Requirementsanalyse

UC2 Contactpagina

Niveau 2

Team SE  
2024

# Distributie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Wijzigingen | Ontvangers |
| Versie | Datum | Wijzigingen | Ontvangers |
| 0.1 | 21-5-2024 | Initiële versie | Karen |
| 1.0 | 4-6-2024 | Scope requirements aangepast | Ernst |
| 1.1 | 21-8-2024 | Laatste controle op fouten en inconsistenties | Ernst |
| 1.2 | 21-7-2024 | Initiële versie | Karen |
| 2.0 | 21-8-2024 | Laatste controle op fouten en inconsistenties | Ernst |

Inhoud

[Distributie 2](#_Toc189819443)

[Inleiding 4](#_Toc189819444)

[Nog te verwerken requirements 4](#_Toc189819445)

[1.1 UC1 4](#_Toc189819446)

[Functionele requirements 4](#_Toc189819447)

[Niet-functionele requirements 4](#_Toc189819448)

[1.2 UC2 5](#_Toc189819449)

[Functionele requirements 5](#_Toc189819450)

[Niet-functionele requirements 5](#_Toc189819451)

[2 Requirements 6](#_Toc189819452)

[2.1 UC1 6](#_Toc189819453)

[2.1.1 Risk assessment 6](#_Toc189819454)

[2.2 UC2 7](#_Toc189819455)

[2.2.1 Risk assessment 7](#_Toc189819456)

[3 Bijlage 1 IV1 Verslag interview opdrachtgever 8](#_Toc189819457)

[4 Bijlage 2 IV1 Verslag interview opdrachtgever 9](#_Toc189819458)

[5 Bijlage 3 Aanpak Requirements Analyse 10](#_Toc189819459)

[5.1 Requirements Traceability 10](#_Toc189819460)

[5.2 Van Requirements naar Risk mitigation 10](#_Toc189819461)

[5.3 Risk Assessment stap 1: Assets vaststellen 11](#_Toc189819462)

[5.4 Risk Assessment stap 2: Risico’s identificeren 11](#_Toc189819463)

[5.5 Risk Assessment stap 3: Risico’s schatten 12](#_Toc189819464)

[5.6 Risk Assessment stap 4: Security Maatregelen 12](#_Toc189819465)

# 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. |

## UC2

### Functionele requirements

|  |
| --- |
| Beschrijving |
| De pagina bevat de naam van de student-webdeveloper |
| Het formulier bevat een invoer voor het onderwerp |
| Het formulier bevat een invoer voor e-mailadres |
| Het formulier bevat een text input voor het bericht |
| Wanneer het formulier verstuurd wordt, ontvangt de student-webdeveloper een mail met de ingevulde gegevens |
| Het formulier bevat een captcha |

### Niet-functionele requirements

|  |  |
| --- | --- |
| Vak | Beschrijving |
| Client | Het formulier wordt alleen verstuurd als de invoervelden valide zijn |
|  | Voorwaarden voor de invoervelden: a. Onderwerp, niet langer dan 200 tekens, b. E-mail, valide e-mailadres, c. Bericht, niet langer dan 600 tekens |
|  | Het formulier bevat een captcha (simpel met een som óf ingewikkelder bijvoorbeeld Recaptcha v2/3) |
| Server | Er wordt een POST-request gedaan naar de MailController in het (REST-API) project ShowcaseAPI, met daarin de ingevulde gegevens uit het contactformulier |
|  | Voor het versturen van de mail wordt gebruikgemaakt van een mail delivery service zoals Mailtrap |
| Security | De contactpagina mag wel een beperkte set HTML opmaak attributen toestaan zoals opsommingen, bold of headers maar in ieder geval geen scripts, verborgen tekst of tekst in de kleur van de achtergrond. |
|  | De contactpagina is beschermd met een CAPTCHA (ASVS V2.2 General Authenticator Security) |

# 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 |

## UC2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Bron | Beschrijving | Asset/Type | MoSCoW | Testen |
| UC2 | IV1 | Als geïnteresseerde wil ik een bericht kunnen sturen aan de student-webdeveloper zodat ik in contact kan komen met de student-webdeveloper |  | Must | Functioneel |
| FR2 |  | De gegevens van de geïnteresseerde die worden meegestuurd: voornaam en achternaam, e-mail, telefoonnummer | AS1 | Must | FT1 |
| NFR4 |  | Na het versturen van het bericht zijn de gegevens niet meer zichtbaar in het formulier | Beperking | Must | FT5 |
| FR4 |  | De gebruiker ontvangt feedback over de status van het verstuurde bericht | Functioneel | Must | FT5 |
| NFR5 |  | De persoonsgegevens worden niet opgeslagen in het systeem | Beperking | Must | FT5 |
| FR5 |  | De pagina bevat de naam van de student-webdeveloper. | Functioneel | Must | FT1 |
| FR6 |  | Het formulier bevat een invoer voor het onderwerp. | Functioneel | Must | FT1 |
| FR7 |  | Het formulier bevat een invoer voor e-mailadres. | Functioneel | Must | FT5 |
| FR8 |  | Het formulier bevat een text input voor het bericht. | Functioneel | Must | FT5 |
| FR9 |  | Wanneer het formulier verstuurd wordt, ontvangt de student-webdeveloper een mail met de ingevulde gegevens. | Functioneel | Must | FT5 |
| FR10 |  | Het formulier bevat een captcha. | Functioneel | Must | FT5 |
| NFR1 | client | Het formulier wordt alleen verstuurd als de invoervelden valide zijn. | Validatie | Must | FT5/FT6 |
| NFR2 | client | Voorwaarden voor de invoervelden: a. Onderwerp, niet langer dan 200 tekens, b. E-mail, valide e-mailadres, c. Bericht, niet langer dan 600 tekens. | Validatie | Must | FT6 |
| NFR3 | client | Het formulier bevat een captcha (simpel met een som óf ingewikkelder bijvoorbeeld Recaptcha v2/3). | Validatie | Must | FT6 |
| NFR6 | Server | Er wordt een POST-request gedaan naar de MailController in het (REST-API) project ShowcaseAPI, met daarin de ingevulde gegevens uit het contactformulier. | kwaliteit | Must | FT5 |
| NFR7 | Server | Voor het versturen van de mail wordt gebruikgemaakt van een mail delivery service zoals Mailtrap. | Techniek | Must | FT5 |
| NFR8 | Security | De contactpagina mag wel een beperkte set HTML-opmaak attributen toestaan zoals opsommingen, bold of headers maar in ieder geval geen scripts, verborgen tekst of tekst in de kleur van de achtergrond. | Security | Must | FT5 |
| NFR9 | Security | De contactpagina is beschermd met een CAPTCHA (ASVS V2.2 General Authenticator Security). | Security | Must | FT5/FT6 |

### Risk assessment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Asset | Bron | Koppeling | | Test/Security Measurement | |
| AS1 | Voornaam en achternaam, e-mail, telefoonnummer | FR2 | | UC# |  |  |
| # | **Beschrijving** | **Kans[[1]](#footnote-2)** | | | **Impact[[2]](#footnote-3)** | **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** |  |
| SM4 | Ingevoerde gegevens zijn gebonden aan een maximum lengte zowel clientside, als serverside | FT5 | | | Niet uitgevoerd |  |
| SM5 | Ingevoerde gegevens zijn strong typed. | FT6 | | | Niet uitgevoerd |  |
| SM6 | Request data wordt server side sanitized. | FT7 | | | Niet uitgevoerd |  |

# Bijlage 1 IV1 Verslag interview opdrachtgever

Opdrachtgever: Karen Brakband

Notulist: Ernst Bolt

Aanwezigen: Karen Brakband

Onderwerp: Verzamelen requirements profielpagina

Datum: 17-5-2024

Locatie: Hanzegebouw Zwolle

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

De opdrachtgever wil dat de student-webdeveloper een systeem ontwerpt en realiseert, waarmee deze makkelijk de technische skills aan de buitenwereld kan laten zien. In de tweede periode van het semester Web Development moet de student namelijk een web development opdracht doen voor een bedrijf, en het is belangrijk dat de student kan laten zien wat die aan technische vaardigheden in huis heeft. Op dit moment kan het bedrijf niet zien wat de technische vaardigheden van de student-webdeveloper zijn.

Het nieuwe systeem zou kunnen lijken op een CV[[3]](#footnote-4), maar dan in de vorm van een webapplicatie. Omdat de gegevens niet vaak veranderen hoeft er geen webpagina te komen om gegevens te wijzigen. Wel is het van belang dat de site snel is. Daarmee bedoelt de opdrachtgever dat de maximale laadtijd één seconde is.

# Bijlage 2 IV1 Verslag interview opdrachtgever

Opdrachtgever: Karen Brakband

Notulist: Ernst Bolt

Aanwezigen: Karen Brakband

Onderwerp: Verzamelen requirements contactpagina

Datum: 17-7-2024

Locatie: Hanzegebouw Zwolle

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

Eerder is al een systeem gerealiseerd waarmee makkelijk de student-webdeveloper makkelijk de technische skills aan de buitenwereld kan laten zien. De samenwerking is goed bevallen, en daarom wil de opdrachtgever nu graag dat er ook een systeem gerealiseerd wordt waarbij een geïnteresseerde contact op kan nemen met de student-webdeveloper.

Geïnteresseerden moeten hun voornaam, achternaam, e-mailadres en telefoonnummer achter kunnen laten via een contactformulier. Als iemand het contactformulier verstuurt, dan moet de student-webdeveloper daarvan een mail ontvangen. Voor nu is het voldoende als de mail bekeken kan worden in Mailtrap of een vergelijkbaar systeem.

# 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:

Table 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.*

## 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.*

1. **Threat Agent Factors**: Skill level, Motive, Opportunity, Size. **Vulerability Factors**: Ease of Discovery, Ease of Exploit, Awareness, Intrusion Detection. [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
3. Als de profielpagina de gegevens bevat van jou zelf, dan kun je deze applicatie gaan gebruiken voor een sollicitatie naar een project voor Webdev in de volgende periode. [↑](#footnote-ref-4)