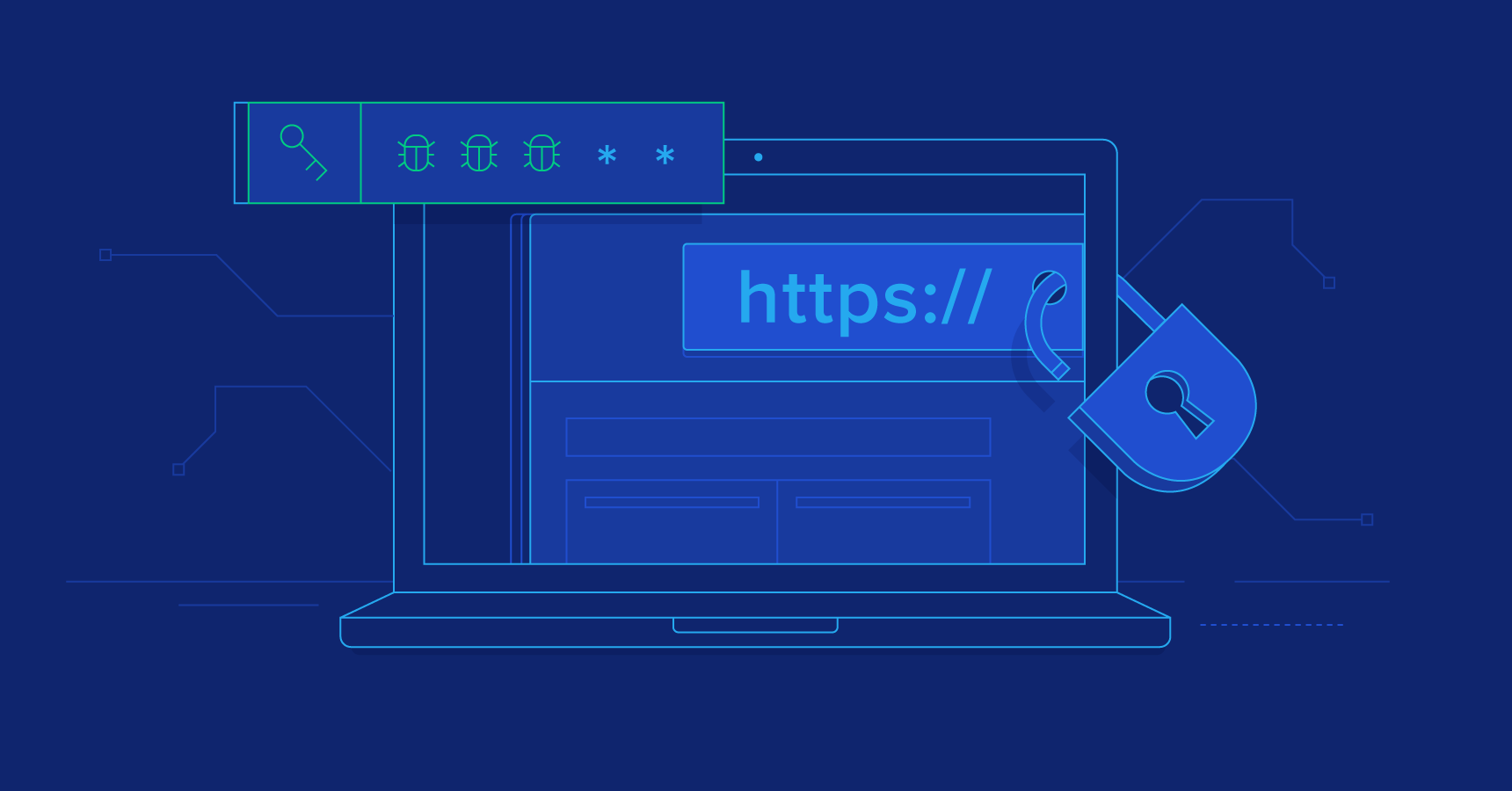
Preventie ontwerp

Cryptografie



Anthony Delgado, Ayoub Lfatmi, Per Taffijn en Mustafa Warsame

Datum:

*13 November 2023*

Deskundige docenten(en):

*H. Middelkoop en P. van den Bosch*

PDP-coach(es):

*M. Dijkstra*

# Inhoudsopgave

[**Toegangsbeheersing Plan**](#_gfcgl7gmbw1j) **2** Welke rollen zijn er? 2  
 Welke rechten zijn er per rol? 2  
 Procedures voor rolwijzigingen en uitschrijving 3

[**Aanvullende veiligheidseisen**](#_6xjfdps3l0a7) **4**

[**Logische testplannen**](#_pz4fycedwaob) **5** Testbasis 5  
 Testgevallen 6  
  
**Literatuurlijst****20**

# Toegangsbeheersing Plan

Welke rollen zijn er?

**Ervaringsdeskundige / Gebruiker:** De eindgebruikers van onze applicatie

**Bedrijven:** Bedrijven die gebruik maken van onze applicatie, deze kunnen ervaringsdeskundige benaderen.

**Beheerders (Stichting Accessibility):** De stichting is als beheerder verantwoordelijk voor bepaalde processen in de applicatie.

**Developers (Wij):** Wij als developers zullen bepaalde rechten in de applicatie krijgen. Zodat we onderhoud kunnen uitvoeren en eventuele fouten die optreden recht kunnen zetten.

Welke rechten zijn er per rol?

**Ervaringsdeskundige/Gebruiker:**

De ervaringsdeskundigen kunnen zichzelf registreren, en later opnieuw inloggen. Verder kunnen ze hun profiel invullen en vrij bewerken zonder toestemming van een beheerder. Ze kunnen beschikbare onderzoeken bekijken en zich hiervoor inschrijven. Tot slot kunnen ze met bedrijven en de Stichting communiceren via een chat-interface. De chats worden ook end-to-end versleuteld. Dus is het niet mogelijk voor de stichting om de chats van de gebruiker met een bedrijf te bekijken. Vice versa is dit ook niet mogelijk. Ook kunnen ze een uitschrijfverzoek voor een onderzoek indienen bij de beheerder.

**Bedrijven:**

Bedrijven kunnen zichzelf ook registreren en een account aanmaken om in te loggen. Verder is het mogelijk voor bedrijven om onderzoeken te plaatsen en beheren(bewerken, verwijderen) via hun eigen panel. Het is mogelijk voor bedrijven om te chatten met deelnemers van hun onderzoek. Uiteraard zijn deze chats end-to-end versleuteld. Indien aangevraagd bij de beheerder kunnen ze toegang krijgen tot de resultaten van het onderzoek.

**Admins binnen de Stichting Accessibility:**

De admin van de applicatie is verantwoordelijk voor het beheren van de toegang. Ook kunnen deze onderzoeken en bedrijven beheren(toevoegen, bewerken, verwijderen). Deze hebben toegang tot de profielen van de ervaringsdeskundige om te kijken of deze correct zijn m.u.v. bijzondere persoonsgegevens, deze zullen zij niet zien. Behalve op aanvraag en met toestemming van de ervaringsdeskundige.

**Overige werknemers van de Stichting Accessibility:**

De overige werknemers zullen vooral read-only rechten hebben, ze kunnen op de site een account aanmaken en chatten met bedrijven en ervaringsdeskundigen. Ook kunnen ze indien ze problemen zien dit aankaarten bij de admin die dit dan zelf kan oplossen of doorgeven aan ons.

**Developers(Wij):**

De developers hebben meer een terughoudende rol met betrekking tot de website. Als de beheerders problemen of bugs tegenkomen, of een probleem met het onderhoud hebben komen de developers van pas. De developers zullen zelf niks te maken hebben met het interne gebruik van de website.

Procedures voor rolwijzigingen en uitschrijving

**Wat is de procedure als personen van rol veranderen?**

Indien iemand op de website van rol wilt veranderen, zullen zij een verzoek moeten indienen bij de beheerder. Beheerders evalueren dit verzoek en passen de rollen en rechten aan op basis van gewijzigde behoeften.

**Wat is de procedure als rollen wijzigen?**

Indien een bepaalde rol op de website een andere vorm krijgt of volledig gewijzigd wordt, wordt er door de beheerders eerst gekeken of de toegewezen personen nog de juiste kandidaten zijn om die bepaalde rol te vervullen. Indien dit niet het geval is, worden er door de beheerders nieuwe personen aangewezen die wel beter geschikt zijn om die rol te vervullen, en wordt het toegangsbeheersysteem daarop aangepast. Uiteraard worden de oorspronkelijke kandidaten van die bepaalde rol overgeplaatst naar een beter geschikte rol

**Wat is de procedure als panelleden niet meer ingeschreven willen staan?**

Indien een ervaringsdeskundige zichzelf wil uitschrijven, kunnen zij via de profielsectie een uitschrijvingsverzoek indienen. Deze wordt geverifieerd door de beheerder en deze verwijdert ook de persoonsgegevens uit de database. De ervaringsdeskundige krijgt hierna een bevestiging dat deze is uitgeschreven. Testdata blijft behouden voor analytische doeleinden zonder identificeerbare persoonsgegevens.

# 

# 

# Aanvullende veiligheidseisen

In de aangeleverde casus van Stichting Accessibility zijn er geen veiligheidseisen opgenomen. Daarom hebben wij de volgende lijst van veiligheidsmaatregelen voor de applicatie opgesteld.

1. **Sterke authenticatie en autorisatie** : Door middel van session management, wachtwoord policies en andere maatregelen zullen wij ervoor zorgen dat alleen echte gebruikers toegang hebben tot de applicatie. Veel van deze autorisatie en authenticatie structuren worden al kant-en-klaar aangeboden door diverse (moderne) frameworks, wat voor ons natuurlijk erg fijn is.
2. **Input validation** : Door middel van input formats en validatie zullen wij voorkomen dat er kwaadaardige data wordt geüpload naar de applicatie. Hiermee voorkomen we aanvallen zoals Cross Site Scripting en SQL injecties.
3. **Secure File Uploads** : Door restricties te plaatsen op het soort bestanden dat geüpload kunnen worden en deze bestanden te checken voorkomen wij dat kwaadaardige scripts uitgevoerd kunnen worden.
4. **Versleutelde communicatie** : Door gebruik te maken van HTTPS zullen wij de communicatie tussen de gebruiker en de applicatie versleutelen om man-in-the-middle aanvallen en data-afluistering te voorkomen.
5. **Logging** : Door middel van logging zullen wij verdachte situaties identificeren en bestrijden.
6. **Access Control** : Door middel van Role-Based Access Control (RBAC) zullen wij ervoor zorgen dat alleen de gebruikers met de juiste autorisatie de bijbehorende privileges hebben, en gaan wij ongeoorloofde toegang tot data tegen.
7. **Firewall** : Door gebruik te maken van een Firewall zullen wij internetverkeer weren waarvan bekend is of verdacht wordt dat het misbruik maakt van web kwetsbaarheden.
8. **Proper Error Handling** : Wij zullen bij het voorkomen van een fout een zelf opgesteld foutmelding bericht laten zien dat geen gevoelige informatie blootstelt.
9. **Patch Management**: Wij zullen regelmatig patches en updates uitvoeren voor besturingssystemen, applicaties en firmware om bekende kwetsbaarheden te verhelpen.
10. **Penetratietesten**: Het uitvoeren van periodieke penetratietesten om te zien of en hoe kwaadwillende aanvallers toegang kunnen krijgen tot systemen of gegevens. Dit omvat externe en interne tests.
11. **Security Headers**: Het implementeren van beveiligingsheaders in de HTTP-responsen van de applicatie, zoals Content Security Policy (CSP), Strict-Transport-Security (HSTS), en X-Content-Type-Options, om bepaalde soorten aanvallen te voorkomen.
12. **Rate Limiting**: We kunnen overwegen om rate limiting, op inlogpogingen en andere kritieke acties, in te stellen om brute force-aanvallen te voorkomen.

Met de hierboven opgestelde methodes willen wij preventieve maatregelen nemen om de veiligheid van de applicatie te waarborgen.

# Logische test plannen

Het doel van de syntax-testen is om te controleren of de beperkingen die gesteld worden aan de invoer (en uitvoer) van de applicatie goed zijn geïmplementeerd. Dit heeft voornamelijk te maken met verifiëren van attribuut restricties, geldige en ongeldige (input) waarden, en de juiste weergave van foutmeldingen. De testbasis wordt gevormd door de systeemeisen, procesbeschrijving, en wetgeving die relevant zijn voor de webapplicatie, wat in dit geval dus is voor de Stichting Accessibility.

Test Basis

De testbasis bevat de volgende punten:

* **Systeemeisen:** Deze omvatten de specificaties voor de ervaringsdeskundigen portal, beheerderportal, bedrijfsportal en de online onderzoeksomgeving. Het bevat ook de eisen met betrekking tot profielpagina's, onderzoeken, bedrijfsprofielen en beheerdersfuncties.
* **Procesbeschrijvingen:** De processen binnen de applicatie, zoals het registreren van gebruikers, plaatsen van opdrachten, beheer van profielen en dergelijke, zijn gedetailleerd beschreven.
* **Wetgeving:** De Stichting Accessibility stelt specifieke eisen aan toegankelijkheid (WCAG 2.2 - AA). Daarnaast zijn er wetten en richtlijnen met betrekking tot privacy die moeten worden nageleefd, denk hierbij aan de Algemene Verordening Gegevensbescherming (AVG)

Testgevallen

| **Titel:**  Registratie van een ervaringsdeskundige | **Initiële situatie (uitgangssituatie)**   * Het systeem is operationeel. * De gebruiker bevindt zich op de registratiepagina. * Er zijn geen gegevens van de gebruiker aanwezig in de database |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Voer geldige gegevens in op de registratiepagina, inclusief vereiste velden (voornaam, achternaam, e-mailadres, etc.). * Probeer de registratie te voltooien zonder een verplicht veld in te vullen. * Probeer de registratie te voltooien met een ongeldig e-mailadres. * Probeer de registratie te voltooien met een bestaand e-mailadres in de database. * Voer geldige gegevens in en geef aan dat commerciële partijen de gebruiker mogen benaderen |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Na correcte invoer wordt de gebruiker geregistreerd en doorgestuurd naar de profielpagina. Gegevens worden correct opgeslagen in de database. * Er moet een foutmelding verschijnen en de registratie mag niet doorgaan. * Er moet een foutmelding verschijnen over het ongeldige e-mailadres. * Er moet een foutmelding verschijnen dat het e-mailadres al in gebruik is. * Na registratie moet de voorkeur voor benadering door commerciële partijen correct worden weergegeven op het profiel. |

| **Titel:**  Bedrijf plaatst een nieuwe onderzoeksopdracht. | **Initiële situatie (uitgangssituatie)**   * Het bedrijf is ingelogd op het bedrijvenportal * Er zijn geen lopende opdrachten geplaatst door het bedrijf |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Voer alle vereiste informatie in voor het plaatsen van een nieuw onderzoek. * Plaats de opdracht zonder selectiecriteria. * Plaats de opdracht met ongeldige criteria (bijv. een ongeldige plaatsnaam of postcode formaat) * Plaats de opdracht met selectiecriteria die geen match hebben met de beschikbare ervaringsdeskundigen. * Probeer een opdracht te plaatsen zonder ingelogd te zijn als bedrijf. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Na correcte invoer wordt de opdracht geplaatst en verschijnt deze in het bedrijfsdashboard. De opdracht is nu zichtbaar voor alle gebruikers van de applicatie. * Zonder selectiecriteria moet het systeem een waarschuwing geven dat criteria nodig zijn. * Bij ongeldige criteria moet het systeem een foutmelding weergeven en de opdracht niet plaatsen. * Als de criteria geen match hebben, moet het systeem dit aangeven en de opdracht niet plaatsen. * Zonder in te loggen moet het systeem het bedrijfsportal beveiligen en toegang weigeren. |

| **Titel:**  Een ervaringsdeskundige wil meedoen aan een onderzoek. | **Initiële situatie (uitgangssituatie)**   * Het systeem is operationeel. * Een geregistreerde ervaringsdeskundige is ingelogd. * Er zijn beschikbare onderzoeken op de website. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Log in als geregistreerde ervaringsdeskundige * Ga naar de pagina met beschikbare onderzoeken * Selecteer een onderzoek waar je als gebruiker aan wilt deelnemen * Meld je aan voor het geselecteerde onderzoek door op de aanmeld knop te klikken. * Controleer of de aanmeldingsstatus voor het specifieke onderzoek correct wordt weergegeven op de profielpagina. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * De ervaringsdeskundige kan succesvol inloggen. * Een overzicht van beschikbare onderzoeken wordt getoond. * Het geselecteerde onderzoek wordt correct geopend met de bijbehorende details. * Aanmelding voor het onderzoek leidt tot een bijgewerkte aanmeldingsstatus op de profielpagina. De ervaringsdeskundige is nu betrokken bij het onderzoek. |

| **Titel:**  Een ervaringsdeskundige probeert functies uit te voeren die zijn voorbehouden aan beheerders. | **Initiële situatie (uitgangssituatie)**   * Het systeem is operationeel. * Er is een gebruiker ingelogd als geregistreerde ervaringsdeskundige * Er zijn beheerdersfuncties in het systeem waar een ervaringsdeskundige normaal geen toegang toe heeft. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Log in als een geregistreerde ervaringsdeskundige. * Probeer toegang te krijgen tot beheerdersfuncties zoals het bewerken van een nieuw onderzoek. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * De ervaringsdeskundige kan succesvol inloggen. * Er moet een foutmelding verschijnen, en de toegang tot de beheerdersfunctie moet worden geweigerd. |

| **Titel:**  Ervaringsdeskundige wijzigt persoonlijke gegevens. | **Initiële situatie (uitgangssituatie)**   * De ervaringsdeskundige is ingelogd op de portal. * Het profiel bevat bestaande gegevens die bekend zijn in de database. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Ga naar het profiel en wijzig enkele persoonlijke gegevens, zoals het telefoonnummer. * Probeer persoonlijke gegevens te wijzigen zonder alle verplichte velden in te vullen. Laat bijvoorbeeld het invoerveld voor voor- en achternaam leeg. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Na het wijzigen van gegevens moet het profiel bijgewerkt zijn met de nieuwe informatie. Dit wordt daarnaast ook bijgewerkt door de backend en opgeslagen in de database. * Het systeem moet een foutmelding geven als niet alle verplichte velden zijn ingevuld. |

| **Titel:**  Ervaringsdeskundige zoekt naar onderzoeken op basis van specifieke criteria. | **Initiële situatie (uitgangssituatie)**   * De ervaringsdeskundige is ingelogd op het portal. * Er zijn meerdere lopende onderzoeken beschikbaar. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Zoek naar onderzoeken met specifieke criteria zoals type onderzoek, locatie, beloning of soort beperking dat nodig is voor het testen van de applicatie.   + Geef specifieke zoekcriteria op, zoals 'Interview', 'Online', of een specifieke locatie.   + Bekijk de resultaten van de zoekopdracht. * Probeer te zoeken zonder geldige zoektermen in te voeren.   + Laat alle zoekvelden bijvoorbeeld leeg, en probeer daarna te zoeken. * Zoek naar onderzoeken die niet bekend zijn binnen het systeem. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Voor de geslaagde zoekopdracht   + Het systeem moet onderzoeken tonen die voldoen aan de opgegeven criteria.   + De ervaringsdeskundige moet de zoekresultaten kunnen bekijken. * Voor de mislukte zoekpogingen:   + Het systeem moet aangeven dat er geen resultaten gevonden zijn bij het zoeken zonder geldige of onbekende zoektermen. |

| **Titel:**  Een gebruiker vraagt om de verwijdering van persoonlijke gegevens conform de AVG. | **Initiële situatie (uitgangssituatie)**   * Een geregistreerde gebruiker, in dit geval een ervaringsdeskundige, heeft persoonlijke gegevens in de database staan. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Log in als de gebruiker die om verwijdering van persoonlijke gegevens vraagt. * Ga naar de profielpagina. * Zoek en selecteer de optie om een AVG-verzoek in te dienen voor verwijdering van persoonlijke gegevens. * Vul het AVG-verzoekformulier in met de benodigde gegevens en verifieer de identiteit van de gebruiker. * Beheerders verifiëren het AVG-verzoek en beoordelen of het voldoet aan de criteria. * Als het AVG-verzoek geldig is, worden persoonlijke gegevens permanent verwijderd uit het systeem. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Succesvolle inlog en weergave van de gebruikersinterface. * De profielpagina van de gebruiker wordt correct weergegeven. * Een formulier of proces wordt geactiveerd voor het indienen van het AVG-verzoek. * Het formulier wordt correct ingevuld en ingediend. * Beheerders verifiëren het verzoek. * Persoonlijke gegevens van de gebruiker worden volledig en permanent verwijderd. |

| **Titel:**  Ervaringsdeskundigen jonger dan 18 jaar meldden zich aan. | **Initiële situatie (uitgangssituatie)**   * De ervaringsdeskundige is jonger dan 18 jaar. * De ervaringsdeskundige meldt zich aan op het portal. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Vul de registratiegegevens in als een ervaringsdeskundige jonger dan 18 jaar.   + Geef een geboortedatum op die aangeeft dat de ervaringsdeskundige jonger is dan 18 jaar.   + Doorloop het registratieproces.. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Het systeem moet aangeven dat de betreffende persoon te jong is om zich te kunnen registreren binnen het systeem. * Beheerders worden op de hoogte gesteld van de mislukte registratie. Dit kan met bijvoorbeeld een audit-log. |

| **Titel:**  Plaatsen van tracking script bij de bedrijven. | **Initiële situatie (uitgangssituatie)**   * Het systeem is operationeel. * Een technisch medewerker van een bedrijf is ingelogd op het bedrijvenportal. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Log in als de technisch medewerker van een bedrijf. * Ga naar het gedeelte waar informatie staat over het plaatsen van een tracking script op de bedrijfswebsite. * Voeg het tracking script toe aan de bedrijfswebsite zoals aangegeven in de instructies. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Succesvolle inlog en weergave van het bedrijvenportal. * Er wordt informatie over het tracking script en de stappen voor implementatie getoond in de sectie over het plaatsen van een tracking script. * Het tracking script is na het volgen van de instructies correct geïmplementeerd en actief op de bedrijfswebsite. |

| **Titel:**  Nieuwe ervaringsdeskundige registreert zich en wordt goedgekeurd door een beheerder. | **Initiële situatie (uitgangssituatie)**   * De nieuwe ervaringsdeskundige heeft nog geen account op de portal. * Er is een beheerder ingelogd op het beheerders portal. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * De nieuwe ervaringsdeskundige meldt zich aan en vult alle vereiste registratiegegevens in.   + Vul alle verplichte velden correct in tijdens het registratieproces.   + Dien de registratie in. * De beheerder bekijkt de nieuwe registratie in het beheerders portal en keurt deze goed.   + Ga naar de lijst met nieuwe registraties.   + Bekijk de gegevens van de nieuwe ervaringsdeskundige.   + Keur de registratie goed. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Voor de geslaagde registratie:   + De nieuwe ervaringsdeskundige moet een bevestigingsmail ontvangen.   + Het systeem moet de registratiegegevens tonen in het beheerders portal.   + Gegevens worden succesvol opgeslagen in de database. * Voor de geslaagde goedkeuring:   + De nieuwe ervaringsdeskundige moet een melding ontvangen dat de registratie is goedgekeurd.   + Het systeem moet de de nieuwe ervaringsdeskundige toevoegen aan de lijst met gebruikers.      * Voor de mislukte registratie:   + Als de nieuwe ervaringsdeskundige essentiële informatie mist, moet het systeem aangeven welke informatie ontbreekt.   + Als de registratie wordt afgekeurd, moet de persoon een melding ontvangen met de reden van afkeuring. |

| **Titel:**  Berichten versturen door ervaringsdeskundigen. | **Initiële situatie (uitgangssituatie)**   * De ervaringsdeskundige is ingelogd op de portal. * Er is een lopend onderzoek waarvoor de ervaringsdeskundige zich heeft aangemeld. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Stuur een bericht naar een bedrijf met een vraag over het lopende onderzoek.   + Vul het bericht formulier in met een duidelijke vraag.   + Verzend het bericht. * Stuur een bericht naar Stichting Accessibility met een suggestie voor verbetering van de webapplicatie.   + Vul het bericht formulier in met een verbetersuggestie.   + Verzend het bericht. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Voor het bericht naar het bedrijf:   + Het bedrijf moet het bericht ontvangen.   + Het bedrijf moet kunnen reageren op het bericht.   + De ervaringsdeskundige moet een melding ontvangen van de reactie van het bedrijf. * Voor het bericht naar Stichting Accessibility:   + Stichting Accessibility moet het bericht ontvangen.   + Stichting Accessibility kan actie ondernemen op basis van de suggestie.   + De ervaringsdeskundige moet een melding ontvangen van de reactie van Stichting Accessibility. |

| **Titel:**  Toegankelijkheid voor Gebruikers met Gehoorverlies | **Initiële situatie (uitgangssituatie)**   * De ervaringsdeskundige heeft gehoorverlies. * Het systeem is operationeel. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * De ervaringsdeskundige gebruikt visuele signalen (m.b.v. externe software) om door de portal te navigeren.   + Controleer of visuele aanwijzingen en signalen duidelijk zijn.   + Navigeer door de portal zonder afhankelijk te zijn van auditieve feedback.   + Bekijk of de gebruiker eenvoudig en zonder problemen kan navigeren door de applicatie, door enkel zijn ‘arrow-keys’ te gebruiken * Probeer belangrijke meldingen te identificeren zonder geluid.   + Controleer of belangrijke meldingen visueel worden weergegeven.   + Ontvang en identificeer een melding zonder het geluid in te schakelen. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Visuele signalen moeten duidelijk zijn en de navigatie vergemakkelijken voor gebruikers met gehoorverlies. * Belangrijke meldingen moeten zichtbaar en begrijpelijk zijn zonder afhankelijk te zijn van geluid. * De gebruiker moet eenvoudig door de applicatie kunnen navigeren, waarbij goed gebruik is gemaakt van de juiste headers en tekst attributen. |

| **Titel:**  Algemene Toegankelijkheidstest | **Initiële situatie (uitgangssituatie)**   * De webapplicatie is operationeel. * Diverse gebruikersprofielen worden gesimuleerd, waaronder visuele, motorische, verstandelijke beperkingen, en gehoorverlies. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Navigeer door de portal met alleen het toetsenbord:   + Probeer alle interactieve elementen te bedienen met het toetsenbord. * Activeer de spraakbesturing opties en navigeer door de portal:   + Geef spraakopdrachten om door de portal te navigeren en interactie te hebben met de functies. * Stel verschillende kleurinstellingen in en controleer de zichtbaarheid:   + Pas de kleurinstellingen aan en controleer of de interface nog steeds begrijpelijk is. * Simuleer het gebruik van een schermlezer:   + Gebruik een schermlezer om door de portal te navigeren en controleer of alle relevante informatie wordt voorgelezen. * Vul een formulier in met spraak-naar-tekst invoermethode:   + Gebruik spraak-naar-tekst om gegevens in een formulier in te voeren en controleer of de ingevoerde gegevens correct worden verwerkt. * Controleer de visuele signalen en meldingen zonder gebruik te maken van geluid:   + Identificeer belangrijke meldingen en visuele signalen zonder afhankelijk te zijn van auditieve feedback. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Navigeer door de portal met alleen het toetsenbord:   + Alle interactieve elementen moeten toegankelijk zijn via het toetsenbord. * Activeer de spraakbesturing opties en navigeer door de portal:   + Spraakbesturing moet correct worden geïntegreerd voor navigatie en interactie met de functies. * Stel verschillende kleurinstellingen in en controleer de zichtbaarheid:   + Het systeem moet de kleurinstellingen correct toepassen, zodat de interface begrijpelijk blijft. * Simuleer het gebruik van een schermlezer:   + De schermlezer moet de relevante informatie correct voorlezen. * Vul een formulier in met spraak-naar-tekst invoermethode:   + Spraak-naar-tekst invoermethode moet goed geïntegreerd zijn, en het systeem moet de ingevoerde gegevens nauwkeurig verwerken. * Controleer de visuele signalen en meldingen zonder gebruik te maken van geluid:   + Belangrijke meldingen moeten zichtbaar en begrijpelijk zijn zonder afhankelijk te zijn van geluid. |

| **Titel:**  Veilige Gegevensuitwisseling | **Initiële situatie (uitgangssituatie)**   * De webapplicatie is operationeel. * Ervaringsdeskundigen voeren gevoelige informatie in via de portal. |
| --- | --- |
|  | **Acties (uit te voeren handelingen)**   * Voer gevoelige informatie in via de portal:   + Vul alle gegevens in op de profielpagina van de ervaringsdeskundige, inclusief persoonlijke en medische informatie. * Toegang tot de database:   + Simuleer de toegang tot de database en controleer of de opgeslagen gegevens versleuteld en veilig zijn. * Verifieer de veilige overdracht van gegevens naar de database:   + Controleer of de ingevoerde gegevens veilig worden overgedragen naar de database.   + Zorg ervoor dat de gegevens onderhevig zijn aan encryptie tijdens de overdracht. |
|  | **Resultaat Voorspelling (het verwachte resultaat)**   * Voer gevoelige informatie in via de portal:   + Het systeem moet alle ingevoerde gegevens correct opslaan in de portal. * Verifieer de veilige overdracht van gegevens naar de database:   + De overdracht van gegevens moet veilig zijn, met gebruikmaking van passende encryptietechnieken. * Toegang tot de database:   + De opgeslagen gegevens in de database moeten veilig zijn en alleen toegankelijk voor geautoriseerde personen. |

# 

# Literatuurlijst

What is web application security? | Web security | Cloudflare. (n.d.). Cloudflare. <https://www.cloudflare.com/learning/security/what-is-web-application-security/>

Logging - OWASP Cheat Sheet Series. (n.d.). <https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html>

Hasson, E. (2023, March 14). Web Application Security | What do You Need to Know? | Imperva. Learning Center. <https://www.imperva.com/learn/application-security/web-application-security/>

IBM documentation. (2023, March 17). <https://www.ibm.com/docs/en/db2/11.5?topic=creation-encrypting-existing-database>

Toegangscontrole, zonder kán een organisatie niet. (2021, 24 juni). https://www.securitymanagement.nl/. Geraadpleegd op 13 november 2023, van <https://www.securitymanagement.nl/toegangscontrole>

Accessibility.nl. (z.d.). Accessibility.nl. <https://www.accessibility.nl/>  
  
How to test web applications manually: A Beginner’s guide | Rainforest QA. (n.d.). Rainforest QA Blog | Software Testing Guides. <https://www.rainforestqa.com/blog/test-web-application-manually>

Unadkat, J. (2023, August 28). Website testing: A detailed guide | BrowserStack. BrowserStack. <https://www.browserstack.com/guide/how-to-perform-website-qa-testing>

Vhorne. (2022, November 10). *Tutorial: Create an application gateway with a Web Application Firewall using the Azure portal*. Microsoft Learn.

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-web-application-firewall-portal>