Auditdienst Rijk
Ministerie van Financiën

DEPARTEMENTAAL VERTROUWELIJK

Rapport van bevindingen - Beveiligingsonderzoek Raad van State

Colofon

Titel	Rapport van bevindingen – Beveiligingsonderzoek Raad van State
Uitgebracht aan	[redacted] Hoofd IT-beheer Raad van State
Contactpersoon	[redacted] Technisch beheerder Raad van State
Bijlagen	4
Datum	23 juli 2015
Status	Definitief
Kenmerk	ADR/2015/945

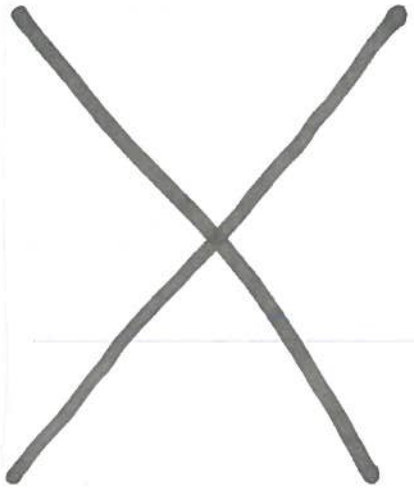
10,2°,e

10,2°,e

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1	**Managementsamenvatting**	**6**
2	**Inleiding**	**7**
2.1	Algemeen	7
2.2	Opdrachtomschrijving	7
2.2.1	Penetratietest (pentest)	8
2.2.2	Vulnerability assessment en blackbox scan	8
2.3	Aanpak en werkwijze	9
2.4	Verantwoording	10
2.5	Verspreidingskring rapportage	10
2.6	Leeswijzer	10
3	**Bevindingen en aanbevelingen**	**11**
3.1	Inleiding	11
3.2	Bestands- en directory toegang	12
3.3	Controle van invoervariabelen	12
3.3.1		12
3.4		13
3.4.1		13
3.4.2		13
3.5		14
3.5.1		14
3.5.2		14
3.5.3		15
3.6		15
3.6.1		15
3.6.2		17
3.6.3		17
3.6.4		18
3.6.5		18
3.6.6		19
4	**Ondertekening**	**20**
Bijlage 1 – Bevindingen per DigiD richtlijn		**21**
Bijlage 2 – Toelichting risicobeschrijving		**23**
Bijlage 3 – Gedetailleerde fasering onderzoek		**24**



1 Managementsamenvatting

Inleiding
In deze managementsamenvatting kunt u de belangrijkste bevindingen lezen uit het onderzoek naar de beveiliging van vier webapplicaties van de Raad van State (RvS). Deze webapplicaties zijn beschikbaar via

- digitaalloket.raadvanstate.nl
- localbox.raadvanstate.nl
- extranet.raadvanstate.nl
- remote.raadvanstate.nl

Voor het onderzoek naar de bovenstaande webapplicaties is de volgende onderzoeksvraag geformuleerd:

- *Welke kwetsbaarheden bevatten de te onderzoeken webapplicaties en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd? (**pentest**)*

Voor de webapplicatie digitaalloket.raadvanstate.nl zijn ten behoeve van de DigiD assessment 2014 de volgende aanvullende onderzoeksvragen geformuleerd:

- *Welke kwetsbaarheden bevat de infrastructuur van de te onderzoeken webapplicaties en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd? (**vulnerability assessment**)*
- *Welke kwetsbaarheden bevatten de programmacode en het applicatieplatform van de te onderzoeken webapplicatie en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd? (**blackbox scan**)*

De uitvoering heeft plaatsgevonden volgens een vooraf met medewerkers van RvS besproken plan van aanpak. De webapplicaties zijn met behulp van geautomatiseerde hulpmiddelen onderzocht op kwetsbaarheden[1] in vijf categorieën: bestands- en directory toegang, controle van invoervariabelen, component afhankelijke kwetsbaarheden, beveiliging van inlogvoorzieningen en de beveiliging van gegevenstransport. Het conceptrapport is d.d. 1 juni 2015 per mail afgestemd met de opdrachtgever van het onderzoek.

Belangrijkste bevinding

Gebruik van SSLv2 en SSLv3
Voor de applicatie op extranet.raadvanstate.nl wordt gebruik gemaakt van een SSL-certificaat voor het opzetten van een beveiligde verbinding.

De details van de gevonden kwetsbaarheden zijn terug te vinden in hoofdstuk 3.

[1] De OWASP top 10 kwetsbaarheden zijn ondermeer onderzocht met de op moment van onderzoek bekende testmethodiek. OWASP staat voor Open Web Application Security Project en is een internationaal initiatief omtrent kennisuitwisseling over de beveiliging van webapplicaties.

2 Inleiding

2.1 Algemeen

Als gevolg van geconstateerde 'lekken in een aantal gemeentelijke websites' (2011) heeft de politiek aandacht voor ICT-beveiliging van webapplicaties. In een brief van 2 februari 2012 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de Tweede Kamer geïnformeerd dat organisaties die gebruik maken van DigiD jaarlijks hun ICT-beveiliging dienen te toetsen in een ICT-beveiligingsassessment (hierna: DigiD assessment) op basis van door BZK vastgestelde normering.

De RvS is onafhankelijk adviseur van de regering over wetgeving en bestuur en hoogste algemene bestuursrechter van het land. Voor het uitvoeren van deze taak wordt gebruik gemaakt van o.a. webapplicaties. De webapplicatie 'Digitaal Loket' (digitaalloket.raadvanstate.nl) biedt burgers de mogelijkheid om digitaal te procederen tegen een beslissing van een bestuursorgaan of tegen een uitspraak van een rechtbank. Hiervoor kunnen burgers inloggen via DigiD en een digitaal formulier invullen en documenten versturen.

In het kader van de DigiD assessment 2014 heeft RvS aan de Auditdienst Rijk (ADR) gevraagd om de uitvoering van de pentest, vulnerability assessment (security scan) en blackbox scan op zich te nemen voor de webapplicatie van het 'Digitaal Loket'. De ADR heeft in dit kader een onderzoek uitgevoerd naar de mogelijke kwetsbaarheden rondom de webapplicatie en in de onderliggende infrastructuur van het 'Digitaal Loket'.

Naast het hiervoor genoemde 'Digitaal Loket' zijn drie andere webapplicaties van de RvS meegenomen in dit beveiligingsonderzoek. Het betreft een applicatie die online bestandsopslag voor geregistreerde gebruikers aanbiedt (localbox.raadvanstate.nl), een webapplicatie die gemeentes de mogelijkheid biedt om plankaarten digitaal aan te bieden (extranet.raadvanstate.nl) en tot slot een webapplicatie die mobile devices van de RvS toegang tot mail en en agenda biedt (remote.raadvanstate.nl). [redacted] 10,1°,b+ 10,1°,c+ 10,2°,g

In de nu voorliggende rapportage zijn de bevindingen van het hierboven genoemde onderzoek beschreven.

2.2 Opdrachtomschrijving

Op 29 januari 2015 heeft een gesprek plaatsgevonden met de heer [redacted] namens RvS en [redacted] namens de ADR. 10,2°,e
In dit gesprek is ondermeer gesproken over de afloop van de DigiD assessment 2013 en planning van de DigiD assessment 2014. Daarnaast is specifiek ingegaan op de uitvoering van de pentest, de vulnerability assessment (security scan) en de blackbox scan.
Voor 2014 heeft RvS aan de ADR gevraagd om de uitvoering van de pentest, vulnerability assessment en blackbox scan op de webapplicatie "Digitaal Loket" op zich te nemen.
Vervolgens is voor dit onderzoek een opdrachtvoorstel (Beveiligingsonderzoek RvS met kenmerk ADR/2015/558) namens de ADR uitgestuurd.

De heer [redacted] is namens de RvS de contactpersoon voor dit onderzoek geweest. 10,2°,e

2.2.1 *Penetratietest (pentest)*

Het hoofd IT-beheer van RvS heeft de ADR verzocht een pentest uit te voeren op een viertal webapplicaties van RvS. Het betreft de webapplicaties op

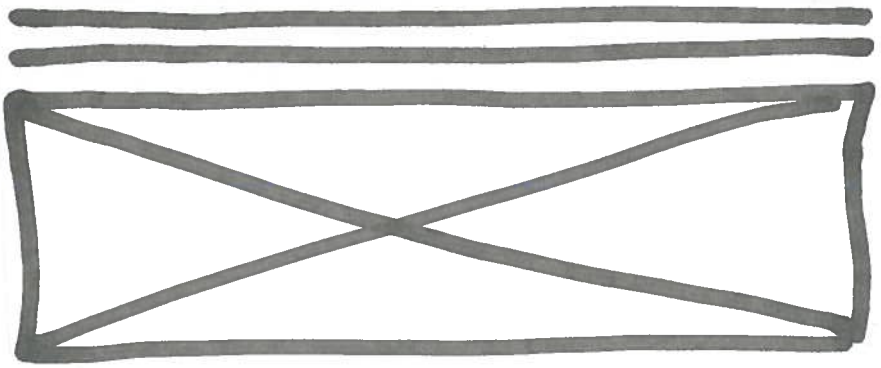
- digitaalloket.raadvanstate.nl
- localbox.raadvanstate.nl
- extranet.raadvanstate.nl
- remote.raadvanstate.nl

Doelstelling van de pentest was om inzicht te geven in de (mogelijke) kwetsbaarheden van de vier genoemde webapplicaties. De onderzoeksvraag was hiertoe als volgt geformuleerd:

- *Welke kwetsbaarheden bevatten de te onderzoeken webapplicaties en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd?*

De pentest heeft zich gericht op de aanwezigheid (het bestaan) van technische maatregelen om de integriteit en exclusiviteit[2] te waarborgen op een met de opdrachtgever bepaald tijdstip in de onderzoeksperiode.
De maatregelen zijn afkomstig uit internationale best practices op het gebied van informatiebeveiliging bij webapplicaties. De aanwezigheid van maatregelen hebben wij getest met behulp van onze testprogramma's. In de volgende paragraaf wordt hier gedetailleerder op in gegaan.

In de pentest is nagegaan of het mogelijk was de functionaliteit van de webapplicaties te misbruiken of binnen te dringen in de applicaties of de onderliggende systemen, zoals de database(s). Het onderzoek heeft [redacted]



10,1°,b +
10,1°,c +
10,2°,g

Wij hebben ons onderzoek uitgevoerd in de productieomgeving en hebben gebruik gemaakt van de aanwijzingen in het document 'Aanbevelingen en criteria penetratietest', versie 1.0 d.d. 21 februari 2012, ten behoeve van de DigiD assessment dat is opgesteld door BZK. Dit was van belang voor de webapplicatie digitaalloket.raadvanstate.nl.

2.2.2 *Vulnerability assessment en blackbox scan*

Het hoofd IT-beheer van RvS heeft de ADR verzocht om voor de webapplicatie van het 'Digitaal Loket' naast een pentest ook een vulnerability assessment en blackbox scan uit te voeren ten behoeve van de DigiD assessment 2014.

Doelstelling van de vulnerability assessment was om inzicht te geven in de (mogelijke) kwetsbaarheden van de infrastructuur van de webapplicatie 'Digitaal Loket' van de RvS.

[2] Onder integriteit verstaan wij de mate waarin het object in overeenstemming is met de afgebeelde werkelijkheid. De mate van getroffen maatregelen onderzoeken wij om na te gaan in hoeverre de juistheid en volledigheid van gegevens zijn gewaarborgd. Onder exclusiviteit verstaan wij de mate waarin uitsluitend geautoriseerde personen via geautoriseerde procedures gebruikmaken van IT-processen. Deze definities zijn afkomstig uit Geschrift No.1 van NOREA, de beroepsorganisatie van IT-auditors.

Doelstelling van de blackbox scan was om ontwikkelaars inzicht te geven in (mogelijke) kwetsbaarheden in de webapplicatie (programmacode en applicatieplatform), exclusief de infrastructuur.

De onderzoeksvragen waren hiertoe als volgt geformuleerd:

- *Welke kwetsbaarheden bevat de infrastructuur van de te onderzoeken webapplicaties en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd?*
- *Welke kwetsbaarheden bevatten de programmacode en het applicatieplatform van de te onderzoeken webapplicatie en hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd?*

NB. Tussen de pentest en de blackbox scan zit veel overlap. De pentest wordt echter veelal extern uitgevoerd op de webapplicatie zoals deze via Internet benaderbaar is, de blackbox scan wordt normaliter intern door ontwikkelaars direct op de webapplicatie uitgevoerd.

De vulnerability assessment en blackbox scan richtten zich op de aanwezigheid (het bestaan) van maatregelen om de integriteit en exclusiviteit[3] te waarborgen op een in overleg met de opdrachtgever bepaald tijdstip in de onderzoeksperiode. De maatregelen zijn afkomstig uit internationale best practices op het gebied van informatiebeveiliging op webapplicaties en infrastructuur. De aanwezigheid van maatregelen onderzoeken wij met behulp van diverse testprogramma's (tools).

Het object van onderzoek zijn de webapplicatie 'Digitaal Loket' en de onderliggende infrastructurele componenten.

Wij hebben door middel van (geautomatiseerde) testen onderzocht of het mogelijk was de functionaliteit van de webapplicatie of onderliggende infrastructuur te misbruiken of binnen te dringen in de applicatie of de onderliggende systemen.

De blackbox scan is op de acceptatieomgeving uitgevoerd. Hier staat de meest courante versie van de 'Digitaal Loket' webapplicatie.

2.3 Aanpak en werkwijze

De pentest is opgebouwd uit drie fasen, waarbij wij in de eerste fase de webserver en de daarbinnen gebruikte technieken hebben verkend. In de tweede fase hebben wij een (geautomatiseerde) test op de applicaties uitgevoerd. In de derde fase hebben wij de resultaten geanalyseerd en handmatige tests uitgevoerd om vast te stellen of meldingen daadwerkelijk tekortkomingen zijn.

De vulnerability assessment is opgebouwd uit twee fasen, waarbij wij in de eerste fase een (geautomatiseerde) test op de infrastructuur hebben uitgevoerd. In de tweede fase hebben wij de resultaten geanalyseerd en handmatige tests uitgevoerd om vast te stellen of meldingen daadwerkelijk tekortkomingen zijn.

De blackbox scan is opgebouwd uit twee fasen, waarbij wij in de eerste fase een (geautomatiseerde) test op de applicatie hebben uitgevoerd. In de tweede fase hebben wij de resultaten geanalyseerd en handmatige tests uitgevoerd om vast te stellen of meldingen daadwerkelijk tekortkomingen zijn.

3 Onder integriteit verstaan wij de mate waarin het object in overeenstemming is met de afgebeelde werkelijkheid. De mate van getroffen maatregelen onderzoeken wij om de juistheid en volledigheid van gegevens te waarborgen. Onder exclusiviteit verstaan wij de mate waarin uitsluitend geautoriseerde personen via geautoriseerde procedures gebruikmaken van IT-processen. Deze definities zijn afkomstig uit Geschrift No.1 van de beroepsorganisatie van IT-auditors, NOREA.

Een uitgebreide beschrijving van de aanpak van de pentest, vulnerability assessment en blackbox scan kunt u lezen in bijlage 4 van dit rapport.

Dit onderzoek is uitgevoerd in maart t/m april 2015. Op 25 en 26 maart 2015 is de pentest vanaf het internet op de webapplicaties uitgevoerd. Op 27 maart 2015 zijn de vulnerability assessment en blackbox scan uitgevoerd vanaf het interne netwerk van RvS.

De bevindingen uit dit onderzoek zijn op 30 maart 2015 afgestemd met een applicatiebeheerder van RvS. Het conceptrapport is op 1 juni 2015 per mail afgestemd met de opdrachtgever.

Dit onderzoek is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (IIA 2200-2600). Bij de uitvoering van dit onderzoek wordt geen assurance verstrekt, maar is volstaan met het rapporteren van de onderzoeksresultaten.

2.4 Verantwoording

Het beveiligingsonderzoek is indicatief en geeft geen totaaloordeel over het beveiligingsniveau van de onderzochte webapplicaties. Kwetsbaarheden kunnen vaak, door de beperkte tijd en middelen, niet zover worden onderzocht dat het mogelijk wordt de kwetsbaarheid volledig uit te buiten. Gedurende de onderzoeksperiode

2.5 Verspreidingskring rapportage

Dit rapport is uitsluitend bestemd voor de opdrachtgever met wie de uitgevoerde werkzaamheden zijn overeengekomen. De opdrachtgever is verantwoordelijk voor het correcte gebruik van dit rapport.

2.6 Leeswijzer

Hoofdstuk 3 bevat de detailbevindingen en aanbevelingen en is bedoeld als verdieping van de managementsamenvatting. In bijlage 1 is de koppeling tussen de aangetroffen kwetsbaarheden op het Digitaal Loket en de DigiD applicatiescan normen opgenomen. In bijlage 2 van dit rapport is beschreven hoe de risicoclassificaties van gevonden kwetsbaarheden zijn te interpreteren. Bijlage 3 bevat een gedetailleerde beschrijving van de fasering van dit onderzoek.

3 Bevindingen en aanbevelingen

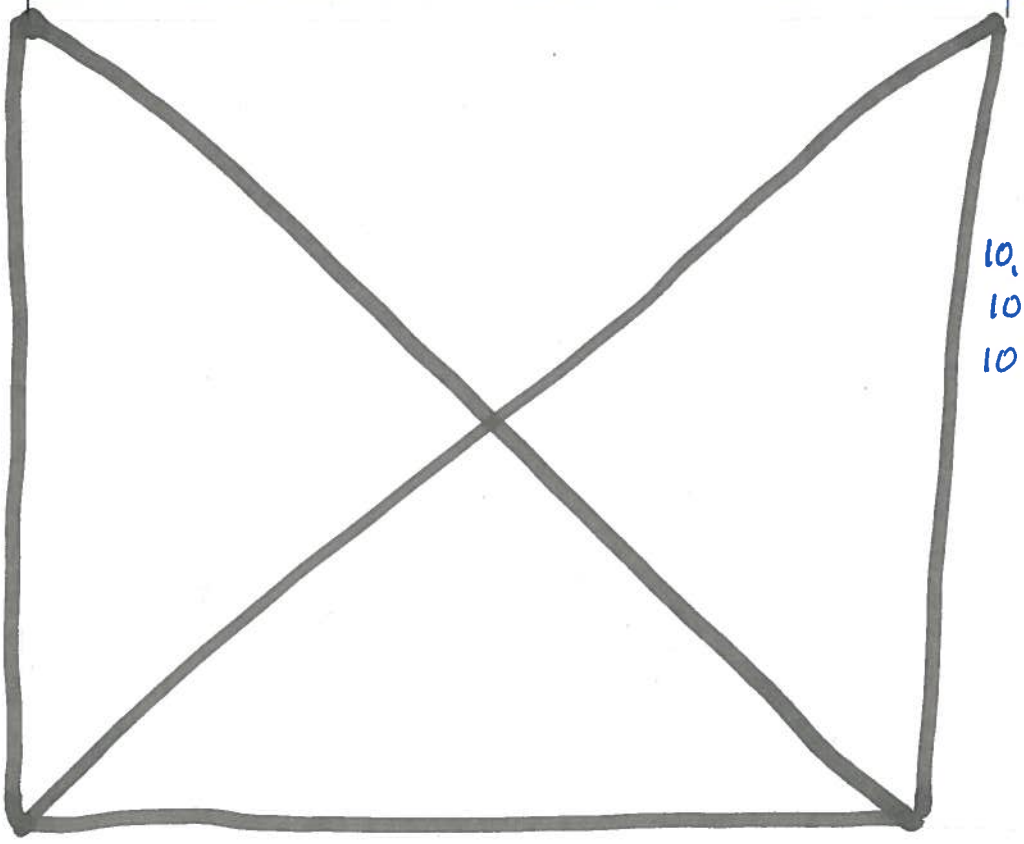
3.1 Inleiding

In dit hoofdstuk worden de bevindingen en aanbevelingen uit het onderzoek in detail beschreven. Wij hebben handmatig de kwetsbaarheden nagelopen die door onze testprogramma's zijn gevonden. Daarbij verifiëren wij of de kwetsbaarheden werkelijk in de webapplicaties of de onderliggende systemen aanwezig zijn of dat de testprogramma's valse meldingen hebben gegeven. Na de verificatie hebben wij van de aangetroffen kwetsbaarheden de risicoclassificaties bepaald en een inschatting gemaakt van de inspanning die nodig is om de kwetsbaarheid te verhelpen.

De aangetroffen kwetsbaarheden zijn in onderstaande tabel samengevat. Deze zijn onderverdeeld in vijf onderwerpen van kwetsbaarheden. Daarnaast is een risicoclassificatie opgenomen en een indicatie over de benodigde inspanning (Insp.). Tot slot zijn de gevonden kwetsbaarheden in de een-na-laatste kolom van de tabel opgedeeld naar webapplicatie (A) of de onderliggende infrastructuur (I), zoals de webserver. Hiermee wordt aangegeven op welk niveau de kwetsbaarheid zich bevindt[4]. De laatste kolom, test, geeft aan of de bevinding gedurende de penetratietest (P), blackbox scan (B) of vulnerability scan (V) is aangetroffen.

In bijlage 2 van dit rapport is beschreven hoe de risicoclassificaties zijn te interpreteren. De toelichting op de onderwerpen en op de aangetroffen kwetsbaarheden is opgenomen in de volgende paragrafen.

Kwetsbaarheid	Applicatie(s)	Risico	Insp.	Soort	Test



10,1°,b+
10,1°,c+
10,2°,g

alles 10,1°, b + 10,1°, c + 10,2°, g

Kwetsbaarheid	Applicatie(s)	Risico	Insp.	Soort	Test
[redacted]					

Tabel 1: Overzicht van aangetroffen kwetsbaarheden

3.2 Bestands- en directory toegang

Op de server aanwezige bestanden bieden kwaadwillenden mogelijk extra informatie om de server aan te vallen. Dit geldt zowel voor bestanden die alleen informatie bevatten als voor programma's voor test- of beheerdoeleinden. Tijdens de test [redacted]

Gedurende de onderzoeksperiode zijn op dit onderdeel geen kwetsbaarheden aangetroffen met een hoog, midden of laag risico.

3.3 Controle van invoervariabelen

Aandacht voor de controle van invoervariabelen is bij webapplicaties van groot belang. De programmeur moet er vanuit gaan dat alle invoer onbetrouwbaar is. De client valt buiten de invloedssfeer van de organisatie en kan daarmee niet gebruikt worden om invoer te controleren, dit moet op de server gebeuren. Tijdens de test is foutieve en malafide invoer aangeboden om te zien hoe de webapplicatie hiermee omgaat.

3.3.1 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

Gedurende het onderzoek is naar voren gekomen dat [redacted]

alles 10,1°,b + 10,1°,c + 10,2°,g

3.4

3.4.1

Applicatie(s)	Risico	Inspanning	Soort

3.4.2

Applicatie(s)	Risico	Inspanning	Soort

alles 10,1°,6 + 10,1°,c + 10,2°, g

[redacted]

3.5 [redacted]

Een webapplicatie kan gebruik maken van een beveiligingsmechanisme als vertrouwelijke en/of persoonlijke gegevens kunnen worden ingevoerd of geraadpleegd. De sterkte van dit mechanisme bepaalt voor een groot gedeelte het beveiligingsniveau van de webapplicatie. Tijdens de test is onderzocht of een adequaat beveiligingsmechanisme is toegepast, of mogelijkheden aanwezig zijn om de beveiliging te omzeilen of om kwetsbaarheden van een gebruikt beveiligingsmechanisme aan zijn te tonen.

3.5.1 [redacted]

Applicatie(s)	Risico	Inspanning	Soort

[redacted]

3.5.2 [redacted]

Applicatie(s)	Risico	Inspanning	Soort

[redacted]

alles 10,1°b + 10,1°c + 10,2°g

3.5.3

Applicatie(s)	Risico	Inspanning	Soort

3.6

3.6.1

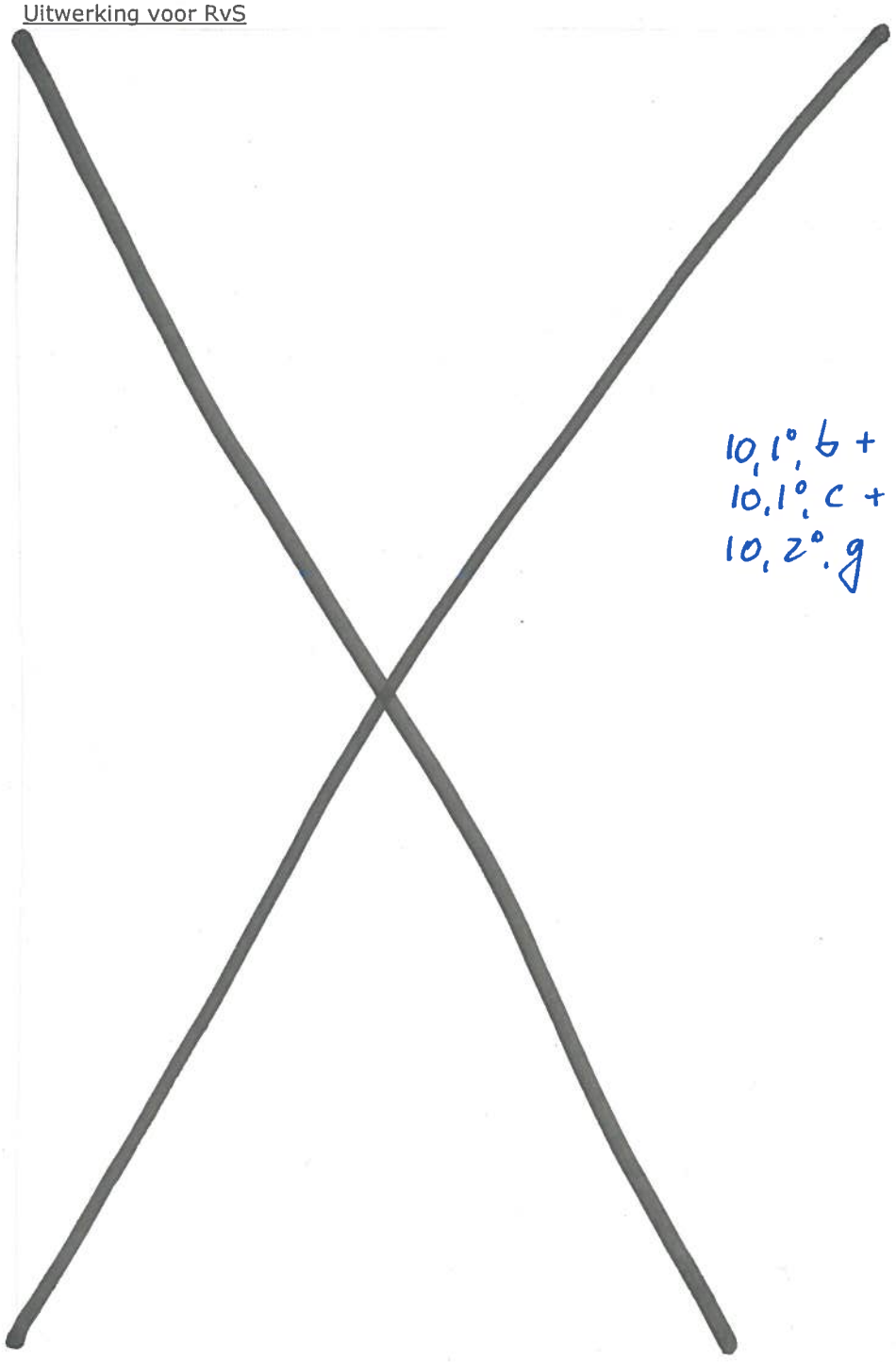
Applicatie(s)	Risico	Inspanning	Soort

Om een beveiligde verbinding op te zetten naar een webapplicatie kan gebruik worden gemaakt van encryptie via het SSL/TLS protocol. Met een SSL-certificaat kan een eigenaar van een webapplicatie aan een bezoeker de identiteit van de webserver garanderen. De eigenaar geeft hierbij het vertrouwen aan de bezoeker dat bijvoorbeeld de invoer van gegevens door de gebruiker via een beveiligde verbinding wordt gestuurd naar de webapplicatie.

De kwaliteit van (de configuratie van) het gebruikte SSL-certificaat kan worden bepaald door vier kwaliteitseisen: *Certificate*, *Protocol Support*, *Key Exchange* en *Cipher Strength*.

- *Certificate* bekijkt of het aangetroffen certificaat betrekking heeft op de bezochte domeinnaam, de geldigheid van het certificaat en de betrouwbaarheid van de certificerende autoriteit.
- *Protocol Support* bekijkt welke protocollen worden ondersteund door de SSL-server. Oudere SSL-versies bevatten bijvoorbeeld kwetsbaarheden waardoor het gebruik van een oudere SSL-versie een lagere kwaliteitsscore veroorzaakt.
- In de *Key Exchange* fase wordt de authenticiteit van één van de partijen vastgesteld en de generatie en beveiligde overdracht van de SSL-sessiesleutel vindt plaats.
- De *Cipher Strength* geeft de sterkte van de beveiligde verbinding weer. Een sterke Cipher (versleutelingsalgoritme) zorgt voor een sterkere encryptie en bemoeilijkt dus het doorbreken van de beveiligde verbinding.

Uitwerking voor RvS



alles 10,1°,b + 10,1°,c + 10,2°,g

[redacted]

3.6.2 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

3.6.3 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

Uitwerking voor RvS

[redacted]

alles 10.1°.b + 10.1°.c + 10.2°.g

3.6.4 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

Uitwerking voor RvS

[redacted]

3.6.5 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

Uitwerking voor RvS

[redacted]

Figuur 2. [redacted]

alles 10,1°.b + 10,1°,c + 10,2°.g

3.6.6 [redacted]

Applicatie(s)	Risico	Inspanning	Soort
[redacted]			

Uitwerking voor RvS

Gedurende het onderzoek [redacted]

[redacted]

* * *

4 Ondertekening

Tot het geven van een nadere toelichting zijn wij gaarne bereid.

Auditdienst Rijk,

Den Haag, 23 juli 2015

Projectleider ADR
(opdrachtnemer)

10,2 ; e

Bijlage 1 – Bevindingen per DigiD richtlijn

Het beveiligingsonderzoek raakt beveiligingsrichtlijnen van de ICT-beveiligingsassessment DigiD (hierna: DigiD assessment). In deze bijlage vindt u een tabel die de beveiligingsrichtlijnen relateert aan de bevindingen uit dit rapport met betrekking tot het Digitaal Loket. Dit beveiligingsonderzoek is echter niet gedreven vanuit een DigiD assessment. Wij hebben zo breed mogelijk getest en kunnen ook kwetsbaarheden aantreffen die niet aan een DigiD richtlijn zijn te relateren.

De bevindingen in Tabel 2 kunnen de auditor van de DigiD assessment input geven om te komen tot een oordeel per richtlijn voor het Digitaal Loket.

Nr.	Omschrijving DigiD beveiligingsrichtlijn	Bevinding
B0-6	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	Geen kwetsbaarheden aangetroffen.
B0-7	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	Geen kwetsbaarheden aangetroffen.
B0-8	Penetratietests worden periodiek uitgevoerd.	Wordt deels aangetoond met deze rapportage (in het bestaan uitgevoerd).
B0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	Wordt deels aangetoond met deze rapportage (in het bestaan uitgevoerd).
B0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	Geen kwetsbaarheid vanuit de internettoegang aangetroffen.
B2-1	Maak gebruik van [redacted]	[redacted] die aan deze norm is te relateren. Zie paragraaf 3.5.2.
B3-1	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-3	De webapplicatie normaliseert invoerdata voor validatie.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.

10,1°b +
10,1°c +
10,2°g

B3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	Geen kwetsbaarheid aangetroffen die aan deze norm is te relateren.
B3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	Wordt deels aangetoond met deze rapportage (in het bestaan uitgevoerd).
B3-16	Zet de cookie attributen 'HttpOnly' en 'Secure'.	Volledig getest. Geen kwetsbaarheid aangetroffen.
B5-2	Maak gebruik van versleutelde (HTTPS) verbindingen.	Volledig getest. Geen kwetsbaarheid aangetroffen.
B5-4	Versleutel cookies.	Volledig getest. Geen kwetsbaarheid aangetroffen.

Tabel 2. Aan de DigiD assessment te relateren bevindingen voor het Digitaal Loket

Bijlage 2 – Toelichting risicobeschrijving

In dit rapport zijn risicoclassificaties opgenomen om de bevindingen te categoriseren. In tabel 1 hebben wij de gehanteerde risicoclassificatie opgenomen. Daarnaast geven wij per bevinding een schatting aan van de benodigde inspanning om de bevinding te verhelpen. In tabel 2 hebben wij de gehanteerde inspanningsclassificatie opgenomen.

Classificatie	Risico
Hoog (**H**)	Een bevinding met hoog risico betreft een situatie die direct kan leiden tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Hoge risico's dienen zo snel mogelijk gemitigeerd, of beter nog, te worden weggenomen.
Midden (**M**)	Een bevinding met midden risico betreft een situatie die niet op zichzelf de mogelijkheid biedt tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Wel biedt het een mogelijkheid, of verschaft het de informatie, om dat in combinatie met andere hulpmiddelen of informatie *eenvoudig* te bereiken. Middelmatige risico's verdienen ook de aanbeveling om te mitigeren of weg te nemen, maar hebben geen directe urgentie.
Laag (**L**)	Een bevinding met laag risico betreft een situatie die niet op zichzelf de mogelijkheid biedt tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Wel biedt het een mogelijkheid, of verschaft het informatie, om dat in combinatie met andere hulpmiddelen of informatie te bereiken. Lage risico's dienen overwogen te worden om te mitigeren of weg te nemen.

Tabel 3: Classificatie van risico's

Classificatie	Inspanning
Hoog (**H**)	Een aanbeveling die hoge inspanning vereist, omvat omvangrijke onderzoek- en implementatieactiviteiten.
Midden (**M**)	Een aanbeveling die middelmatige inspanning vereist, omvat gemiddelde onderzoeks- en implementatieactiviteiten.
Laag (**L**)	Een aanbeveling die lage inspanning vereist, omvat geringe onderzoeks- en implementatieactiviteiten.

Tabel 4: Classificatie van benodigde inspanning

Bijlage 3 – Gedetailleerde fasering onderzoek

De **penetratietest** was opgebouwd uit drie fasen:

Fase 1 - is een verkenning van de webserver en de daarbinnen gebruikte technieken. De (eventueel) aanwezige documentatie is doorgenomen en de functionaliteit van de applicatie is met een reguliere browser verkend. Op basis van de bevindingen is [redacted]

Fase 2 - is een (geautomatiseerde) test van de applicatie. De webapplicatie is met behulp van het testprogramma gescand op kwetsbaarheden van de webserver, het applicatieplatform en de programmacode. Aanvullend zijn ook andere programma's, waaronder [redacted] ingezet om resultaten uit het testprogramma te verifiëren en ter aanvulling van het onderzoek.

Onderwerpen die tijdens de (geautomatiseerde) test aan de orde zijn gekomen:

- *Bestands- en directory toegang*
  De op de servers aanwezige bestanden bieden aanvallers mogelijk extra informatie om de servers aan te vallen. Dit geldt zowel voor bestanden die alleen informatie bevatten als voor programma's voor test- of beheerdoeleinden. Tijdens de test is gezocht naar veel voorkomende bestanden en directories.

- *Controle van invoervariabelen*
  Aandacht voor de controle van invoervariabelen is bij webapplicaties van groot belang. De programmeur moet er vanuit gaan dat alle invoer onbetrouwbaar is. De client valt buiten de invloedssfeer van de organisatie en kan daarmee niet gebruikt worden om invoer te controleren, dit moet op de server gebeuren. Tijdens de test is foutieve invoer aangeboden om te zien hoe de webapplicatie hiermee omgaat.

- *Component afhankelijke kwetsbaarheden*
  Een webapplicatie maakt veelal gebruik van verschillende componenten. Het bekend worden van kwetsbaarheden in deze componenten kan ertoe leiden dat de beveiliging van de applicatie, de webserver of de database in het geding is. Tijdens de test zijn bekende kwetsbaarheden onderzocht op de applicatie en de onderliggende componenten.

- *Beveiligingsmechanisme*
  Een webapplicatie kan gebruik maken van een beveiligingsmechanisme als vertrouwelijke en/of persoonlijke gegevens kunnen worden ingevoerd of geraadpleegd. De sterkte van dit mechanisme bepaalt voor een groot gedeelte het beveiligingsniveau van de webapplicatie. Tijdens de test is nagegaan of een adequaat beveiligingsmechanisme is toegepast, of mogelijkheden aanwezig zijn om de beveiliging te omzeilen of om kwetsbaarheden van een gebruikt beveiligingsmechanisme aan zijn te tonen.

- *Beveiliging gegevenstransport*
  Webapplicaties bevatten vaak diverse voorzieningen waarmee de gebruiker (persoonlijke) informatie stuurt naar een achterliggende database. Denk hierbij ondermeer aan inlogvoorzieningen en contactformulieren. Indien het (privacy)gevoelige gegevens betreft, dienen de door de gebruiker ingevoerde gegevens versleuteld te worden verstuurd, overeenkomstig hetgeen gesteld en geëist wordt in de Wet bescherming persoonsgegevens (Wbp). De versleuteling dient om de privacy van de gegevens tijdens transport te kunnen waarborgen. Gedurende de test is onderzocht of de geïmplementeerde versleuteling geen kwetsbaarheden bevat.

Fase 3 - is een analyse van de resultaten die het testprogramma heeft opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde "false positives" opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om "false positives" zoveel mogelijk uit te sluiten zijn de meldingen handmatig onderzocht.

Het is [redacted]

10,1°,b+
10,1°,c+
10,2°,g

De **vulnerability assessment** was opgebouwd uit de volgende fasen:

Fase 1 - bestaat uit een (geautomatiseerde) test van de infrastructurele componenten. De componenten zullen met testprogramma's worden gescand op ondermeer kwetsbaarheden in de configuratie en missende patches. Er zullen verschillende programma's worden ingezet om resultaten te verifiëren en ter aanvulling van het onderzoek.

Fase 2 - is een analyse van de resultaten die de testprogramma's hebben opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde "false positives" opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om "false positives" zoveel mogelijk uit te sluiten worden de resultaten handmatig gevalideerd.

De **blackbox scan** was opgebouwd uit de volgende fasen:

Fase 1 - bestaat uit een (geautomatiseerde) test van de applicatie. De webapplicatie zal met testprogramma's worden gescand op kwetsbaarheden van het applicatieplatform en de programmacode. Er zullen verschillende programma's worden ingezet, enerzijds om resultaten te verifiëren en anderzijds ter aanvulling van het onderzoek.

Fase 2 - is een analyse van de resultaten die de testprogramma's hebben opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde "false positives" opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om "false positives" zoveel mogelijk uit te sluiten worden de resultaten handmatig gevalideerd.

NB. Tussen de penetratietest en de blackbox scan zit veel overlap. De pentest is [redacted]
zoals dit normaliter door ontwikkelaars wordt gedaan.

10,1°,b+
10,1°,c+
10,2°,g

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00