|  |
| --- |
| Sjabloon voor aanpassingen  aan de webapplicatie van  Ultima Casa  **op basis van de aanbevelingen van HackEt.** |

**Inhoud**

[1. Inleiding 3](#_Toc83290512)

[1.1. Categorie-indeling 3](#_Toc83290513)

[2. *<Hoofdstuk uit aanbevelingen HackIt>* 4](#_Toc83290514)

[2.1. Categorie 4](#_Toc83290515)

[2.2. Vereiste aanpassingen 4](#_Toc83290516)

[2.2.1. Functioneel ontwerp 4](#_Toc83290517)

[2.2.2. Product backlog 4](#_Toc83290518)

[2.2.3. Definition of done 4](#_Toc83290519)

[3. *<Hoofdstuk uit aanbevelingen HackIt>* 5](#_Toc83290520)

[3.1. Categorie 5](#_Toc83290521)

[3.2. Vereiste aanpassingen 5](#_Toc83290522)

[3.2.1. Functioneel ontwerp 5](#_Toc83290523)

[3.2.2. Product backlog 5](#_Toc83290524)

[*3.2.3.* Definition of Done 5](#_Toc83290525)

[4. *<Hoofdstuk uit aanbevelingen HackIt>* 6](#_Toc83290526)

[4.1. Categorie 6](#_Toc83290527)

[4.2. Vereiste aanpassingen 6](#_Toc83290528)

[4.2.1. Functioneel ont..... 6](#_Toc83290529)

# Inleiding

Op basis van de aanbevelingen van HackIt moet de webapplicatie van Ultima Casa worden aangepast.

## Categorie-indeling

De volgende categorieën zijn beschikbaar.

|  |  |  |
| --- | --- | --- |
| **Security**  **OWASP** | **Privacy**  **AVG** | **Ethisch**  **Rathenau Instituut** |
| S1. Injection  S2. Broken Authentication  S3. Sensitive Data Exposure  S4. Broken Access Control  S5. Cross Site Scripting XS  S6. Insecure Deserialization | P1. Algemene persoonsgegevens  P2. Bijzondere persoonsgegevens  P3. Strafrechtelijke persoonsgegevens | E1. Maatwerk  E2. Bescheidenheid  E3. Transparantie |

# *Zoekveld Mijn Ultima casa*

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

*Categorie S1 (Injection)*

omdat

*er word een injection gedaan*

*<Waarom denken jullie dat dit de juiste categorie is?>*

De injection word gedaan door bij “Zoek alles” “% OR $=” in te vullen. Zo word er naar data gezocht die mogelijk geclassificeerd is.

## Vereiste aanpassingen

### Functioneel ontwerp

<*Beschrijf hieronder kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *2.2 zoekcriteria* | De mogelijkheid voor SQL injections weghalen |
|  |  |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hieronder kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer product backlog** | **Aanpassing** |
| *2.2 zoekcriteria* | Extra checkbox voor het onmogelijk maken van sql injections |
|  |  |
| *.....* | *.....* |

### Definition of done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

Een filter/zoekfunctie creëren met bindParam in plaats van $\_GET.

# *Gegevens voor server via link ($\_GET)*

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

S3 Sensitive data exposure

omdat

*gevoelige gegevens worden makkelijk gevonden en uitgelezen in de URL*

*<Waarom denken jullie dat dit de juiste categorie is?>*

Omdat er niks aan hacking gedaan word, je kan het meteen uitlezen zonder enige bescherming

## Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *globaal* | *Afschermen van gevoelige gegevens in de URL* |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *Globaal* | Checkbox erbij, post gebruiken bij persoonsgegevens. |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

Wanneer er voor gevoelige gegevens POST is gebruikt.

# Rollensysteem functioneert niet

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

S4. Broken Access Control

Omdat

Een user die niet als admin is ingelogd kan gemakkelijk in de admin panel zonder dat die rechten heeft

*<Waarom denken jullie dat dit de juiste categorie is?>*

*Omdat een normale user doormiddel van de URL te veranderen in de admin panel kan en daar kan de user accounts aanpassen.*

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *6 ultima casa administrator* | Een validatiesysteem maken dat controleert of de gebruiker is ingelogd als administrator |
| *5 ultima casa beheer* | Een validatiesysteem maken dat controleert of de gebruiker is ingelogd als administrator |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *5 ultima casa beheer* | Check maken waar word gecontroleerd of de ingelogde gebruiker een administrator is. |
| *6 ultima casa administrator* | Check maken waar word gecontroleerd of de ingelogde gebruiker een administrator is. |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

De oplossing is gedaan wanneer er een actieve validatie word gedaan van het account wanneer de url word geladen. Wanneer een gebruiker niet is ingelogd word de gebruiker gelijk naar de homepage geboot met een error message.

# Veel wachtwoorden zijn zwak

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

P1 algemene persoonsgegevens.

Omdat

Zwakke wachtwoorden kunnen makkelijk worden aangepast en het valt onder persoonsgegevens.

*<Waarom denken jullie dat dit de juiste categorie is?>*

*Omdat er bij andere categorieën niks word gezegd over slechte wachtwoorden, ook omdat dit niet een security issue is meer een onhandigheid omdat de wachtwoorden alsnog de accounts beveiligen, maar wel makkelijk te raden zijn.*

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *1 inloggen* | *Alle gebruikers een beter wachtwoord laten kiezen.* |
| *2.4 account* | Parameters geven aan gebruikers voor bijvoorbeeld unieke wachtwoorden (generators kunnen) of verplichte hoofdletters of tekens. |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *1.2 account aanmaken* | Check maken waar verplichtingen worden gegeven aan de gebruiker om een beter wachtwoord te maken, denk aan hoofdletters, lengte en tekens. |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

De aanpassingen zijn compleet wanneer er voor elke user een uniek wachtwoord is dat goeg genoeg beveiligd is.

# Invoervelden kunnen script bevatten

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

S1. Injection

omdat

*er een js script inject wordt.*

*<Waarom denken jullie dat dit de juiste categorie is?>*

Omdat er code gebruikt wordt om de website te manipuleren waar dat niet hoort te kunnen.

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *2.4.1 account wijzigen* | Limiteren van type tekens die gebruikt mogen worden bij het maken van een account |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *1.2* | Checkbox waar wordt gechecked of de usernames en andere velden sanitized zijn (geen speciale tekens) |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

Wanneer er geen speciale tekens kunnen worden gebruikt bij het creëren van een account.

# Privacy gevoelige gegevens in database niet versleuteld

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

S3. Sensitive Data Exposure

omdat

*er gevoelige data in de database zit die niet goed versleuteld is en dus makkelijker kan worden uitgelezen*

*<Waarom denken jullie dat dit de juiste categorie is?>*

Omdat gevoelige data makkelijk te vinden is als de database niet goed afgeschermt is.

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *algemeen* | Afschermen van gevoelige data in de database |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *2.4.0* | Check toevoegen waar wordt gecontroleerd of de data in de database goed is afgeschermd en alleen kan worden uitgelezen door de correcte gebruiker |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

De aanpassing is klaar wanneer de data van accounts in de database goed is afgeschermd en alleen door de juiste gebruikers kan worden uitgelezen

# Verboden zoekcriteria

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

P3. Strafrechtelijke persoonsgegevens

Omdat

Er op persoonlijke gegevens gezocht kan worden

*<Waarom denken jullie dat dit de juiste categorie is?>*

Omdat de gegevens waarop gezocht kan worden persoonlijk kunnen zijn

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *2.2 zoekcriterium* | Onmogelijk maken om bepaalde zoekcriteria te gebruiken bij het zoeken naar een huis. |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *2.2.1 criterium toevoegen* | Een limiet zetten op hoe persoonlijk de zoekcriteria kunnen worden gemaakt |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

*De aanpassing is klaar wanneer de zoekcriteria tot een bepaald niveau persoonlijk kunnen zijn.*

# Toestemming gebruik persoonlijke gegevens

## Categorie

*<Welke categorie uit hoofdstuk 2.1 Categorie-indeling hoort bij deze aanbeveling van HackEt?>*

P3. Strafrechtelijke persoonsgegevens

Omdat

Er persoonlijke data

*<Waarom denken jullie dat dit de juiste categorie is?>*

Omdat de gegevens waarop gezocht kan worden persoonlijk kunnen zijn

Vereiste aanpassingen

### Functioneel ontwerp

<B*eschrijf hier kort in welke hoofdstukken van het huidige functioneel ontwerp je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Functioneel ontwerp** | **Aanpassing** |
| *2.2 zoekcriterium* | Onmogelijk maken om bepaalde zoekcriteria te gebruiken bij het zoeken naar een huis. |
| *.....* | *.....* |

### Product backlog

*<Beschrijf hier kort in welke hoofdstukken van de huidige product backlog je welke aanpassingen moet maken.*>

|  |  |
| --- | --- |
| **Hoofdstuknummer Product Backlog** | **Aanpassing** |
| *2.2.1 criterium toevoegen* | Een limiet zetten op hoe persoonlijk de zoekcriteria kunnen worden gemaakt |
| *.....* | *.....* |

### Definition of Done

*<Beschrijf hier welke aanvullingen/aanpassingen je moet maken in de huidige definition of done.>*

*De aanpassing is klaar wanneer de zoekcriteria tot een bepaald niveau persoonlijk kunnen zijn.*