Requirements Analyse Showcase

Niveau 2

Ernst Bolt
2023

Distributie

Versie	Datum	Wijzigingen	Ontvangers
0.3	31-5-2023	RA uitgebreid met de stap: risico's schatten	Bram, Karen, Henk, Thomas
0.4	31-5-2023	Foutieve verwijzingen aangepast Duplicate NFR verwijderd Tekstuele verbeteringen Toelichting voor student toegevoegd	Bram, Karen, Henk, Thomas
0.5	6-6-2023	Om BIV makkelijker onder de aandacht te brengen zijn voetnoten toegevoegd met de factoren. In het hoofdstuk met requirements een verwijzing opgenomen naar de aanpak.	Bram, Karen, Henk, Thomas

Inhoud

Inleiding

Dit document gaat in op de requirements voor het ontwikkelen van de Showcase.

In het volgende hoofdstuk zijn de requirements beschreven. Het proces hoe deze requirements zijn ontstaan is beschreven in Bijlage 1 Aanpak Requirements. Deze bijlage is heel handig om te gebruiken als je zelf requirements gaat ontwikkelen.

Succes met de requirements!

Ernst Bolt

1 Requirements

In dit hoofdstuk zijn de requirements uitgewerkt. De requirements zijn per user story gegroepeerd. Per requirement is vastgelegd wat voor type het is, wat de prioriteit is en/of een test moet worden uitgevoerd. Een beschrijving hoe de requirements tot stand zijn gekomen is te vinden in In Bijlage 1 Aanpak Requirements Analyse.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
US1	IV1	Als gebruiker wil ik de CV van een developer kunnen zien zodat ik me kan oriënteren voordat ik contact leg		Must	Functioneel
NFR1		De gegevens op de pagina zijn niet wijzigbaar via de interface	Beperking	Must	
NFR2		De pagina wordt binnen 1 seconde geladen	Kwaliteit	Must	FT1
NFR3		De pagina is publiek toegankelijk	Beperking	Must	
US2	IV1	Als gebruiker wil ik een bericht kunnen sturen aan een developer zodat ik in contact kan komen met een developer		Must	Functioneel
FR2		De gebruiker gegevens die worden meegestuurd: voornaam en achternaam, email, telefoonnummer	AS1	Must	
NFR4		Na het versturen van het bericht zijn de gegevens niet meer zichtbaar in het formulier	Beperking	Must	FT2
FR4		De gebruiker ontvangt feedback over de status van het verstuurde bericht	Functioneel	Must	FT3
NFR5		De persoonsgegevens worden niet opgeslagen in het systeem	Beperking	Must	FT4

1.1 Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS1	voornaam en achternaam, email, telefoonnummer	FR2	UC#		
#	**Beschrijving**	**Kans[1]**		**Impact[2]**	**Risk**
RSK1	ASVS 5.1.3 Lange invoer leidt tot systeem crash	Hoog		Groot	SM1
RSK2	ASVS 5.1.4 Invoer is invalide doordat data niet strong typed is	Hoog		Groot	SM2
RSK3	ASVS 5.1.5 Injectie van scripts in de invoer	Hoog		Groot	SM3
#	**Beschrijving**	**Test**		**Status**	
SM1	Gebruiker gegevens zijn gebonden aan een maximum lengte zowel clientside, als serverside	FT5		Niet uitgevoerd	
SM2	Gebruiker gegevens zijn strong typed.	FT6		Niet uitgevoerd	
SM3	Request data wordt server side sanitized.	FT7		Niet uitgevoerd	

[1] **Threat Agent Factors**: Skill level, Motive, Opportunity, Size. **Vulerability Factors**: Ease of Discovery, Ease of Exploit, Awareness, Intrusion Detection.

[2] **Technical Impact Factors**: Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Accountability. **Business Impact Factors**: Financial damage, Reputation damage, Non-compliance, Privacy violation.

2 IV1 Verslag interview opdrachtgever

Opdrachtgever:	Karen Brakband
Notulist:	Ernst Bolt
Aanwezigen:	Karen Brakband, Bram Abbekerk, Thomas Boose, Henk Bosman, John Brouwers, Martijn ter Schegget, Aad Glasbergen, Richard Hulsing, Ernst Bolt
Onderwerp:	Verzamelen requirements
Datum:	17-5-2023
Locatie:	Hanzegebouw Zwolle

Dit is het verslag van het interview met de opdrachtgever. Het gesprek dient als basis voor het verzamelen van requirements.

De aanwezigen willen een systeem waarmee ze makkelijker hun technische skills aan de buitenwereld kunnen laten zien. De buitenwereld is in dit geval, iedereen die op internet op zoek is naar een developer. Gedacht wordt aan een webapplicatie waarmee gebruikers inzicht krijgen in de technische vaardigheden van de developers. Dit zou kunnen lijken op een CV[3]. Omdat de gegevens niet vaak wijzigen hoeft er niet een uitgebreid systeem te komen om gegevens te wijzigen. Verder is het van belang dat de site snel is, maximale laadtijd is één seconde.
Ter tafel komt dat het belangrijk is dat gebruikers contact op kunnen nemen met de developer. Dit voorkomt dat gebruikers via de gegevens van het bedrijf, via de front office contact opnemen.

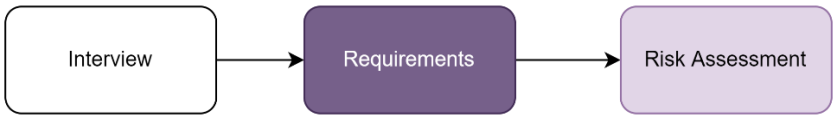
Verder wordt in een vervolg gedacht aan het onder de aandacht brengen van de skills van een developer, een showcase. Deze showcase kan bijvoorbeeld een spel zijn, of een andere uitbreiding die laat zien wat de developer kan. Dit onderdeel behoeft verdere uitwerking.

[3] Als de profielpagina de gegevens bevat van jou zelf, dan kun je deze applicatie gaan gebruiken voor een sollicitatie naar een stage voor Webdev in de volgende periode.

3 Bijlage 1 Aanpak Requirements Analyse

In deze bijlage een overzicht van de stappen die genomen zijn om te komen tot verantwoorde requirements.

Eerst een schematische weergave van de stappen:



Figuur 1 Requirements proces

3.1 Requirements Traceability

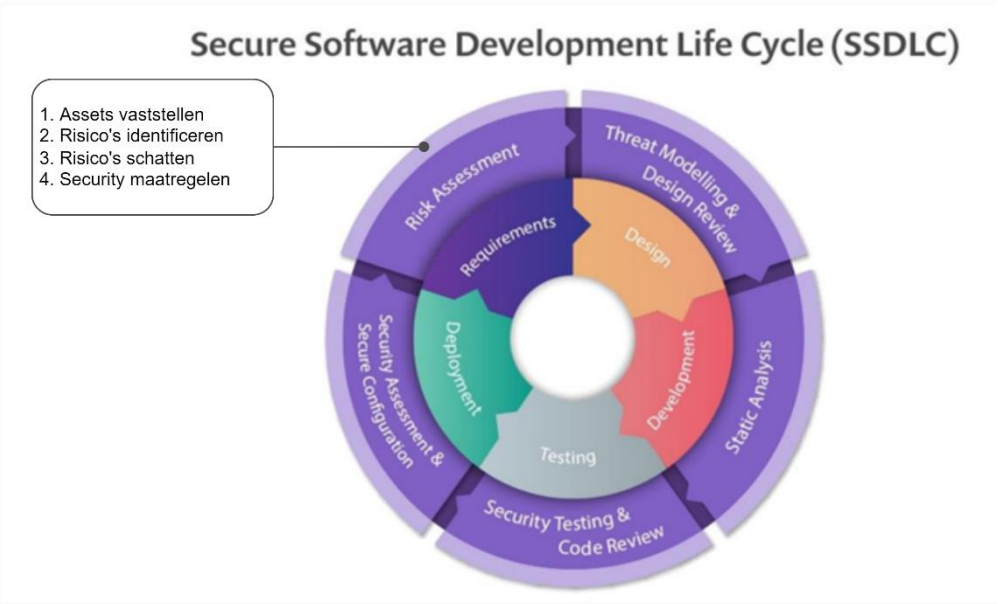
Voor de navolgbaarheid van de requirements gedurende het proces, de zogenoemde traceability, wordt hierna ingegaan hoe dit bereikt wordt. Datadragers in de documentatie worden voorzien van een id:

Onderwerp	**Id**
interview	IV<#>
functionele requirement	FR<#>
non functionele requirement	NFR<#>
asset	AS<#>
risk	RSK<#>
security measurement	SM<#>
userstory	US<#>
acceptatie criterium	AC<#>
functionele test	FT<#>
unit test	UT<#>
configuratie item	CI<#>

In documentatie wordt altijd verwijzen naar een bovenliggende bron, behalve bij interviews. Voorbeeld: een functionele requirement FR1 verwijst naar interview IV1. Zo is vanuit code, inclusief testen te herleiden tot welke requirements zijn geïmplementeerd.

3.2 Van Requirements naar Risk mitigation

De elicitatie van de requirements is uitgevoerd in de volgende stappen. De start van het proces is een interview met de opdrachtgever geweest. Uit dit interview zijn requirements verzameld en vastgelegd in dit document. Daarna is een Risk Assessment uitgevoerd in drie stappen die hierna beschreven zijn. Samengevat in onderstaande diagram.



Figuur 2 Risk management

In latere stappen is steeds weer gekeken of de Requirements aangepast of uitgebreid moesten worden. Dan werden de stappen van Risk Assessment opnieuw doorlopen.

3.3 Risk Assessment stap 1: Assets vaststellen

Om risico's te kunnen identificeren worden eerst de assets bepaald vanuit de vastgelegde requirements. Assets zijn hardware, software, materiële zaken en immateriële onderdelen van het systeem.
Per asset is bepaald welke risico's een rol spelen. Om hier achter te komen zijn persoonsgegevens gemarkeerd als asset. Naast het raadplegen van de AVG voor noodzakelijke maatregelen is gekeken of al sprake is van hardware of software waar rekeningen mee gehouden moet worden. Dit was nog niet het geval.

Voorbeeld: *voornaam en achternaam is een persoonsgegeven volgens de AVG. Dit is dus een asset. De asset is apart vastgelegd met een eigen identificatie.*

3.4 Risk Assessment stap 2: Risico's identificeren

Aan de hand van de hoofdstukken in de ASVS bekeken welke onderwerpen relevant zijn. Per requirement zijn de risico's beschreven.

Voorbeeld: *voornaam en achternaam worden ingevuld in een online formulier. Om achter relevante ASVS items te komen is op de website https://asvs-for-dummies.pages.dev gekeken naar relevante hoofdstukken in de ASVS. In dit geval: Validation, Sanitization and Encoding. Ook andere hoofdstukken hadden gekund, zoals API and Web Service.*
De risico's zijn bij de asset vastgelegd. Vervolgens is een classificatie toegepast.

3.5 Risk Assessment stap 3: Risico's schatten

De grootte van het risico wordt bepaald door de kans te vermenigvuldigen met de impact:

kans * impact = grootte risico

De schatting kan op drie manieren worden uitgevoerd:

- Eén of meer stakeholders de schatting laten uitvoeren (eventueel middelen van de uitkomst)
- Voor kans en impact de factoren bepalen die van invloed zijn en deze laten *schatten* door stakeholders
- Voor kans en impact de factoren bepalen die van invloed zijn en deze laten *scoren* door stakeholders en deze vervolgens middelen

De Risk Rating Methodology (RRM) van OWASP gebruikt de volgende factoren:

Table 1 Factoren om kans en impact te schatten

Factors for estimating likelihood and impact	
Likelihood	
Threat Agent Factors	Skill level, Motive, Opportunity, Size
Vulnerability Factors	Ease of Discovery, Ease of Exploit, Awareness, Intrusion Detection
Impact	
Technical Impact Factors	Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Accountability
Business Impact Factors	Financial damage, Reputation damage, Non-compliance, Privacy violation

De link naar RRM laat met een voorbeeld zien hoe je de factoren kunt koppelen aan een schaal, deze kunt scoren en berekenen.

Voorbeeld*: In een gesprek met de lead developer zijn de factoren van kans en impact per risico langsgelopen en vastgelegd bij de requirements. Daarna is het bijgewerkte requirements document naar de lead developer en de opdrachtgever gestuurd. Dit is vastgelegd in de distributielijst. Bij deze schatting is wel gebruik gemaakt van de factoren, maar deze zijn niet gescoord.*

3.6 Risk Assessment stap 4: Security Maatregelen

Voor zaken met een middelmatig en hoog risico worden security maatregelen vastgesteld.

Voorbeeld*: Aan de hand van de risico classificatie is bepaald welke voor welke risico's security measurements worden genomen. In de Quick Reference Guide van OWASP zijn bijpassende maatregelen opgezocht en gekozen. Deze maatregelen zijn bij het risico opgenomen.*