Requirementsanalyse

Planning Poker

Versie 1.0

Timme Kingma  
2025

# Distributie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Wijzigingen | Ontvangers |

Inhoud

[Distributie 2](#_Toc190461688)

[Inleiding 4](#_Toc190461689)

[Nog te verwerken requirements 4](#_Toc190461690)

[1.1 UC1 4](#_Toc190461691)

[Functionele requirements 4](#_Toc190461692)

[Niet-functionele requirements 4](#_Toc190461693)

[2 Requirements 5](#_Toc190461694)

[2.1 UC1 5](#_Toc190461695)

[2.1.1 Risk assessment 5](#_Toc190461696)

[3 Bijlage 3 Aanpak Requirements Analyse 7](#_Toc190461697)

[3.1 Requirements Traceability 7](#_Toc190461698)

[3.2 Van Requirements naar Risk mitigation 7](#_Toc190461699)

[3.3 Risk Assessment stap 1: Assets vaststellen 8](#_Toc190461700)

[3.4 Risk Assessment stap 2: Risico’s identificeren 8](#_Toc190461701)

[3.5 Risk Assessment stap 3: Risico’s schatten 9](#_Toc190461702)

[3.6 Risk Assessment stap 4: Security Maatregelen 9](#_Toc190461703)

# Inleiding

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

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.

Onderaan deze pagina staan requirements die je verwerkt in de analyse.

# Nog te verwerken requirements

## UC1

### Functionele requirements

|  |
| --- |
| Beschrijving |
| Het profiel bevat een overzicht van skills |
| Het profiel bevat een beschrijving/introductie van de developer |
| Het profiel bevat een afbeelding van de developer: meerdere afbeeldingen toegestaan, slideshow met afbeeldingen is toegestaan |
| De site bevat een manier van thema te verwisselen voor light/dark modus. |

### Niet-functionele requirements

|  |  |
| --- | --- |
| Vak | Beschrijving |
| Client | De gebruikte HTML-tags zijn semantisch waar dit mogelijk is |
|  | Het design is Mobile First |
|  | Het design is Responsive |
|  | De profiel pagina bevat een GDPR (ASVS V8.3 Sensitive Private Data) |
|  | De GDPR-keuze wordt opgeslagen (cookie of localstorage) |
|  | GDPR wordt alleen getoond als er geen consent is gegeven |
|  | Styling GDPR past bij pagina |
|  | Lightmode/Darkmode implementatie en bijbehoren styling |
|  | De thema modes work opgeslagen (cookie of localstorage) |
| Server | N.V.T. |

# Requirements

In dit hoofdstuk zijn de requirements uitgewerkt. De requirements zijn per use case 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 Bijlage 2 Aanpak.

## UC1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Bron | Beschrijving | Asset/Type | MoSCoW | Testen |
| UC1 | IV1 | Als gebruiker wil ik de CV van een developer kunnen zien zodat ik me kan oriënteren voordat ik contact leg |  | Must | Functioneel |
| FR1 |  | Het profiel bevat een overzicht van de skills van de developer. | Functioneel | Must | FT1 |
| FR2 |  | Het profiel bevat een beschrijving/introductie van de developer. | Functioneel | Must | FT1 |
| FR3 |  | Het profiel bevat een afbeelding van de developer, meerdere afbeeldingen toegestaan, slideshow met afbeeldingen is toegestaan. | Functioneel | Must | FT1 |
| FR4 |  | De site bevat een manier van thema te verwisselen voor light/dark modus. | Functioneel | Could have | FT2 |
| NFR1 |  | De gegevens op de pagina zijn niet via de webpagina te beheren | Beperking | Must | FT1 |
| NFR2 |  | De pagina wordt binnen 1 seconde geladen | Kwaliteit | Must | FT1 |
| NFR3 |  | De gebruikte HTML-tags zijn semantisch waar dit mogelijk is. | Kwaliteit | Must | FT1 |
| NFR4 |  | Het design is Mobile First en Responsive | Kwaliteit | Must | FT3 |
| NFR5 |  | De profielpagina bevat een GDPR-verklaring (ASVS V8.3 - Sensitive Private Data). | Kwaliteit | Must | FT4 |
| NFR6 |  | De GDPR-keuze wordt opgeslagen in een cookie of local storage. | Kwaliteit | Must | FT4 |
| NFR7 |  | De GDPR wordt alleen getoond als er geen consent is gegeven. | Kwaliteit | Must | FT4 |
| NFR8 |  | Styling van de GDPR past bij de pagina. | Kwaliteit | Must | FT4 |
| NFR9 |  | De Lightmode/Darkmode-implementatie is aanwezig en de bijbehorende styling is correct. |  | Could have | FT2 |
| NFR10 |  | De thema-modus wordt opgeslagen in een cookie of local storage. | Kwaliteit | Could have | FT2 |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Profielfoto van de developer | Persoonlijke data(mogelijk AVG) | (autoriteitpersoonsgegevens, 2025) |
| AS2 | Cookievoorkeuren | Privacygevoelige data |  |
| AS3 | Light/Dark mode voorkeur | Niet-gevoelige gebruikersdata |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Ongeautoriseerde toegang tot of scraping van de profielfoto | AS1 | V1.12 Secure File Upload Architectural Requirements |
| RSK2 | Manipulatie of diefstal van cookievoorkeuren door een aanvaller. | AS2 | V3.4 Cookie-based Session Management |
| RSK3 | Gebruikersvoorkeurenn (dark mode) kunnen worden gewijzigd door een derde partij via JS injection. | AS3 | V5.3 Output encoding and Injection Prevention Requirements |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 2 | 1 | 2 | Laag |
| RSK2 | 3 | 1 | 3 | Laag |
| RSK3 | 2 | 1 | 2 | Laag |

#### **Risico’s schatting**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Beperk toegang tot profielfoto via cors in de .htacces bestand | Niet geïmplementeerd |
| SM2 | RSK2 | Gebruik httponly. Secure en samesite strickt cookies op de server | Niet geïmplementeerd |
| SM3 | RSK3 | Gebruik (constent security policy) om js injection te voorkomen | Geïmplementeerd |

# Bijlage 3 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:

Afbeelding met tekst, schermopname, Lettertype, ontwerp

Automatisch gegenereerde beschrijving

Figuur Requirements proces

## 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.

## 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.

Afbeelding met tekst, schermopname, cirkel, diagram

Automatisch gegenereerde beschrijving

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.

## 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.*

## Risk Assessment stap 2: Risico’s identificeren

Aan de hand van de [hoofdstukken in de ASVS](https://asvs-for-dummies.pages.dev/) 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.*

## 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](https://owasp.org/www-community/OWASP_Risk_Rating_Methodology) (RRM) van OWASP gebruikt de volgende factoren:

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.*

## 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.*