Beveiliging IV Toets NFRs

oBRP16 maart 2017

Inleiding

Met een eerste toets van de NFRs van het type beveiligbaarheid is gekeken naar de eventuele risico's bij IV ten aanzien van de applicatie beveiliging. Bijkomend is de herkomst en onderbouwing van met name de voor IV van toepassing zijnde NFRs van het type beveiligbaarheid uitgewerkt.

NFR beveiligbaarheid 'BEV' herkomst

Non-functional requirements:

Deze zijn in het verleden opgesteld conform ISO 25010 waar beveiligbaarheid onderdeel van uit maakt. Alle NFRs zijn opgenomen in een mastertable excel document.

Merk op: De mastertable (v2) gebruikt soms een andere formulering van de requirements dan de andere documenten. Ook zijn er zo nu en dan inhoudelijke verschillen. De formulering van de NFRs van het type beveiligbaarheid doet vermoeden dat deze zijn geformuleerd in de geest van applicatieontwikkeling voor algemene, openbare internettoepassingen. Bijvoorbeeld in maatregelen die malafide gebruik van buitenaf moeten tegengaan is dit terug te herkennen. Dit sluit niet aan bij het type applicatie en de moderne ontwikkelmethodiek in gebruik bij het project.

Uit het requirementsdossier:

> "Voor zover het eisen betreft die betrekking hebben op de door oBRP te ontwikkelen software is het informatiebeveiligingsplan in afstemming met RvIG omgezet in requirements beveiligbaarheid (RD-BEV). Met betrekking tot informatiebeveiliging hanteert oBRP deze eisen en niet het informatiebeveiligingsplan."

Dit is een afbeelding van de eerder gestelde eisen ten aanzien van beveiligbaarheid op de eisen in het beveiligingsplan. Volgens **'Koppeling IBP en Requirements Beveiligbaarheid'** zijn de normen uit het beveiligingsplan geconsolideerd of herschikt binnen de requirements beveiligbaarheid.

Beperking impact NFR BEV:

In dit document zijn de eisen voor beveiligbaarheid in een subset vervat die buiten de codeerrichtlijnen vallen. De eisen die onder de codeerrichtlijnen vallen zijn uit de requirements beveiligbaarheid v2.5 weggelaten.

Merk op: Enkele van de resterende eisen zijn in de mastertable soms wel onder 'defensief programmeren' geschaard en lijken in voorkomende gevallen oor de codeerrichtlijnen te raken.

Uit requirements beveiligbaarheid v2.5:

> "De requirements zijn opgedeeld in de groepen 'algemeen', 'koppelvlakken' en 'gebruikersinterface'. Aangezien de centrale BRP geen gebruikersinterface ten behoeve van reguliere gebruikers heeft, betreft die laatste groep alleen de gebruikersinterface ten behoeve van beheer van de voorziening."

Voor IV zijn alleen deels de requirements in de groep 'algemeen' van toepassing. Voor IV zijn de requirements 'koppelvlakken' en 'gebruikersinterface' niet van toepassing. Door het team (onderling overleg betrokken expertises) zijn deze aangemerkt als niet van toepassing zijnde of als afgedekt door specifieke functionele eisen. Dit is beschreven in het Excel overzicht 'NFRs IV'.

Requirements algemeen

Navolgende algemene requirements worden gesteld aan de door het project O&R op te leveren maatwerkcomponenten van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging, de requirements die niet van toepassing zijn verklaard voor IV zijn doorgehaald:

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
~~RD-BEV-006~~	~~Technische fouten en bijbehorende technische meldingen (zoals een stacktrace of melding van een extern systeem) mogen nooit zichtbaar zijn voor de eindgebruiker[1]; er mag geen info over het onderliggende of achterliggende systeem naar buiten.~~
~~RD-BEV-037~~	~~Foutmeldingen aan eindgebruikers bevatten geen persoonsgegevens, met uitzondering van persoonsgegevens die door deze zelfde eindgebruiker zijn opgegeven in een bericht waar de foutmelding op volgt.~~
~~RD-BEV-050~~	~~Gebruik voor "one-way hashes" altijd een salt.~~
~~RD-BEV-019~~	~~Voorkom het gebruik van third party libraries die niet in de repository manager staan en release builds dienen altijd alleen vanuit de repository manager hun dependencies te downloaden.~~
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.

[1] Een beheerder wordt niet beschouwd als eindgebruiker.

RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
~~RD-BEV-025~~	~~Het systeem heeft gescheiden koppelvlakken/gebruikersinterfaces voor enerzijds beheer en anderzijds eindgebruikerstoegang zodat het systeem kan functioneren op een infrastructuur met (eventueel virtueel) gescheiden netwerken voor eindgebruikerstoegang (koppelvlakken), beheer en opslag.~~
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico's zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.
~~RD-BEV-036~~	~~Verifieer voor een verwerking of de gebruiker (of beheerder) geautoriseerd is voor betreffende verwerking.~~
~~RD-BEV-039~~	~~Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.~~
~~RD-BEV-040~~	~~Stapelen van fouten wordt voorkomen door toepassing van "noodstop" mechanismen.~~
~~RD-BEV-041~~	~~Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.~~
RD-BEV-049	Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.
RD-BEV-032	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext) Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.
~~RD-BEV-052~~	~~In het systeem opgenomen persoonsgegevens kunnen door de bijhouder worden gecorrigeerd.~~

Requirements IV interpretatie

In het navolgende overzicht is een interpretatie voor IV gegeven per requirement met een invulling van de mogelijke acties uit het perspectief van testen hiervoor.

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Interpretatie	In deze maatregel is te lezen dat er sprake zou zijn van malafide handelen van buitenaf. Dit is voor IV als applicatie nauwelijks van toepassing. In zowel de applicatie-architectuur, functionele eisen als de ontwikkelmethodiek komen deze aspecten terug. Het draait om het controleren en bewaken van (gegevens)integriteit en het voorkomen van manipulatie van de applicatie. **Testen** Het testen van validatie, integriteit zit verwerkt in de functionele testen van IV. Zo is er de syntax- en preconditie-controle waarin dit aan bod komt. Daarnaast is er sprake van codereviews in de teams en de inzet van tooling. Advies: Voor deze eis zijn geen aanvullende testen nodig.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Interpretatie	Hier is controle op onterechte toegang beschreven en het melden van fouten voor opvolging, zo mogelijk correctie. Veel van de beschreven punten zijn niet van toepassing voor IV of slechts deels. **Testen**

	Het gedrag van de applicatie bij storingen en foutmeldingen is te testen bij voorkomende scenario's. Een aantal zit al in functionele testen verwerkt. Op onderdelen is mogelijk foutinjectie in testscenario's uit te voeren (de vraag is hoeveel dit toevoegt). Deze eis zal in relatie tot infrastructuur ook terugkomen in testen. Advies: Voor deze eis testen de teams IV zelf op foutsituaties. I&T gaat na hoe de teams dit afdekken en toetsen dit zo mogelijk aan het technisch ontwerp.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Interpretatie	Eis om te loggen op een ander systeem met oog op compartimenteren. **Testen** Advies: Maak een test die naar een andere locatie de log wegschrijft.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
Interpretatie	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren. **Testen** Advies: Review of dit technisch mogelijk is.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico's zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.
Interpretatie	De OWASP lijst komt tot stand door jaarlijks bij een aantal organisaties incidenten te inventariseren aangaande webapplicaties. De laatste release van de lijst was in 2013. Wel is er onverwerkte data uit 2014 en 2015. Op basis van 2013 zijn uit de 10 meest voorkomende kwetsbaarheden de volgende relevante punten te herleiden: • Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie. Vergelijk RD-BEV-004. • Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc. Vergelijk RD-BEV-049/032 • Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack. • Bekende kwetsbaarheden in gebruikte standaard software componenten. OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik.

	Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn. De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'. **Testen** Nagaan of in de documentatie is vastgelegd dat een punt van toepassing is. Controle via SOnarQube regels, review van gebruikte software componenten op bekende kwetsbaarheden en expertreview van configuratie op foutgevoeligheid. Advies: Ga na of er geen openstaande issues zijn in het SonarQube dashboard. Review de documentatie of in het SAD is opgenomen welke punten van toepassing zijn, of er een verwijzing is naar een overzicht van relevante punten.
RD-BEV-049	Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.
Interpretatie	Autorisatie op onderdelen volgt het principe van 'least privilege'. **Testen** Nalopen van documentatie op resource toegang en review op het principe. Uiteindelijk komt dit aan bod bij de inrichting van de infrastructuur, systeemsoftware. Advies: Verifieer of in het SAD is beschreven wat de resources zijn die de applicatie gebruikt en of dit overeenkomt met de werkelijkheid.
RD-BEV-032	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext) Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.
Interpretatie	Veilige omgang met wachtwoorden door de applicatie, goede versleuteling bij opslag. Als opslag in een configuratiebestand van een wachtwoord echt nodig is dan is hier een uitzondering op te maken mits het zorgvuldig gebeurd zodat de omgeving, infrastructuur hier aanvullende maatregelen bij kan treffen. **Testen** Advies: Nalopen van de documentatie en review van configuratiebestanden op wachtwoorden. Gebruiker en wachtwoord aanpassen in een testscenario.

Van de NFRs voor IV is vanuit het perspectief van testen beoordeeld dat requirement RD-BEV-019 buiten de scope valt. Dit betreft:

> *"Voorkom het gebruik van third party libraries die niet in de repository manager staan en release builds dienen altijd alleen vanuit de repository manager hun dependencies te downloaden."*

De reden hiervoor is dat dit uiteindelijk is afgedekt door de procesinrichting van de beheerder. In het proces van ontwikkeling is er echter wel sprake van dat deze requirement invulling krijgt ten tijde van de ontwikkeling van de applicatie. Dit is in het SAD van de software opgenomen waar het gebruik van third-party libraries beperkt is tot de Nexus repository voor ontwikkeling op modernodam.

Invulling van de NFRs – maatregelen en testen

Gezien de aard van IV staat functioneel het bewaken van de integriteit van de gegevens bovenaan de doelstellingen gevolgd door controle op het proces dat de applicatie ondersteunt. Het aspect beschikbaarheid is functioneel gezien vanuit gebruik van de applicatie minder van belang. De waarborgen voor vertrouwelijkheid bij IV zijn hoofdzakelijk buiten de applicatie belegd wanneer de ISC beheerder gebruik maakt van de IV applicatie.

De maatregelen voor ontwikkeling en de uit te voeren testen bij IV zijn per NFR opgenomen in het Excel overzicht 'NFRs IV'. Deze betreffen:

- Peer reviews (ontwikkeling)
- Steekproefsgewijs testen (ontwikkeling)
- Expertreviews (ontwikkeling en test)
- Vastlegging in SAD (ontwikkeling)
- Vastlegging in TO (ontwikkeling)
- Expliciet testen (test)

Merk op: In voorkomende gevallen kan een NFR beveiligbaarheid een relatie hebben met een ander type NFR zoals bijvoorbeeld betrouwbaarheid als het gaat om logging. De NFRs liggen soms dicht tegen elkaar aan.

In de invulling van het normenkader codekwaliteit is ook aandacht voor maatregelen die de NFRs van beveiligbaarheid ondersteunen. In het bijzonder de tooling die op punten toeziet die beveiliging direct raken zoals de "security" categorie voor Findbugs en PMD.

De ontwikkelaars maken gebruik van SonarQube voor het bewaken van de gestelde normen. De regels uit de normen dekken op het gebied van beveiligbaarheid de OWASP RD-BEV-030 NFR af. Naast de OWASP regels zijn onder andere ook CWE en SANS25 regels opgenomen. Dit is dus een bredere groep regels dan die van OWASP zoals gesteld in de NFRs.

Observaties

Gezien de aard van het project, langlopend en een behoorlijke omvang, valt op dat de broncode en bijbehorende tooling goed onderhouden zijn. De toegepaste regels binnen een SonarQube zijn bijvoorbeeld actueel. Ontwikkelaars en testers in de teams streven naar voortdurende kwaliteitsverbetering, dat draagt bij aan een goede invulling van de betrouwbaarheid,

beveiligbaarheid en onderhoudbaarheid in overeenstemming met het normenkader voor codekwaliteit.

Op de NFRs ten aanzien van beveiligbaarheid is het nodige aan te merken. Er is sprake van een gedateerde verzameling eisen die niet past bij de aard van het BRP project maar eerder bij de ontwikkeling van een website rond 2008. Eisen overlappen, zijn niet alleen op de BRP applicatie van toepassing en de mogelijke interpretatie voor de applicatie is ruim.

Naar de letter is er geen invulling gegeven aan het gevraagde OWASP argumentatie per punt in softwaredocumentatie. Om verwarring te voorkomen is het handig deze (als verwijzing) toe te voegen en daarbij gebruik te maken van de hier opgenomen interpretatie, of deze van toepassing is en een verwijziging naar de inzet van SonarQube met de OWASP regels.

Bij de controle op nieuwe versies van de onderliggend gebruikte softwarecomponenten komt nu niet expliciet het aspect veiligheid aan bod. De controle vindt nu incidenteel plaats. Dit zou het project in een periodieke afweging moeten betrekken voor het doorvoeren van de inzet.

Bijlage OWASP interpretatie

Laatste versie uit 2013 (daarna is geen top 10 meer gepubliceerd – zie owasp.org).

- A1-Injection
  - Een specifieke manipulatie techniek. Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie.
- A2-Broken Authentication and Session Management
  - Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc.
- A3-Cross-Site Scripting (XSS)
  - Validatiefouten in webapplicaties in combinatie met een webbrowser bij de gebruiker. Niet van toepassing.
- A4-Insecure Direct Object References
  - Een specifieke manipulatie techniek. Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie.
- A5-Security Misconfiguration
  - Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack.
- A6-Sensitive Data Exposure
  - Het lekken van gevoelige informatie. Niet van toepassing.
- A7-Missing Function Level Access Control
  - Het onbedoeld verkrijgen van toegang tot (delen) van functies.
- A8-Cross-Site Request Forgery (CSRF)
  - Een aanval gericht op de webbrowser van een gebruiker waarbij een webapplicatie dit kan voorkomen. Niet van toepassing.
- A9-Using Components with Known Vulnerabilities
  - Bekende kwetsbaarheden in gebruikte standaard software componenten.
- A10-Unvalidated Redirects and Forwards
  - Validatie problemen op websites. Niet van toepassing.

Op basis van de in 2016 gepubliceerde ruwe data over 2014 en 2015, in volgorde van het aantal meldingen zou de lijst er als volgt uitzien:

- Number of Cross-Site Scripting (XSS) Vulnerabilities Found (CWE-79)?
    - A3
- Number of SQL Injection Vulnerabilities Found (CWE-89)?
    - A1
- Number of Unchecked Redirect Vulnerabilities Found (CWE-601)?
    - A10
- Nieuw: Number of XML eXternal Entity Injection (XXE) Vulnerabilities Found (CWE-611)?
    - URI referenties buiten het verwachte domein. Niet van toepassing
- Nieuw: Number of Path Traversal Vulnerabilities Found (CWE-22)?
    - Externe invoer die paden in de applicatie beïnvloedt. Niet van toepassing.
- Number of Security Misconfiguration Vulnerabilities Found (CWE-2)?
    - A5
- Nieuw: Number of Cryptographic Vulnerabilities Found (CWEs-310/326/327/etc)?
    - Verkeerd gebruik van cryptografie of verouderde cryptografische software. Variant van A2. Niet van toepassing voor IV.
- Nieuw: Number of Command Injection Vulnerabilities Found (CWE-77)?
    - Commando's doorgeven vanuit externe invoer. A4 en A7 gerelateerd. Niet van toepassing.
- Nieuw: Number of Mass Assignment Vulnerabilities Found (CWE-915)?
    - Externe invoer die attributen, eigenschappen van de applicatie beïnvloedt. Niet van toepassing.
- Number of Session Fixation Vulnerabilities Found (CWE-384)?
    - A2
- Input Validation
    - Generalisatie van A1, A4, A7 en A10.

CWE staat voor Common Weakness Enumeration, een standaard voor het aanduiden van de veelvoorkomende kwetsbaarheden in software.