hogeschool Windesheim
Dichter bij jou

dinsdag 26 maart 2024

Requirements Analyse Showcase

Versie 0.3

Martijn Schuman
Client & Server & Security
S1186586
ICTWDf
H. Bosman & R. Hulsing & J. Brouwers

Algemene informatie

Versiebeheer

Versie	Datum	Omschrijving
0.1	6-2-2024	Initiële opzet
0.2	2-3-2024	Requirements UC1-7 uitgewerkt
0.3	24-03-2024	Requirements bijwerken

Distributie

Ontvanger	Datum	Versie
H. Bosman & R. Hulsing & J. Brouwers	04-03-2024	0.2
H. Bosman & R. Hulsing & J. Brouwers	26-03-2024	0.3

Inhoudsopgave

1 Requirements 3
1.1 Globale requirements 3
1.2 US1 4
1.3 UC2 6
1.4 UC3 8
1.5 UC4 9
1.6 UC5 10
1.7 UC6 11
1.8 UC7 12

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 Bijlage 1 Aanpak Requirements Analyse.

1.1 Globale requirements

In de onderstaande tabel zijn globale requirements opgenomen. Deze niet functionele requirements zijn van toepassing op de gehele applicatie.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
NFR1		De gegevens op de pagina zijn niet wijzigbaar via de interface	Beperking	**Must**	Functioneel
NFR2		De pagina wordt binnen 1 seconde geladen	Kwaliteit	**Must**	Functioneel
NFR3		De gebruikte HTML-tags zijn semantisch waar dit mogelijk is	Beperking	**Must**	Functioneel
NFR4		De profiel pagina bevat een GDPR (ASVS V8.3 Sensitive Private Data)	Beperking	**Must**	Functioneel
NFR5		De GDPR-keuze wordt opgeslagen	Beperking	**Must**	Functioneel
NFR6		GDPR wordt alleen getoond als er geen consent is gegeven	Beperking	**Must**	Functioneel
NFR7		Styling GDPR past bij pagina	Kwaliteit	**Must**	Functioneel

1.2 US1

In de onderstaande tabel zijn requirements voor US1 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
US1	Brainstormsessie	Als uitdager en damspeler wil ik kunnen registreren, zodat ik mijn eigen damspellen kan aanmaken en tegen anderen kan spelen.	Functioneel	**Must**	Functioneel
FR1.1		De pagina moet een registratieformulier hebben.	Beperking	**Must**	
FR1.2		Het registratieformulier bevat invoervelden voor ‘gebruikersnaam, ‘email’, ‘wachtwoord’, ‘wachtwoord herhalen’, ‘’.	AS1.1	**Must**	
FR1.3		Het registratieformulier bevat een reCAPTCHA beveiliging	Beperking	**Must**	
NFR1.1		Registratiegegevens moeten versleuteld worden opgeslagen.	Kwaliteit	**Must**	
NFR1.2		De inputgegevens worden live gecontroleerd	Kwaliteit	**Must**	
NFR1.3		Als de gegevens correct zijn wordt de uitdager of damspeler automatisch ingelogd	Kwaliteit	**Must**	
NFR1.4		Als de gegevens niet correct zijn worden de invoervelden rood en wordt er foutmelding getoond.	Kwaliteit	**Should**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS1.1	Gebruikersnaam, email, wachtwoord		UC1		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK1.1	**ASVS 5.1.3** Lange invoer leidt tot systeem crash	Hoog		Groot	SM1.1
RSK1.2	**ASVS 5.1.4** Invoer is invalide doordat data niet strong typed is	Hoog		Groot	SM1.2
RSK1.3	**ASVS 5.1.5** Injectie van scripts in de invoer	Hoog		Groot	SM1.3
RSK1.4	Database lek	Gemiddeld		Groot	SM1.4
RSK1.5	Wachtwoorden worden gekraakt	Hoog		Groot	SM1.5
#	**Beschrijving**	**Test**		**Status**	
SM1.1	Gebruiker gegevens zijn gebonden aan een maximumlengte zowel clientside, als serverside	Functioneel		Voltooid	
SM1.2	Gebruiker gegevens zijn strong typed.	Functioneel		Voltooid	
SM1.3	Request data wordt server side sanitized. **ASVS V2.5.4** Controleer of er geen gedeelde of standaardaccounts aanwezig zijn	Functioneel		Voltooid	

SM1.4	**ASVS V2.4.1** Controleer of wachtwoorden worden opgeslagen in een vorm die bestand is tegen offline aanvallen. Wachtwoorden MOETEN worden gesalt en gehasht met behulp van een goedgekeurde eenrichtingssleutelafleiding of wachtwoord-hashing-functie **ASVS V2.5.4** Controleer of er geen gedeelde of standaardaccounts aanwezig zijn	Functioneel	Voltooid	
SM1.5	**ASVS V2.1.1**. Wachtwoorden moeten minimaal 12 karakters lang zijn, een hoofdletter, speciaal teken en een getal hebben. **ASVS V2.1.2**. Wachtwoorden mogen maximaal 128 karakters lang zijn **ASVS V2.1.4**. Controleer of elk afdrukbaar Unicode-teken, inclusief taalneutrale tekens zoals spaties en emoji's, in wachtwoorden is toegestaan. **ASVS V2.1.11** Controleer of de 'plak'-functionaliteit, browserwachtwoord helpers en externe wachtwoordbeheerders zijn toegestaan.	Functioneel	Voltooid Voltooid Voltooid Voltooid	

1.3 UC2

In de onderstaande tabel zijn requirements voor US2 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
UC2	Brainstormsessie	Als uitdager en damspeler wil ik kunnen inloggen zodat ik verder kan gaan met mijn actieve spellen.	Functioneel	**Must**	Functioneel
FR2.1		De pagina bevat een inlogformulier	Beperking	**Must**	
FR2.2		Het inlogformulier bevat invoervelden voor een ‘gebruikersnaam’ of ‘email’ en een wachtwoord.	AS2.1		
FR2.3		Het inlogformulier bevat een reCAPTCHA beveiliging	Beperking	**Must**	
FR2.4		Na het inloggen wordt de uitdager of damspeler doorgestuurd naar de pagina met gedetailleerde damspelresultaten.	Kwaliteit	**Must**	
NFR2.1		Bij foutieve inloggegevens worden de invoervelden rood en wordt er een foutmelding getoond.	Kwaliteit	**Must**	
NFR2.2		Het account is beschermd met een 2FA	AS2.2	**Must**	
NFR2.3		Als een gebruiker een derde keer het wachtwoord fout in typt wordt het account geblokkeerd.	Beperking	**Should**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS2.1	Gebruikersnaam, email, wachtwoord		UC2		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK2.1	ASVS 5.1.3 Lange invoer leidt tot systeem crash	Hoog		Groot	SM2.1
RSK2.2	ASVS 5.1.4 Invoer is invalide doordat data niet strong typed is	Hoog		Groot	SM2.2
RSK2.3	ASVS 5.1.5 Injectie van scripts in de invoer	Hoog		Groot	SM2.3
RSK2.4	Database lek	Gemiddeld		Groot	SM2.4
RSK2.5	Onvoldoende authenticatie en autorisatiecontroles	Gemiddeld		Groot	SM2.5
#	**Beschrijving**	**Test**		**Status**	
SM2.1	Gebruiker gegevens zijn gebonden aan een maximumlengte zowel clientside, als serverside	Functioneel Unit		Voltooid	
SM2.2	Gebruiker gegevens zijn strong typed.	Functioneel Unit		Voltooid	
SM2.3	Request data wordt server side sanitized.	Functioneel Unit		Voltooid	

SM2.4	Wachtwoord hashing	Functioneel Unit		Voltooid	
SM2.5	Sterke authenticatie- en autorisatiemechanismen, zoals 2fa en het principe van minste privilege worden gebruikt	Functioneel		Voltooid	
#	**Asset**	**Bron**	**Koppeling**	**Test/Security Measurement**	
AS2.2	2FA secret		UC2		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK2.1	**ASVS V2.8.4** Verify that time-based OTP can be used only once within the validity period.	Hoog		Hoog	SM2.1
RSK2.2	**ASVS V2.9.3** Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.	Gemiddeld		Hoog	SM2.2
RSK2.3	**ASVS V2.10.3** Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.	Gemiddeld		Hoog	SM2.3
RSK2.4	**ASVS V2.10.4** Verify passwords, integrations with databases and third-party systems, seeds and internal secrets, and API keys are managed securely and not included in the source code or stored within source code repositories.	Gemiddeld		Hoog	SM2.4
#	**Beschrijving**	**Test**		**Status**	
SM2.1	Geldigheidsduur waarborgen door aan te geven wat de marge van de test is	Functioneel		Voltooid	
SM2.2	80 bit secret gebruiken voor backwards compatibility	Functioneel Unit		Voltooid	
SM2.3	Database en systeem wachtwoorden gebruiken	Functioneel		Voltooid	
SM2.4	ENV opnemen in .gitignore	Functioneel		Voltooid	

1.4 UC3

In de onderstaande tabel zijn requirements voor US3 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
UC3	Brainstormsessie	Als uitdager en damspeler wil ik een gedetailleerde geschiedenis van al mijn damspelresultaten kunnen zien, inclusief winst, verlies en gelijkspel, zodat ik mijn prestaties in de loop van de tijd kan volgen.	Functioneel	**Should**	Functioneel
FR3.1		De pagina bevat een overzicht van de 20 meest recente damspellen.	Beperking	**Should**	
FR3.2		De damspellen zijn gesorteerd op meest recente bovenaan	Kwaliteit	**Should**	
FR3.3		Per damspel is te zijn hoelang het spel duurde, tegen wie hij was, wie er heeft gewonnen	AS3.1	**Should**	
FR3.4		Boven in de pagina is te zien hoe vaak de uitdager of damspeler heeft gewonnen, verloren en gelijkgespeeld	Kwaliteit	**Should**	
NFR3.1		Als er nog een damspel actief is staat dit spel bovenaan de lijst.	Beperking	**Should**	
NFR3.2		Als er nog een damspel actief is, wordt dit duidelijk aangegeven met een opmerking	Beperking	**Should**	
NFR3.3		Actieve spellen hebben een oranje achtergrond, gewonnen een groene, gelijk geel en verloren rood.	Kwaliteit	**Should**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS3.1	Damspel gegevens		UC3		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK3.1	Ongeautoriseerde toegang tot damspelgegevens	Gemiddeld		Gemiddeld	SM3.1
RSK3.2	Onjuiste weergave van damspelresultaten	Gemiddeld		Gemiddeld	SM3.2
#	**Beschrijving**	**Test**		**Status**	
SM3.1	Implementeren van authenticatie en autorisatie			Voltooid	
SM3.2	Grondig testen om te controleren of de resultaten kloppen				

1.5 UC4

In de onderstaande tabel zijn requirements voor US4 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
US4	Brainstormsessie	Als uitdager wil ik damspel kunnen aanmaken zodat ik een damspeler kan uitdagen.	Functioneel	**Must**	Functioneel
FR4.1		Na het klikken op de knop “Spel aanmaken” wordt de uitnodigingscode getoond.	AS4.1	**Must**	
FR4.2		Zolang er nog een uitnodiging open staat kan er geen nieuw spel worden aangemaakt.	Beperking	**Must**	
FR4.3		De uitnodiging is gedurende 30 minuten openen, waarna de uitdager een nieuwe uitnodiging zou moeten maken.	Beperking	**Should**	
NFR4.1		De uitnodigingscode wordt duidelijk getoond door middel van een melding.	Kwaliteit	**Must**	
NFR4.2		De uitnodigingscode is niet handmatig aan te passen.	Beperking	**Must**	
NFR4.3		De uitnodigingscode bestaat enkel uit een getal van minimaal acht cijfers.	Beperking	**Must**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS4.1	Damspel		UC4		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK4.1	Damspel maken onder de naam van iemand anders	Gemiddeld		Hoog	SM4.1
RSK4.2	Meerdere damspellen maken	Gemiddeld		Hoog	SM4.2
RSK4.3	Uitnodigingscode wordt onbedoeld gedeeld	Gemiddeld		Gemiddeld	SN4.3
#	**Beschrijving**	**Test**		**Status**	
SM4.1	Er is 2FA geïmplementeerd, JWST-token worden bij elke request gevalideerd.	Functioneel		Voltooid	
SM4.2	De client en de server controleren of er een spel actief is.	Functioneel		Voltooid	
SM4.3	Implementatie van duidelijke waarschuwingsmeldingen om te voorkomen dat de uitnodigingscode onbedoeld wordt gedeeld.				

1.6 UC5

In de onderstaande tabel zijn requirements voor US5 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
US5	Brainstormsessie	Als damspeler wil me bij een damspel kunnen aansluiten zodat ik tegen de uitdager kan spelen.	Functioneel	**Must**	Functioneel
FR5.1		Boven in de pagina is een invoerveld aanwezig waarbij de damspeler een uitnodigingscode kan invoeren.	Beperking	**Must**	
FR5.2		Als de code geldig is wordt er een knop getoond waarmee de damspeler naar het spel kan gaan.	Beperking	**Must**	
FR5.3		Als de code niet geldig is wordt er een foutmelding getoond.	Kwaliteit	**Should**	
NFR5.1		Het invoerveld is altijd zichtbaar	Beperking	**Must**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
	Damspel		UC5		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK5.1	Een derde persoon neemt deel aan een damspel	Gemiddeld		Hoog	SM5.1
RSK5.2	ASVS 5.1.3 Lange invoer leidt tot systeem crash	Hoog		Groot	SM5.2
RSK5.3	ASVS 5.1.4 Invoer is invalide doordat data niet strong typed is	Hoog		Groot	SM5.3
RSK5.4	ASVS 5.1.5 Injectie van scripts in de invoer	Hoog		Groot	SM5.4
#	**Beschrijving**	**Test**		**Status**	
SM5.1	Limiet op het aantal deelnemers instellen Uitnodigingscode inactief maken zodra hij is gebruikt.	Functioneel		Niet aan begonnen	
SM5.2	Gebruiker gegevens zijn gebonden aan een maximumlengte zowel clientside, als serverside	Functioneel		Niet aan begonnen	
SM5.3	Gebruiker gegevens zijn strong typed.	Functioneel		Niet aan begonnen	
SM5.4	Request data wordt server side sanitized.	Functioneel		Niet aan begonnen	

1.7 UC6

In de onderstaande tabel zijn requirements voor US6 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
US6	Brainstormsessie	Als uitdager wil ik tegen de damspeler een damspel kunnen spelen zodat ik kan weten wie er beter is.	Functioneel	**Must**	Functioneel
FR6.1		Op de pagina is een virtueel dambord aanwezig.	Kwaliteit	**Must**	
FR6.2		Bij het begin van het spel zijn alle damstenen al op het dambord aanwezig.	Kwaliteit	**Must**	
FR6.3		Op de pagina is te zien wie de tegenstander is, hoeveel damstenen iedereen nog heeft, wanneer het damspel is begonnen en hoeveel stenen iedereen nog over heeft.	AS6.1	**Must**	
FR6.4		Zodra er geslagen moet worden is er geen andere damsteen te selecteren dan het damsteen dat moet slaan.	Beperking	**Must**	
NFR6.1		De damstenen zijn duidelijk uit elkaar te houden.	Beperking	**Must**	
NFR6.2		De dam is duidelijk te onderscheiden van de andere damstukken.	Beperking	**Must**	
NFR6.3		Het damspel kan later worden afgemaakt.	Kwaliteit	**Must**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS6.1	Damspelgegevens		UC6		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK6.1	Meer dan twee spelers	Gemiddeld		Hoog	SM6.1
RSK6.2	Onbevoegde toegang tot het damspel	Gemiddeld		Hoog	SM6.2
#	**Beschrijving**	**Test**		**Status**	
SM6.1	Limiet op aantal deelnemers instellen. Uitnodigingscode inactief maken zodra hij is gebruikt. Controleren of de gebruiker wel op de pagina mag komen	Functioneel		Voltooid	
SM6.2	Implementatie van strikte autorisatiemechanismen om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot het damspel	Functioneel		Voltooid	

1.8 UC7

In de onderstaande tabel zijn requirements voor US7 opgenomen. De tabel is opgesplitst in functionele en niet functionele requirement. Per requirement is opgenomen wat het type is, hoe belangrijk hij is en hoe hij getest gaat worden.

#	Bron	Beschrijving	Asset/Type	MoSCoW	Testen
UC7	Brainstormsessie	Als beheerder wil ik een damspel kunnen annuleren als er gedurende 7 dagen geen activiteit heeft plaatsgevonden, zodat inactieve damspellen worden gesloten.	Functioneel	**Should**	Functioneel
FR7.1		Als er een spel al 7 dagen geen activiteit meer heeft gehad staat dit spel boven in de beheerderspagina.	Beperking	**Should**	
FR7.2		Om het spel te annuleren moet de beheerder op een speciale knop klikken.	Beperking	**Must**	
FR7.3		Voordat een spel geannuleerd kan worden wordt er om bevestiging gevraagd.	Beperking	**Must**	
FR7.4		Het annuleren van een damspel is permanent.	Kwaliteit	**Must**	
NFR7.1		De beheerderspagina bevat een overzicht met alle gespeelde spellen.	Beperking	**Should**	
NFR7.2		De annuleren knop is alleen zichtbaar bij spellen die inactief zijn.	Beperking	**Must**	

Risk assessment

#	Asset	Bron	Koppeling	Test/Security Measurement	
AS	Damspel gegevens		UC7		
#	**Beschrijving**	**Kans**		**Impact**	**Risk**
RSK7.1	Annuleren van een damspel namens de beheerder	Gemiddeld		Gemiddeld	SM7.1
RSK7.2	Onbedoelde annulering van een damspel	Gemiddeld		Gemiddeld	SM7.2
#	**Beschrijving**	**Test**		**Status**	
SM7.1	2FA Gebruikersrechten controleren op client Gebruikersrechten controleren op server	Functioneel		Voltooid	
SM7.2	Het systeem vraagt eerst om bevestiging	Functioneel		Voltooid	