
Tijd van	20:00	Tijd tot	20:15
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		☐ Calamiteitenmanager ■ Juridische zaken ■ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	06-02-2017	Stand-by manager	10.2e
Tijd van	21:37 en 21:41	Tijd tot	21:41
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		☐ Calamiteitenmanager ☐ Juridische zaken ☐ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	☐ Dig ☐ MijnOverheid ■ Anders : DigiPoort PP ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	12-02-2017	Stand-by manager	10.2e
Tijd van	19:29	Tijd tot	19:37
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		■ Calamiteitenmanager ■ Juridische zaken ■ NCSC ☐ Taskforce Ddos ☐ Taskforce DigiStorm ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	26-02-2017	Stand-by manager	10.2e
Tijd van	0:51	Tijd tot	0:59
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	■ Calamiteitenmanager ☐ C&RM Jurist ☐ C&RM CISO ■ NCSC ☐ Anders	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	17 april 2017	Stand-by manager	10.2e
Tijd van	20.40 uur	Tijd tot	20.45 uur
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius	Geïnformeerd	
Maatregelen	■ 10.2g ☐ Anders.....	☐ Calamiteitenmanager ■ C&RM Jurist ■ C&RM CISO ■ NCSC ☐ Anders	
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Cyberregistratie

Datum	18-4-2017	Stand-by manager	10.2e
Tijd van	20:26	Tijd tot	20:54 (unban)
Tijd van		Tijd tot	
Geïnformeerd door	☐ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd ■ Calamiteitenmanager ☐ C&RM Jurist ☐ C&RM CISO ☐ NCSC ☐ Anders .....
Maatregelen	■ 10.2g ■ 10.2g		
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	8-8-2017	Stand-by manager	10.2e
Tijd van	17:40	Tijd tot	17:50
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd ■ Calamiteitenmanager ☐ C&RM Jurist ■ C&RM CISO ■ NCSC ☐ Anders .....
Maatregelen	■ 10.2g ☐ Anders.....		
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	☐ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	20-11-2017	Stand-by manager	10.2e
Tijd van	22:52	Tijd tot	23:02
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		■ Calamiteitenmanager ☐ C&RM Jurist ☐ C&RM CISO ☐ NCSC ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	23-11-2017	Stand-by manager	10.2e
Tijd van	07:34	Tijd tot	07:37
Tijd van		Tijd tot	
Geïnformeerd door	■ 10.2g ☐ Leverancier ..... ☐ Intern Logius		Geïnformeerd
Maatregelen	■ 10.2g ☐ Anders.....		■ Calamiteitenmanager ☐ C&RM Jurist ☐ C&RM CISO ☐ NCSC ☐ Anders .....
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Cyberregistratie

Datum	02-08-2017	Stand-by manager	10.2e
Tijd van	23:22	Tijd tot	23:32
Tijd van		Tijd tot	
Geïnformeerd door	☐ 10.2g ☐ ☐ Intern Logius		Geïnformeerd ■ Calamiteitenmanager ☐ C&RM Jurist ■ C&RM CISO ■ NCSC ☐ Anders .....
Maatregelen	■ 10.2g ☐ Anders.....		
Onbeschikbaarheid	☐ Ja ■ Nee		
Primair doel aanval	■ DigiD ☐ MijnOverheid ☐ Anders ..... ☐ Weet niet / onduidelijk		
Opmerkingen	10.2g		

Opslaan als document met prefix:

Call nummer – Product – beschrijving - registratie Datum.doc

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.0

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst	
☒ DigiD 4	☐ Digikoppeling
☐ eHerkenning	☐ Service Register
☐ DigiD Machtigen	☐ CPA Creatie
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	☒ Logius.nl / overheid.nl
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
27 januari 2017	( ) Ja (•) Nee

Aanwezig	
☒ Standbymanager	
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
415616	10.2g	☒ Dienstverlening onbeschikbaar	☐ Imago schade
☐ Anders:			
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
10 januari 2017	onbekend		10 januari 2017
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:			
☐ Beveiligingsincident	☒ Storing Infrastructuur	☐ Storing Software	☐ Imago schade
☐ Anders:			

Rootcause:	
☐ Rootcause aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
Juridische Zaken geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/ kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
nvt
Actiepunten:
nvt
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☐ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
nvt	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
417958	Logius	Nee	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
18-01-2017 15:52	18-01-2017 15:52	nvt	19-01-2017
Standbymanager:	Calamiteiten manager:	Specialisten:	
		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:	zie boven	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
421089	10.2g	Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
30-01-2017 9:48	29-01-2017 20:00		29-01-2017 20:15
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	zie boven

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	( ) Ja ( ) Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	Ketenbeheer

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
421969		Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
09-02-2017 13:20	09-02-2017 13:20		09-02-2017 14:00
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☒ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update ☐ Hardware Update ☐ Herstart Server ☐ Backup Procedure ☐ Database Wijziging	☒ Anders:	10.2g
Aanpassingen:		
☐ SLA / DAP Wijziging ☐ Incidenthandboek ☐ Productkaart ☐ Mailplus ☐ Clientele	☐ Procedure:	
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	◉ Ja ○ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	extern
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	( ) Ja (•) Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	Ketenbeheer

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
422512		Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
08-02-2017 17:43	19:30		08-02-2017 19:49
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	zie boven

Oorzaak:

☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☒ Externe Informatiebron

10.2g

☐ Software Update	☒ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☒ Productkaart		
☐ Mailplus		
☐ Clientele		
	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	10.2g

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	10.2g
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	Ketenbeheer

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
422514	10.2g	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
12-09-2017 10:30	23-1-2017 10:41		12-09-2017 10:41
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:
10.2g

Technische specificatie:	
☒ Technische specs aanwezig:	
☒ Oorzaak bekend:	10.2g

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☒ Procedure:	
☐ Incidenthandboek		
☒ Productkaart		
☐ Mailplus		
☐ Clientele		

Aangifte politie	○ Ja	◉ Nee

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja	○ Nee
C&RM geïnformeerd?	○ Ja	◉ Nee
Informatie Beveiliging geïnformeerd?	○ Ja	◉ Nee
Extern gecommuniceerd?	○ Ja	◉ Nee
Incidentproces gevolgd?	◉ Ja	○ Nee
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja	◉ Nee

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	10.2g
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	Ketenbeheer

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
422518		nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
12-02-2017 19:40	12-02-2017 19:30		12-02-2017 19:45
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	10.2g

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
422530	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
13-2-2017	13-2-2017 10:37 uur		
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe Informatiebron	
Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	10.2g

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
De samenwerking met TD
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
422704	10.2g	Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
13-2-2017	13-2-2017 18:34 uur		
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
geen
Actiepunten:
geen
Opmerkingen algemeen:
geen

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
424125	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
20-2-17 21.50	20-2-17 21.32		
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort incident:
10.2g

Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	zie boven

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10 2g
Verbeterpunten:
10 2g
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
425303	10.2g	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
27-2-17 08:10	27-2-17 08:00		27-2-17 voor 08:10
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	zie boven

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	10.2g
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	○ Ja ◉ Nee	N.v.t.

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	N.v.t.
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		N.v.t.

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
Nvt	( ) Ja (•) Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	Nvt

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
426994	10.2g	Nee	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
7-3-2017 10:28	Onbekend		8-3-2017
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☒ Anders:	Fraude team		

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	

Technische specificatie:	
☐ Technische specs aanwezig:	
☒ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☒ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10 2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	Nvt
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	◉ Ja ○ Nee	
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
Nvt	( ) Ja (•) Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	Nvt

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
427476	10.2g	Nee	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
8-3-2017 15:30	Bij bouw systeem	8-3-2017 15:30	8-3-2017 18:00
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g t		
Technische specificatie:		
☒ Technische specs aanwezig:		
☒ Oorzaak bekend:		
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☒ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure: -	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
433046	10.2g	Ja	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
3-4-2017 22:09	3-4-2017 22:09	nvt	nog niet
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☒ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe Informatiebron	
Oplossing:		
☒ Software Update ☐ Hardware Update ☐ Herstart Server ☐ Backup Procedure ☐ Database Wijziging	☐ Anders:	
Aanpassingen:		
☐ SLA / DAP Wijziging ☐ Incidenthandboek ☐ Productkaart ☐ Mailplus ☐ Clientele	☐ Procedure:	
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	nvt
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
434468		Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
10-4-2017 11:17	10-4-2017 11:04		10-4-2017 11:29
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☒ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	nvt
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
434531	Capgemini	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
12:32	10-4-17 12:09		10-4-17 12:20
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☒ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	ja
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	ja

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	◉ Ja ○ Nee	10.2g
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	nvt
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Business Impact:	
434636	10.2g	Ja	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
10-4-2017 16:54	10-4-2017 16:54		8-5-2017 0:00
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☒ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	10.2g
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	nvt
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	Standby manager 10.2e

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
435900	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
18-04-2017/ 16:15	18-04-2017/ 15:52		18-04-2017/ 15:54
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☒ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
Actiepunten:
10.2g
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
5-7-17 10:00 uur	◉ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☒ Woordvoerder	
☒ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☒ Overig:	Fraudeteam

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
437721	10.2g	Ja	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
28-4-17 om 8:20 uur	28-4-17 om 8:20 uur	N.v.t.	28-4-2017 om 11:30 uur
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☒ Communicatie ☐ JZ ☒ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	N.v.t.
☐ Oorzaak bekend:	10.2g

Oorzaak:

☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☒ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:

☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:

☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Actiepunten:

10.2g

Opmerkingen algemeen:

10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☒ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
439331	10.2g		
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
4-5-17 13:20	4 mei 2017	n.v.t.	n.v.t.
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		
Oorzaak:		
☒ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
7 juni 2017	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
442369	10.2g	Nee	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
16 mei 2017			23 mei 2017
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☐ Oorzaak bekend:		

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☒ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	n.v.t.
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: (•) Standbymanager ( ) Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	( ) Ja (•) Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
442599	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
24-5-2017 14:22	24-5-2017 14:22		24-5-2017 14:53
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	

Technische specificatie:	
☐ Technische specs aanwezig:	
☒ Oorzaak bekend:	10.2g

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☒ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		

Aangifte politie	○ Ja	◉ Nee

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja	○ Nee	
C&RM geïnformeerd?	○ Ja	◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja	◉ Nee	
Extern gecommuniceerd?	◉ Ja	○ Nee	
Incidentproces gevolgd?	◉ Ja	○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja	○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	◉ Ja ○ Nee	10.2g
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
442665	10.2g	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
23-5-2017 22:33	23-5-2017 22:10		23-5-2017 22:22
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☒ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☐ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☒ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
445483	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
12-6-17 12:25	12-6-2017 12:00		
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:

Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		

Aangifte politie	○ Ja	◉ Nee

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja	○ Nee	
C&RM geïnformeerd?	○ Ja	◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja	◉ Nee	
Extern gecommuniceerd?	◉ Ja	○ Nee	
Incidentproces gevolgd?	◉ Ja	○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja	○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ○ Standbymanager ◉ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
27-6-2017 14.00 uur	◉ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☒ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☒ Overig:	SM Leverancier (Marco Rits), Fraudeteam

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
446072	10.2g	Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
14-6-2017 om 18:00 uur	14-6-2017 om 18:00 uur	14-6-2017 om 22:15 uur	15-6-2017 om 08:00 uur
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:	10.2g	
☐ Oorzaak bekend:		

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	10.2g
☒ Incidenthandboek		
☒ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
MT geïnformeerd?	○ Ja ◉ Nee	Aanvullen 10.2e
C&RM geïnformeerd?	○ Ja ◉ Nee	Aanvullen 10.2e
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	Aanvullen 10.2e
Extern gecommuniceerd?	○ Ja ◉ Nee	Nvt
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van de calamiteit?	○ Ja ◉ Nee	10.2g

Evaluatiepunt		Toelichting:
Als deze calamiteit zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	Aanvullen 10.2e
Verliep de samenwerking met de Standbymanager goed?	◉ Ja ○ Nee	Aanvullen 10.2e
Welke tips heb je voor de Standbymanager in dezelfde situatie?		N.v.t.

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Actiepunten:

10.2g

Opmerkingen algemeen:

10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ○ Standbymanager ◉ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
3-7-2017 om 14:00 uur	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☒ Calamiteitenmanger	
☒ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☒ Overig:	Fraudeteam 10.2e

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
446072	10.2g	Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
14-6-2017 om 09:00 uur	14-6-2017 om 09:00 uur	14-6-2017 om 09:00 uur	
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	N.v.t.
☐ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☒ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	10.2g
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
MT geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van de calamiteit?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als deze calamiteit zich weer voordoet, pak je het dan anders aan?	◉ Ja ○ Nee	
Verliep de samenwerking met de Standbymanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Standbymanager in dezelfde situatie?		N.v.t.

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Actiepunten:

10.2g

Opmerkingen algemeen:

10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	standbymanager 10.2e

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
448116	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
27-6-17 19:19u	27 juni 2017 om 19.15u		27 juni 2017 om 20.16u
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			
Incident omschrijving:			
10.2g			

Oorzaak:

Soort Incident:	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☒ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☒ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ○ Nee

Aanwezig:	
☐ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
449104	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
4-7-17 11:22	4-7-17 11:17	n.v.t.	12.11 4-7-17
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☒ Communicatie ☐ JZ ☒ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☒ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe Informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
450314	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
10-7-17 16:44	9 juli 2017		10-7-17 17:40
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			
Incident omschrijving:			
10.2g			

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:		
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☒ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	10.2g
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	N.v.t.
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
Opmerkingen algemeen

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigID 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
13-07-2017 11:40	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
450571	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
12-7-17 08:00	12-7-17 01:11		12-7-17 01:16
Standbymanager:	Calamiteiten manager:	Speciallsten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☒ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
14 augustus 2017	◉ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☒ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☒ Overig:	Ketenbeheer, Communicatieadviseur

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
451275	10.2g	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
17 juli 201 09.40 uur	08.41 uur		18-08-2017 01:10
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e		☐ Dienstverlening ☒ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☒ Technische specs aanwezig:	10.2g
☒ Oorzaak bekend:	10.2g

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☒ Wijziging	☐ Externe informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☒ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aanglfte politie	○ 10.2g ◉	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ ☐ ○ ☐	
C&RM geïnformeerd?	○ ☐ ◉ ☐	
Informatie Beveiliging geïnformeerd?	○ ☐ ◉ ☐	
Extern gecommuniceerd?	◉ ☐ ○ ☐	10.2g
Incidentproces gevolgd?	◉ ☐ ○ ☐	10.2g
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ ☐ ○ ☐	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Actiepunten:

10.2g

Opmerkingen algemeen:

10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
31-7-2017	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
452537	10.2g	Ja	Productverstoring
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
24-7-2017 20:23	24-7-2017		25-7-2017 14:40
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☒ Anders:	10.2g		

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☒ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt:		Toelichting:
Calamiteitenmanager geïnformeerd?	○ Ja ◉ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
28-7-2017 13:30	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
453026	10.2g		Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
26-7-2017 20:04	26-07-2017 20:00		26-7-2017 20:40
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
10.2g	
Technische specificatie:	
☐ Technische specs aanwezig:	
☒ Oorzaak bekend:	10.2g

Oorzaak:	
☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☒ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe Informatiebron

Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	◉ Ja ○ Nee	10.2g
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
7 augustus 2017	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☒ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☒ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
453116	10.2g	Ja	Dienstverlening onbeschikbaar
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
27-7-2017 10:37	27-7-2017 10:37		27-7-2017 10:57
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:	10.2g	
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☒ Technische Storing	☐ Onderhoud Leverancier	
☒ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	○ Ja ◉ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:

10.2g

Verbeterpunten:

10.2g

Acticpunten:

10.2g

Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.1

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD 4	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort OTP	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
23-08-2017	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☐ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☐ Overig:	

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
453950	10.2g	Nee	
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
02-08-2017 23:45	02-08-2017 23:22		02-08-2017 23:32
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☐ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:	
Technische specificatie:	
☐ Technische specs aanwezig:	
☐ Oorzaak bekend:	zie boven

Oorzaak:

☐ Technische Storing	☐ Onderhoud Leverancier
☐ Software Storing	☐ (poging) Systeem Hacking
☐ Fout leverancier	☐ (poging) Diefstal gegevens
☐ Update	☐ (poging) Phishing, Malware, Virus
☐ Wijziging	☐ Externe informatiebron

Oplossing:

☐ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		

Aanpassingen:

☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	◉ Ja ○ Nee	
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	
Extern gecommuniceerd?	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	○ Ja ◉ Nee	
Verliep de samenwerking met de Calamiteitenmanager goed?	◉ Ja ○ Nee	
Welke tips heb je voor de Calamiteitenmanager in dezelfde situatie?		

Evaluatie

Wat ging goed:
Verbeterpunten:
Actiepunten:
Opmerkingen algemeen:

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.2

RoL: ◉ Standbymanager ○ Calamiteitenmanager

Dienst:	
☒ DigiD	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigiD Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort H&T	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
	○ Ja ◉ Nee

Aanwezig:	
☒ Standbymanager	☐ Procesbegeleider Crisismanagement
☐ Calamiteitenmanger	
☒ Woordvoerder	
☐ Servicecentrum	
☒ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	Fraudeteam, KB MO, KB DigiD

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
456467			Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgeloct
23-8-17 / 17:07	23 augustus 2017		25 augustus 2017
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☒ Communicatie ☒ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☐ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☒ Externe Informatiebron	
Oplossing:		
☐ Software Update	☒ Anders:	10.2g
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	
☐ Incidenthandboek		
☐ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
Calamiteitenmanager geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	◉ Ja ○ Nee	
Informatie Beveiliging geïnformeerd?	○ Ja ◉ Nee	10.2g ?
Extern gecommuniceerd?	○ Ja ◉ Nee	
Belastingdienst CIE geïnformeerd ? *Zo ja, CIE nummer noteren bij 'Toelichting'	○ Ja ◉ Nee	
Incidentproces gevolgd?	◉ Ja ○ Nee	

Evaluatiepunt		Toelichting:
Als dit incident zich weer voordoet, pak je het dan anders aan?	(•) Ja ( ) Nee	10.2g
Verliep de samenwerking met de Calamiteitenmanager goed?	(•) Ja ( ) Nee	
Had je voldoende informatie/kennis voor het oplossen van het incident?	(•) Ja ( ) Nee	

Evaluatie

Wat ging goed:
10.2g
Verbeterpunten:
10.2g
Actiepunten:
10.2g
Opmerkingen algemeen:
10.2g

Verzenden via e-mail

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatieformulier Incident / Calamiteit

Versie 1.2

RoL: ○ Standbymanager ◉ Calamiteitenmanager

Dienst:	
☒ DigiD	☐ Kantoorautomatisering
☐ eHerkenning	☐ Diginetwerk
☐ DigID Machtigen	☐ Managed Services
☐ MijnOverheid	☐ Digimelding
☐ Digipoort H&T	☐ Digilevering
☐ Digipoort PI	
☐ Overig:	
Evaluatie Datum / Tijdstip	Evaluatie leverancier aanwezig
31 augustus 2017	◉ Ja ○ Nee

Aanwezig:	
☒ Standbymanager	☒ Procesbegeleider Crisismanagement
☒ Calamiteitenmanger	
☒ Woordvoerder	
☐ Servicecentrum	
☐ Juridische Zaken	
☐ Informatie Beveiliging	
☐ Servicemanager	
☒ Overig:	Ketenbeheer DigiD

Incident/Calamiteit informatie:

Clientele nummer:	Leverancier:	Bussines Impact	
456880	10.2g	Ja	Informatie beveiliging
Datum / tijd 1ste Melding	Datum / tijd ontstaan	Datum / tijd Calamiteit	Datum / tijd Opgelost
23-8-1716:45	24-8-17 10:15	24-8-17 14:45	26-08-2017 06.49 uur
Standbymanager:	Calamiteiten manager:	Specialisten:	
10.2e	10.2e	☒ Dienstverlening ☐ Communicatie ☐ JZ ☐ SM	
☐ Anders:			

Incident omschrijving:

10.2g

Oorzaak:

Soort Incident:		
10.2g		
Technische specificatie:		
☐ Technische specs aanwezig:		
☒ Oorzaak bekend:	10.2g	
Oorzaak:		
☐ Technische Storing	☐ Onderhoud Leverancier	
☐ Software Storing	☐ (poging) Systeem Hacking	
☒ Fout leverancier	☐ (poging) Diefstal gegevens	
☐ Update	☐ (poging) Phishing, Malware, Virus	
☐ Wijziging	☐ Externe informatiebron	
Oplossing:		
☒ Software Update	☐ Anders:	
☐ Hardware Update		
☐ Herstart Server		
☐ Backup Procedure		
☐ Database Wijziging		
Aanpassingen:		
☐ SLA / DAP Wijziging	☐ Procedure:	10.2g
☐ Incidenthandboek		
☒ Productkaart		
☐ Mailplus		
☐ Clientele		
Aangifte politie	○ Ja ◉ Nee	

Evaluatiepunt		Toelichting:
MT geïnformeerd?	◉ Ja ○ Nee	
C&RM geïnformeerd?	◉ Ja ○ Nee	10.2g
Informatie Beveiliging geïnformeerd?	◉ Ja ○ Nee	10.2g
Extern gecommuniceerd?	◉ Ja ○ Nee	10.2g
Belastingdienst CIE geïnformeerd ? *Zo ja, CIE nummer noteren bij 'Toel chting'	○ Ja ◉ Nee	
Had je voldoende informatie/kennis voor het oplossen van de calamiteit?	◉ Ja ○ Nee	