|  |
| --- |
| Aanbevelingen  voor aanpassingen aan de webapplicatie van  Ultima Casa  teneinde de  **security, privacy en etische**  **normen en waarden van hedendaagse software te respecteren** |
| **door HackEt**  ***De ethische hackers voor het MKB***  **www.hacket.nl** |

[1. Inleiding 3](#__RefHeading__94_1612747664)

[2. Zoekveld Mijn Ultima Casa 4](#__RefHeading__96_1612747664)

[2.1. URL 4](#__RefHeading__98_1612747664)

[2.2. Trigger 4](#__RefHeading__100_1612747664)

[2.3. Resultaat 4](#__RefHeading__102_1612747664)

[3. Gegevens voor server via link ($\_GET) 5](#__RefHeading__104_1612747664)

[3.1. URL 5](#__RefHeading__106_1612747664)

[3.2. Trigger 5](#__RefHeading__108_1612747664)

[3.3. Resultaat 5](#__RefHeading__110_1612747664)

[4. Rollensysteem functioneert niet 6](#__RefHeading__112_1612747664)

[4.1. URL 6](#__RefHeading__114_1612747664)

[4.2. Trigger 6](#__RefHeading__116_1612747664)

[4.3. Resultaat 6](#__RefHeading__118_1612747664)

[5. Veel wachtwoorden zijn zwak 7](#__RefHeading__120_1612747664)

[5.1. URL 7](#__RefHeading__122_1612747664)

[5.2. Trigger 7](#__RefHeading__124_1612747664)

[5.3. Resultaat 7](#__RefHeading__126_1612747664)

[6. Invoervelden kunnen script bevatten 8](#__RefHeading__128_1612747664)

[6.1. URL 8](#__RefHeading__130_1612747664)

[6.2. Trigger 8](#__RefHeading__132_1612747664)

[6.3. Resultaat 8](#__RefHeading__134_1612747664)

[7. Privacy gevoelige gegevens in database niet versleuteld 9](#__RefHeading__136_1612747664)

[7.1. URL 9](#__RefHeading__138_1612747664)

[7.2. Trigger 9](#__RefHeading__140_1612747664)

[7.3. Resultaat 9](#__RefHeading__142_1612747664)

[8. Verboden zoekcriteria 10](#__RefHeading__144_1612747664)

[8.1. URL 10](#__RefHeading__146_1612747664)

[8.2. Trigger 10](#__RefHeading__148_1612747664)

[8.3. Resultaat 10](#__RefHeading__150_1612747664)

[9. Toestemming gebruik persoonlijke gegevens 11](#__RefHeading__152_1612747664)

[9.1. URL 11](#__RefHeading__154_1612747664)

[9.2. Trigger 11](#__RefHeading__156_1612747664)

[9.3. Resultaat 11](#__RefHeading__158_1612747664)

[10. Getoonde tabbladen 12](#__RefHeading__160_1612747664)

[10.1. URL 12](#__RefHeading__162_1612747664)

[10.2. Trigger 12](#__RefHeading__164_1612747664)

[10.3. Resultaat 12](#__RefHeading__166_1612747664)

[11. Summiere meldingen 13](#__RefHeading__168_1612747664)

[11.1. URL 13](#__RefHeading__170_1612747664)

[11.2. Trigger 13](#__RefHeading__172_1612747664)

[11.3. Resultaat 13](#__RefHeading__174_1612747664)

# Inleiding

De onderstaande bevindingen en aanbevelingen zijn tot stand gekomen

* naar aanleiding van het rapport van de AVG waakhond (Algemene verordening gegevensbescherming).
* op basis van de huidige algemeen geaccepteerde sociaal maatschappelijke normen en waarden.
* met als uitgangspunt de huidige in de beroepsgroep stand van zaken v.w.b. secure software development, zoals beschreven in de Top 10 Web Application Security Risks (OWASP).

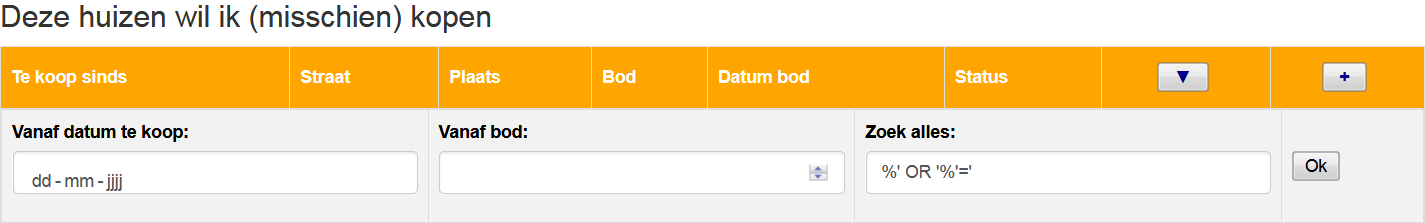
Niet alle aanbevelingen zijn gebaseerd op wettelijk verplichtingen.

# Zoekveld Mijn Ultima Casa

## URL

relatie.php?RID=521

## Trigger

In het veld *Zoek alles:* invullen %' OR '%'='

## Resultaat

|  |  |
| --- | --- |
|  | Alle huizen waarin alle relaties interesse hebben worden (soms meerdere keren) zichtbaar. Zo kunnen alle relaties zien wat andere relaties hebben geboden op alle te koop staande huizen. |

# Gegevens voor server via link ($\_GET)

## URL

vrijwel alle URL's in Ultima Casa webapplicatie

## Trigger

Bijvoorbeeld:

*koopupd.php?Bod=520000&Datum=2021-02-01&BID=3&RID=673*

of

*maakaccount-save.php?Naam=aaaaaa&Email=matahari@gmail.com&Wachtwoord=12345&Tel .......*

## Resultaat

Op deze wijze is eenvoudig zichtbaar, aanpasbaar en traceerbaar welke gegevens de browser verzendt en in de database bij welke ID's deze worden opgeslagen. Een willekeurige gebruiker kan met wat proberen eenvoudig de gegevens van een andere relatie aanpassen. Een onbeveiligd verstuurd wachtwoord kan zo eenvoudig worden onderschept.

# Rollensysteem functioneert niet

## URL

admin.php?RID=529

## Trigger

Een willekeurige gebruiker/relatie kan met wat proberen bovenstaande URL achterhalen.

## Resultaat

Een willekeurige gebruiker/relatie heeft toegang tot de admin functionaliteiten.Op deze manier kan iedereen alle accounts beheren zonder als admin te zijn ingelogd. Voor hackers is dit een koud kunstje.

# Veel wachtwoorden zijn zwak

## URL

maakaccount.php

## Trigger

|  |  |
| --- | --- |
| Ultima Casa account aanvragen, wachtwoord kiezen. |  |

## Resultaat

De gebruiker kan een willekeurig (zwak) wachtwoord intikken wat veelal resulteert in een wachtwoord dat in de bij hackers bekende database van veel voorkomende wachtwoorden staat. Een hackers heeft zo'n wachtwoord al snel achterhaald.

# Invoervelden kunnen script bevatten

## URL

relatie.php?RID=673

## Trigger

|  |  |
| --- | --- |
| Mijn Ultima Casa tabblad Account, bij het veld Naam een script invullen:  <script>location.href = "http://www.w3schools.com";</script> |  |

## Resultaat

Elke keer als de Ultima Casa webapplicatie de Naam van relatie 673 laat zien, wordt de in dit geval onschuldige website www.w3schools.com geopend. Dit kan echter ook een site zijn waarmee hackers kwade bedoelingen hebben.

# Privacy gevoelige gegevens in database niet versleuteld

## URL

relatieins.php, relatieupd.php, adresins.php, adresupd.php

## Trigger

Privacy gevoelige gegevens (naam, email, telefoon, adres en de combinatie hiervan) kan eenvoudig uit een kopie of een backup van de database of een sql export van de database gelezen worden. Zeker als de database(inhoud) door kwaadwillenden gestolen wordt.

## Resultaat

De privacy gevoelige gegevens van alle relatie kunnen zomaar "op straat" komen te liggen.

# Verboden zoekcriteria

## URL

verkoopplus.php, verkoopedit.php, relatie.php tabblad Zoekcriteria

## Trigger

Invullen van de zoekcriteria voor het kopen van of te koop aanbieden van een huis.

## Resultaat

De zoekcriteria op basis waarvan een relatie een huis te koop aanbied of een huis zoekt bevatten verboden elementen. Aan de AVG voorwaarden voor verwerking van Algemene, Bijzondere en Strafrechtelijke persoonsgegevens wordt niet in voldoende mate voldaan.

# Toestemming gebruik persoonlijke gegevens

## URL

maakaccount.php

## Trigger

Invullen van de persoonlijke gegevens en deze gegevens opslaan.

## Resultaat

De persoonlijke gegevens worden opgeslagen zonder hiervoor toestemming wordt gevraagd. In de AVG staat een aantal eisen waaraan toestemming moet voldoen. De persoonsgegevens mogen zonder deze toestemming niet verwerkt worden.

# Getoonde tabbladen

## URL

relatie.php

## Trigger

Actie op een tabblad anders dan het eerste.

## Resultaat

Nadat de gebruiker een actie heeft bevestigd (bijvoorbeeld op de knop Annuleren klikt op het tabblad Account) toont de applicatie het eerste tabblad (Huizen die ik wil kopen). Dit is voor onervaren gebruikers verwarrend.

# Summiere meldingen

## URL

Alle pagina's met invoervelden die aan zekere voorwaarden moeten voldoen (zoals Telefoon, Email).

URL's die gegevens in de database opslaan.

|  |  |
| --- | --- |
| Trigger | Resultaat |
| Onjuiste / onvolledige invoer. | De meldingen zijn vaag.  *Gebruik de gevraagde indeling* geeft onvoldoende duidelijk aan wat er wel ingevuld moet worden. |
| Systeemfout bij toevoegen/wijzigen/verwijderen in database | Onduidelijk voor de gebruiker hoe dit op te lossen (bijvoorbeeld *neem contact op met de helpdesk)* |