Requirementsanalyse

Planning Poker

Versie 1.0

Timme Kingma  
2025

# Distributie

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

Inhoud

[Distributie 2](#_Toc190624873)

[Inleiding 4](#_Toc190624874)

[1 Requirements 5](#_Toc190624875)

[1.1 UC1 5](#_Toc190624876)

[2 Bijlage 3 Aanpak Requirements Analyse 8](#_Toc190624877)

[2.1 Requirements Traceability 8](#_Toc190624878)

[2.2 Van Requirements naar Risk mitigation 8](#_Toc190624879)

[2.3 Risk Assessment stap 1: Assets vaststellen 9](#_Toc190624880)

[2.4 Risk Assessment stap 2: Risico’s identificeren 9](#_Toc190624881)

[2.5 Risk Assessment stap 3: Risico’s schatten 10](#_Toc190624882)

[2.6 Risk Assessment stap 4: Security Maatregelen 10](#_Toc190624883)

# 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.

# 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.

## Toelichtingen

In dit hoofdstuk wordt aan de hand van verschillende tabellen, afkortingen en termen verder toegelicht die in dit hele bestand worden gebruikt.

### Requirments

|  |  |
| --- | --- |
| 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<#> |

### MoSCoW

|  |  |
| --- | --- |
| **Definitie** | **Toelichting** |
| **M (Must)** | Verplichte onderdelen. Zonder deze vereisten kan het project niet als succesvol worden beschouwd. |
| **S (Should)** | Belangrijke onderdelen die niet essentieel zijn, maar een aanzienlijke toegevoegde waarde bieden als ze worden geïmplementeerd. |
| **C (Could)** | Wenselijke onderdelen die leuk zijn om te hebben, maar kunnen worden uitgesteld zonder grote impact. |
| **W (Won't)** | Zaken die voorlopig niet worden geïmplementeerd, mogelijk wel in toekomstige iteraties. |

### Assets/Type

|  |  |
| --- | --- |
| **Asset/Type** | **Toelichting** |
| Functioneel | Beschrijft de gewenste functionaliteit van het systeem |
| Beperking | Geeft aan welke beperkingen of randvoorwaarden gelden |
| Security | Richt zich op beveiligingsmaatregelen. |
| Validatie | Bevat regels voor het valideren van invoervelden. |
| kwaliteit | Omvat technische en prestatienormen. |
| UX | UX staat voor user experience en richt op wat fijn werkt/voelt voor een bezoeker |

### Risico Niveau’s

|  |  |  |
| --- | --- | --- |
| **Risico Niveau** | **Toelichting** | **Score Threshold** |
| Laag | Het laagste niveau wat er is ingrijpen zou handig zijn maar niet perse genoodzaakt. | 0-5 |
| Medium | Net een niveau boven laag zit het medium niveau. Hierbij is het handig om te kijken naar de impact van de dreiging en vervolgens te beoordelen of ingrijpen nodig is of niet. | 5-10 |
| Hoog | Het niveau hoog is urgent, er zijn mogelijke risico’s met een grote impact als ze door een hacker worden gemanipuleerd. | 10-20 |
| Kritisch | Het kritische niveau is nog ernstiger, dit is het hoogste risiconiveau. Hackers kunnen hierbij de applicatie op een andere manier laten werken of eenvoudig toegang krijgen tot belangrijke gegevens, deze bewerken of andere dreigingen veroorzaken. Hierop reageren is dringend! | 20+ |

## Use Case: Bekijken Home pagina

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
| De homepagina moet toegankelijk iedereen. |
| De homepagina moet informatie tonen over het planning poker. |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
| 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 |
| De gegevens op de pagina zijn niet via de webpagina te beheren. |
| De pagina wordt binnen 1 seconde geladen. |

### Requirments overzicht

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Beschrijving | Asset/Type | MoSCoW | Testen |
| FR1 | De homepagina moet toegankelijk zijn voor iedereen. | Functioneel | Must |  |
| FR2 | De homepagina moet informatie tonen over het planning poker. | Functioneel | Must |  |
| FR3 | De gebruikte HTML-tags zijn semantisch waar dit mogelijk is. | Kwaliteit | Should |  |
| FR4 | Het design is Mobile First. | UX | Must |  |
| NFR1 | Het design is Responsive. | UX | Must |  |
| NFR2 | de profielpagina bevat een GDPR (ASVS V8.3 Sensitive Private Data). | Kwaliteit | Must |  |
| NFR3 | De GDPR-keuze wordt opgeslagen (cookie of localStorage). | Kwaliteit | Must |  |
| NFR4 | GDPR wordt alleen getoond als er geen consent is gegeven. | Kwaliteit | Must |  |
| NFR5 | Styling van GDPR past bij de rest van de pagina. | UX | Must |  |
| NFR8 | De gegevens op de pagina zijn niet via de webpagina te beheren. | Beperking | Must |  |
| NFR9 | De pagina wordt binnen 1 seconde geladen. | Kwaliteit | Must |  |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Webpagina code | Software |  |
| AS2 | Cookievoorkeuren | Gegevens |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Ongeautoriseerde toegang tot of scraping van de webpagina-code | 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 | Cross-Site Scripting (XSS) aanval waarbij schadelijke scripts via de webpagina worden uitgevoerd. | AS1 | V3.3 Cross-Site Scripting Prevention |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 2 | 2 | 4 | Laag |
| RSK2 | 3 | 3 | 9 | Middel |
| RSK3 | 4 | 4 | 16 | Hoog |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Beperk toegang tot webpagina via robots.txt en implementeer rate limiting. | Niet geïmplementeerd |
| SM2 | RSK2 | Gebruik HttpOnly, Secure en SameSite=Strict cookies om cookie hijacking te voorkomen. Voeg ook Encyptie toe om cookies niet aanpas baar te maken voor gebruikers. | Niet geïmplementeerd |
| SM3 | RSK3 | Gebruik een Content Security Policy (CSP) om XSS-aanvallen te blokkeren. | Niet geïmplementeerd |

## Use Case: Acountcreatie

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
| Een developer kan een account aanmaken. |
| De developer moet zijn account verifiëren via e-mailauthenticatie. |
| De developer kan inloggen met zijn nieuwe account. |
| Bij het inloggen kan de developer alsnog zijn account verifiëren als dit niet eerder is gebeurd. |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
| Verificatie via e-mail is vereist voor accountactivatie. |
| De sessie/cookie wordt opgeslagen voor 15 dagen. |
| De authenticatie voldoet aan best practices zoals hashing en beveiligde sessies. |
| Alleen veilige wachtwoorden worden geaccepteerd (min. 8 tekens, cijfers, speciale tekens). |
| Foutmeldingen mogen geen gevoelige informatie lekken. |
| Email word gevalideerd op een geldig adress. |

### Requirments overzicht

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Beschrijving | Asset/Type | MoSCoW | Testen |
| FR1 | Een developer kan een account aanmaken. | Functionaliteit | Must |  |
| FR2 | De developer moet zijn account verifiëren via e-mailauthenticatie. | Functionaliteit | Must |  |
| FR3 | De developer kan inloggen met zijn nieuwe account. | Functionaliteit | Must |  |
| FR4 | Bij het inloggen kan de developer alsnog zijn account verifiëren als dit niet eerder is gebeurd. | Functionaliteit | Must |  |
| NFR1 | Verificatie via e-mail is vereist voor accountactivatie. | Security | Must |  |
| NFR2 | De sessie/cookie wordt opgeslagen voor 15 dagen. | Security | Should have |  |
| NFR3 | De authenticatie voldoet aan best practices zoals hashing en beveiligde sessies. | Security | Must |  |
| NFR4 | Alleen veilige wachtwoorden worden geaccepteerd (min. 8 tekens, cijfers, speciale tekens). | Validatie | Must |  |
| NFR5 | Foutmeldingen mogen geen gevoelige informatie lekken. | Security | Must |  |
|  | Email word gevalideerd op een geldig adress. | Validatie | Must |  |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Accountgegevens (gebruikersnaam, wachtwoordhash, e-mail) | Gegevens |  |
| AS2 | Sessiecookies | Gegevens |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Onbevoegde toegang tot accountgegevens door een datalek. | AS1 | V2.1 Password Storage |
| RSK2 | Sessiehijacking: een aanvaller steelt een actieve sessie. | AS2 | V3.4 Cookie-based Session Management |
| RSK3 | Brute-force aanvallen op het inlogscherm. | AS1 | V2.2 Authentication |
| RSK4 | hishing-aanvallen via valse verificatiemails. | AS1 | V5.2 Verify Email Ownership |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 3 | 5 | 15 | Hoog |
| RSK2 | 4 | 4 | 16 | Hoog |
| RSK3 | 3 | 3 | 9 | Middel |
| RSK4 | 3 | 3 | 9 | Middel |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Versleutel wachtwoorden met bcrypt. | Niet geïmplementeerd |
| SM2 | RSK2 | Gebruik HttpOnly, Secure en SameSite=Strict cookies om sessies te beschermen. Encrypt cookies voor extra security | Niet geïmplementeerd |
| SM3 | RSK3 | Implementeer rate limiting (bijv. 5 pogingen per minuut) op het inlogscherm. | Niet geïmplementeerd |
| SM4 | RSK4 | Gebruik DKIM en SPF om phishing te verminderen en informeer gebruikers over verificatiemails. | Niet geïmplementeerd |

## Use Case: Game starten

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
| De Scrum Master moet een game kunnen starten. |
| De Scrum Master moet de game-instellingen kunnen configureren (zoals naam, timer en type stemmen). |
| De game moet een unieke ID genereren bij het aanmaken. |
| Spelers moeten kunnen deelnemen via een unieke link en gamecode. |
| De Scrum Master moet de game kunnen annuleren voordat deze wordt gestart. |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
| De game moet real-time updates ondersteunen voor deelnemers. |
| De gegenereerde game-ID’s moeten veilig en niet voorspelbaar zijn. |
| De game moet schaalbaar zijn voor meerdere gelijktijdige games. |

### Requirments overzicht

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Beschrijving | Asset/Type | MoSCoW | Testen |
| FR1 | De Scrum Master moet een game kunnen starten. | Functionaliteit | Must |  |
| FR2 | De Scrum Master moet de game-instellingen kunnen configureren (zoals naam, timer en type stemmen). | Functionaliteit | Should have |  |
| Fr3 | De game moet een unieke ID genereren bij het aanmaken. | Functionaliteit | Must |  |
| FR4 | Spelers moeten kunnen deelnemen via een unieke link en gamecode. | Functionaliteit | Must |  |
| FR5 | De Scrum Master moet de game kunnen annuleren voordat deze wordt gestart. | Functionaliteit | Should have |  |
| NFR1 | De game moet real-time updates ondersteunen voor deelnemers. | Functionaliteit | Must |  |
| NFR2 | De gegenereerde game-ID’s moeten veilig en niet voorspelbaar zijn. | Security | Should have |  |
| NFR3 | De game moet schaalbaar zijn voor meerdere gelijktijdige games. | Kwaliteit | Should have |  |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Game-instellingen(naam timer type stemmen) | Gegevens |  |
| AS2 | Game-ID en sessie data | Gegevens |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Ongeautoriseerde gebruikers starten een game zonder rechten. | AS1 | V2.2 Authentication |
| RSK2 | Game-ID’s zijn voorspelbaar, waardoor anderen games kunnen joinen zonder uitnodiging. | AS2 | V3.4 Session Management |
| RSK3 | Een kwaadwillende gebruiker start te veel games, wat de server overbelast. | AS2 | V7.5 Denial of Service |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 2 | 4 | 8 | Middel |
| RSK2 | 4 | 4 | 16 | Hoog |
| RSK3 | 4 | 5 | 20 | Kritisch |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Verifieer de rol binnen de applicatie zodat de gene die de game start de juiste rechten heeft voordat een game gestart wordt. | Niet geïmplementeerd |
| SM2 | RSK2 | Gebruik cryptografisch sterke UUIDs voor game-ID’s. | Niet geïmplementeerd |
| SM3 | RSK3 | Implementeer rate limiting en een maximumaantal actieve games per IP. | Niet geïmplementeerd |

## Use Case: Game joinen

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
| Een speler kan via een link op de juiste gamepagina komen. |
| Een speler kan een eigen naam invoeren of inloggen. |
| Een speler developer moet een geldige code invoeren om zichzelf te verifiëren. |
| Een speler kan succesvol een game joinen. |
| Er wordt een foutmelding weergegeven als de game niet meer bestaat. |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
| De verificatiecode moet uniek en moeilijk te raden zijn. |
| de gamepagina moet binnen 2 seconden laden.(delay mag door realtime sync) |
| De UI moet duidelijke foutmeldingen tonen bij een mislukte login of ongeldig spel. |
| De game moet real-time updates ontvangen zodra de developer succesvol joined. |
| Er mogen geen gevoelige gegevens in de URL worden opgeslagen. |
| Als er twee mensen met de zelfde naam zijn moeten ze in de UI verschillend zijn door kleur of icon. |

### Requirments overzicht

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Beschrijving | Asset/Type | MoSCoW | Testen |
| FR1 | Een speler kan via een link op de juiste gamepagina komen. | Functionaliteit | Must |  |
| FR2 | Een speler kan een eigen naam invoeren of inloggen. | Functionaliteit | Should have |  |
| FR3 | Een speler developer moet een geldige code invoeren om zichzelf te verifiëren. | Security | Must |  |
| FR4 | Een speler kan succesvol een game joinen. | Functionaliteit | Must |  |
| FR5 | Er wordt een foutmelding weergegeven als de game niet meer bestaat. | UX | Should have |  |
| NFR1 | De verificatiecode moet uniek en moeilijk te raden zijn. | Security | Must |  |
| NFR2 | de gamepagina moet binnen 2 seconden laden.(delay mag door realtime sync) | Kwaliteit | Could have |  |
| NFR3 | De UI moet duidelijke foutmeldingen tonen bij een mislukte login of ongeldig spel. | UX | Should have |  |
| NFR4 | De game moet real-time updates ontvangen zodra de developer succesvol joined. | Functionaliteit | Must |  |
| NFR5 | Er mogen geen gevoelige gegevens in de URL worden opgeslagen. | Security | Must |  |
| NFR6 | Als er twee mensen met de zelfde naam zijn moeten ze in de UI verschillend zijn door kleur of icon. | UX | Would have |  |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Game- en verificatiegegevens (gamecode, sessie-ID) | Gegevens |  |
| AS2 | Inlog- en identificatiegegevens van de developer | Gegevens |  |
| AS3 | SignalR token/authorization voor toegang tot realtime game data | Security |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Ongeautoriseerde toegang tot een game door het raden of manipuleren van de gamecode | AS1 | V3.4 Session Management |
| RSK2 | evoelige gegevens worden blootgesteld in de URL (zoals tokens of gamecodes) | AS1 | V2.1 Data Protection |
| RSK3 | Onbevoegde toegang tot accounts door zwakke of gestolen verificatiecodes | AS2 | V4.1 Authentication |
| RSK4 | Onveilige SignalR tokens kunnen de toegang tot realtime gegevens ongeautoriseerd geven | AS3 | V4.1 Authentication |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 3 | 4 | 12 | Hoog |
| RSK2 | 2 | 4 | 8 | Midel |
| RSK3 | 2 | 5 | 10 | Midel |
| RSK4 | 3 | 5 | 15 | Hoog |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Gebruik secure random tokens voor gamecodes, zodat ze moeilijk te raden of te manipuleren zijn. | Niet geïmplementeerd |
| SM2 | RSK2 | Zorg ervoor dat gevoelige gegevens zoals gamecodes en tokens niet in de URL worden opgeslagen en altijd via beveiligde kanalen worden verzonden. | Niet geïmplementeerd |
| SM3 | RSK3 | Implementeer tweefactorauthenticatie voor toegang tot accounts en gebruik sterke wachtwoorden om ongeautoriseerde toegang te voorkomen. | Niet geïmplementeerd |
| SM4 | RSK4 | SignalR-tokens moeten veilig worden gegenereerd en opgeslagen en geverifieerd bij elke verbinding. Gebruik SSL/TLS voor encryptie van alle SignalR-verbindingen. | Niet geïmplementeerd |

## Use Case: Game spelen

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
| De Game leider kan een game starten en een backlog item selecteren. |
| Het geselecteerde backlog item wordt correct weergegeven met realtime communicatie. |
| Spelers en de leider kunnen storypoints toekennen. |
| De applicatie of de leider kan een ronde beëindigen. |
| Er moet foutafhandeling zijn bij synchronisatiefouten. |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
| De game moet realtime communicatie ondersteunen voor storypoint-input. |
| De game moet betrouwbaar zijn bij het toekennen van storypoints zonder vertraging. |
| De UI moet foutmeldingen tonen wanneer een synchronisatiefout optreedt. |
| De applicatie moet binnen 1 seconde reageren op een actie van de speler. |
| Er mogen geen gevoelige gegevens via de applicatie worden opgeslagen zonder encryptie. |

### Requirments overzicht

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Beschrijving | Asset/Type | MoSCoW | Testen |
| FR1 | De Game leider kan een game starten en een backlog item selecteren. | Functionaliteit | Must |  |
| FR2 | Het geselecteerde backlog item wordt correct weergegeven met realtime communicatie. | Functionaliteit | Must |  |
| FR3 | Spelers en de leider kunnen storypoints toekennen. | Functionaliteit | Must |  |
| FR4 | De applicatie of de leider kan een ronde beëindigen. | Functionaliteit | Must |  |
| FR5 | Er moet foutafhandeling zijn bij synchronisatiefouten. | Security | Should have |  |
| NFR1 | De game moet realtime communicatie ondersteunen voor storypoint-input. | Functionaliteit | Must |  |
| NFR2 | De game moet betrouwbaar zijn bij het toekennen van storypoints zonder vertraging. | Functionaliteit | Must |  |
| NFR3 | De UI moet foutmeldingen tonen wanneer een synchronisatiefout optreedt. | UX | Should have |  |
| NFR4 | De applicatie moet binnen 1 seconde reageren op een actie van de speler. | Kwaliteit | Should have |  |
| NFR5 | Er mogen geen gevoelige gegevens via de applicatie worden opgeslagen zonder encryptie. | Security | Must |  |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |
| AS1 | Game- en verificatiegegevens (game-ID, sessie-ID, backlog-item) | Gegevens |  |
| AS2 | Verificatie- en sessie-informatie van spelers en de game leider Gegevens | Gegevens |  |
| AS3 | Real-time communicatiegegevens via SignalR voor storypoint-input | Comunicatie |  |
| AS4 | Gevoelige gegevens (zoals speler-ID, persoonlijke voorkeuren) die via de applicatie kunnen worden opgeslagen | Gegevens |  |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |
| RSK1 | Ongeautoriseerde toegang tot game- en sessiegegevens door het raden of manipuleren van de game-ID | AS1 | V3.4 Session Management |
| RSK2 | Vertraging of mislukking van de reactie van de applicatie bij een speleractie, wat leidt tot een slechte gebruikerservaring | AS2 | V5.2 Resilience & Fault Tolerance |
| RSK3 | Foutieve synchronisatie van realtime gegevens, wat leidt tot inconsistente storypoint-toekenning tussen spelers | AS3 | V5.3 Input Validation and Data Integrity |
| RSK4 | Het toekennen van storypoints zonder betrouwbare real-time communicatie, wat kan leiden tot verkeerde gegevens | AS3 | V5.4 Real-Time Data Processing |
| RSK5 | Gevoelige gegevens kunnen onterecht blootgesteld worden of onversleuteld opgeslagen worden in de applicatie | AS4 | V2.1 Data Protection |
| RSK6 | Ongeautoriseerde toegang tot gevoelige gegevens tijdens de transmissie of opslag door onvoldoende encryptie | AS4 | V2.5 Cryptographic Key Management |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |
| RSK1 | 4 | 3 | 12 | Hoog |
| RSK2 | 3 | 1 | 3 | Laag |
| RSK3 | 3 | 3 | 9 | Medium |
| RSK4 | 3 | 4 | 12 | Hoog |
| RSK5 | 2 | 5 | 10 | Medium |
| RSK6 | 2 | 5 | 10 | Medium |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |
| SM1 | RSK1 | Implementeer sterke sessiebeveiliging en validatie van de gamecode, gebruik van veilige en niet-gemakkelijke te raden gamecodes | Niet geïmplementeerd |
| SM2 | RSK2 | Verbeter de performance door middel van asynchrone communicatie en foutafhandelingsmechanismen voor vertragingen bij reacties | Niet geïmplementeerd |
| SM3 | RSK3 | Gebruik SignalR met redundantie en betrouwbare foutafhandelingsprotocollen om data consistentie te waarborgen | Niet geïmplementeerd |
| SM4 | RSK4 | Zorg voor betrouwbare SignalR-communicatie en gebruik verbindingscontrolemechanismen voor accurate storypoint-toekenning | Niet geïmplementeerd |
| SM5 | RSK5 | Encryptie van gevoelige gegevens bij opslag en transmissie via veilige verbindingen zoals HTTPS | Niet geïmplementeerd |
| SM6 | RSK6 | Implementeer end-to-end encryptie en gebruik veilige cryptografische methoden voor opslag en transmissie van gevoelige gegevens | Niet geïmplementeerd |

## Use Case: Naam

### Functionele requirements

|  |
| --- |
| **Beschrijving:** |
|  |
|  |

### Niet-functionele requirements

|  |
| --- |
| Beschrijving |
|  |

### Requirments overzicht

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Bron | Beschrijving | Asset/Type | MoSCoW | Testen |

### Risk assessment

#### **Assets vaststellen**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset ID | Beschrijving | Type | Bron |

#### **Risico’s identificeren**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico ID | Beschrijving | Asset | Relevant ASVS Hoofdstuk |

#### **Risico’s schatting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risico ID | Kans(1-5) | Inpact(1-5) | Risicoscore | RisicoNiveau |

#### **Mitigerende maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Measure ID | Risico ID | Maatregel | Status |

# 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 1 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.*