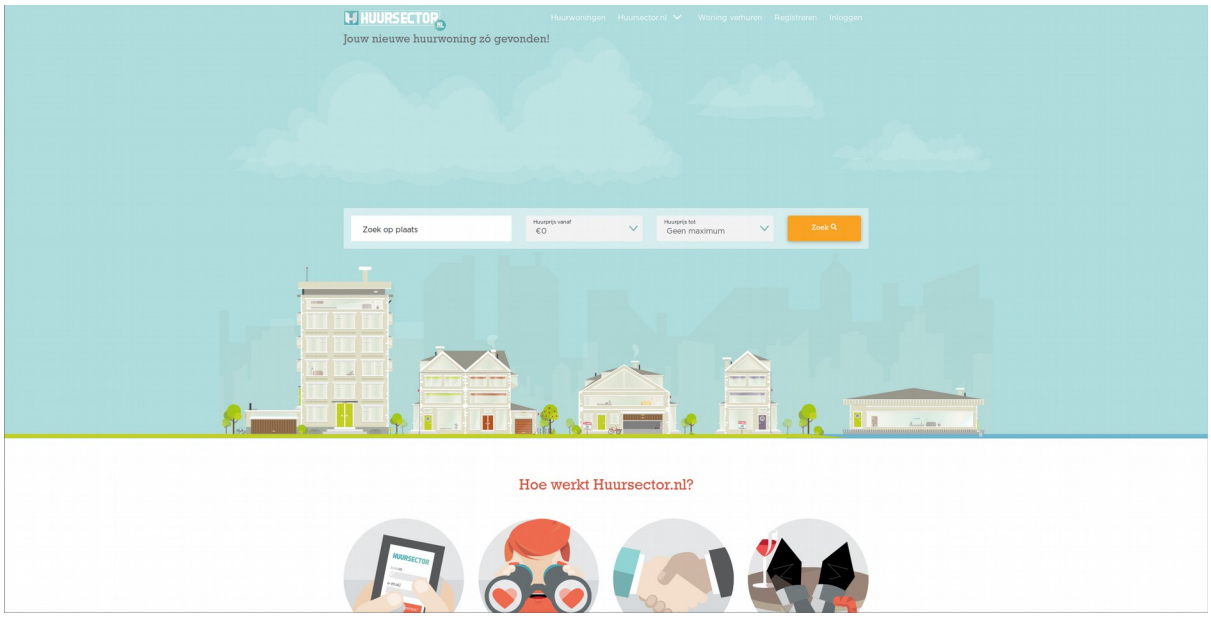
Vulnerability rapport over:

https://www.huursector.nl/



Bedrijf: Hackoclipse
Datum: 9 September 2019

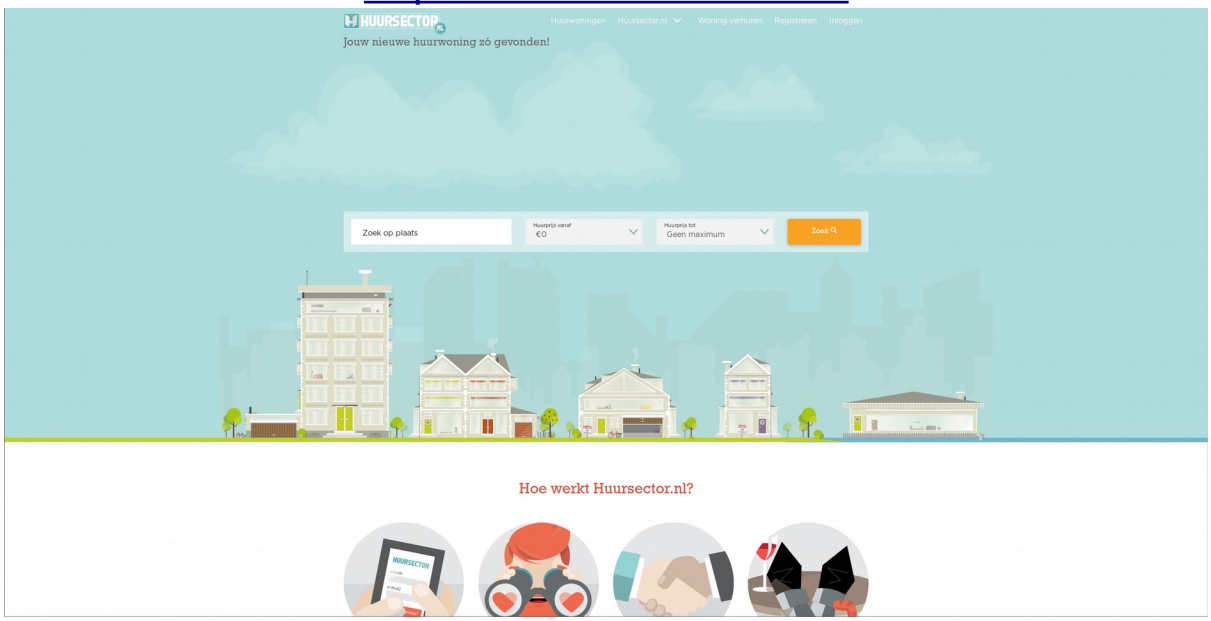
Inhoud

1. Wat is de opdracht....3
1. Zeer hoge prioriteit....4
1.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van iemand anders advertentie....4
1.2. Insecure direct object reference in advertentie bewerken leidt tot verwijdering van iemand anders advertentie....10
2. Hoge prioriteit....14
2.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van al geaccepteerde advertentie....14
2.2. Insecure direct object reference in bewerken leidt tot verwijdering van al aangeboden advertentie....19
2.3. Stored cross site scripting door middel van het bewerken van een woning voordat het geaccepteerd is....23
3. Gemiddelde prioriteit....28
3.1. 2 reflective xss'en in de facebook autorisatie en google autorisatie doormiddel van malformed url....28
3.2. Bypass om een naam van een premium account aan te passen zonder dat de user dit hoort te kunnen....33
3.3. Klachten die worden ontvangen worden niet escaped voordat ze worden verstuurt....37
3.4. Reacties die worden ontvangen bij adverteerders worden niet escaped voordat ze worden verstuurt....39
3.5. Berichten die worden verstuurt naar de medewerkers worden niet escaped voordat ze worden verstuurt....42
3.6. De bevestigingsmails van het contactformulier worden niet escaped waardoor het mogelijk is om spam te sturen vanaf het huursector domein....45
4. lage prioriteit....47
4.1. Geen rate limiting op contact en klachtenformulier....47

1. Wat is de opdracht

Het testen van mogelijke kwetsbaarheden van de website:

https://www.huursector.nl/



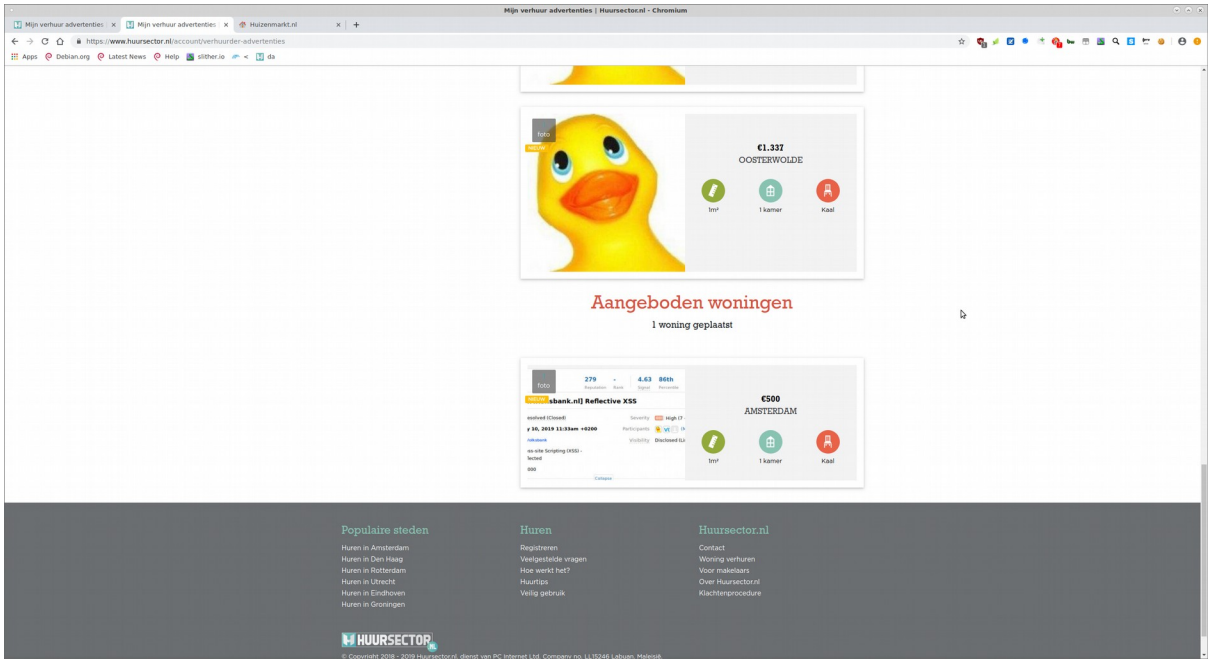
De test moest gedaan worden op 1,4 en 9 September 2019.
Hiervan moet een duidelijk rapport gemaakt worden.
Voor alle proof of concepts is of chrome/chromium gebruikt of firefox en soms burpsuite, maar dit is niet verplicht om de poc's uit te voeren.
Sommige lekken zijn al verholpen.

1. Zeer hoge prioriteit

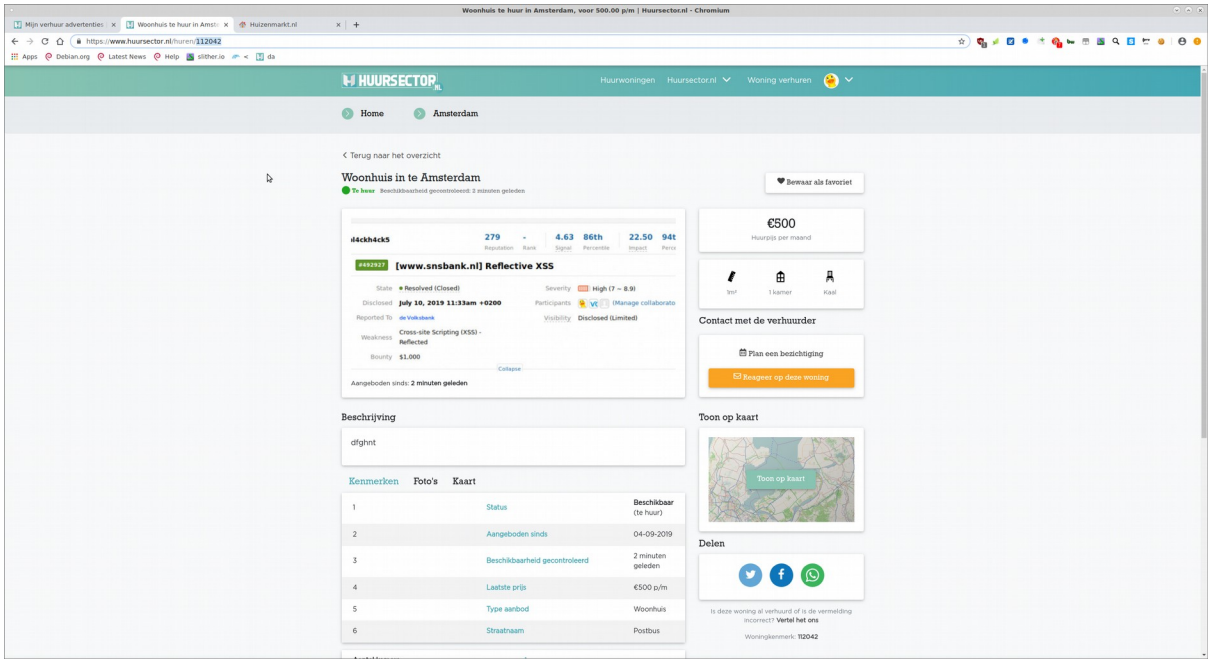
1.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van iemand anders advertentie.

Tijdens mijn onderzoeken op 4 September kwam ik er achter dat als je een advertentie aanmaakt met een premium account die nog niet is goedgekeurd, als je dan die advertentie verwijdert en het advertentienummer vervangt met een andere advertentie die niet van jouw is.
Dan wordt die andere advertentie verwijdert ook al hoor je dit recht niet te hebben.
Dit maakt het mogelijk om iedereens advertentie te verwijderen.

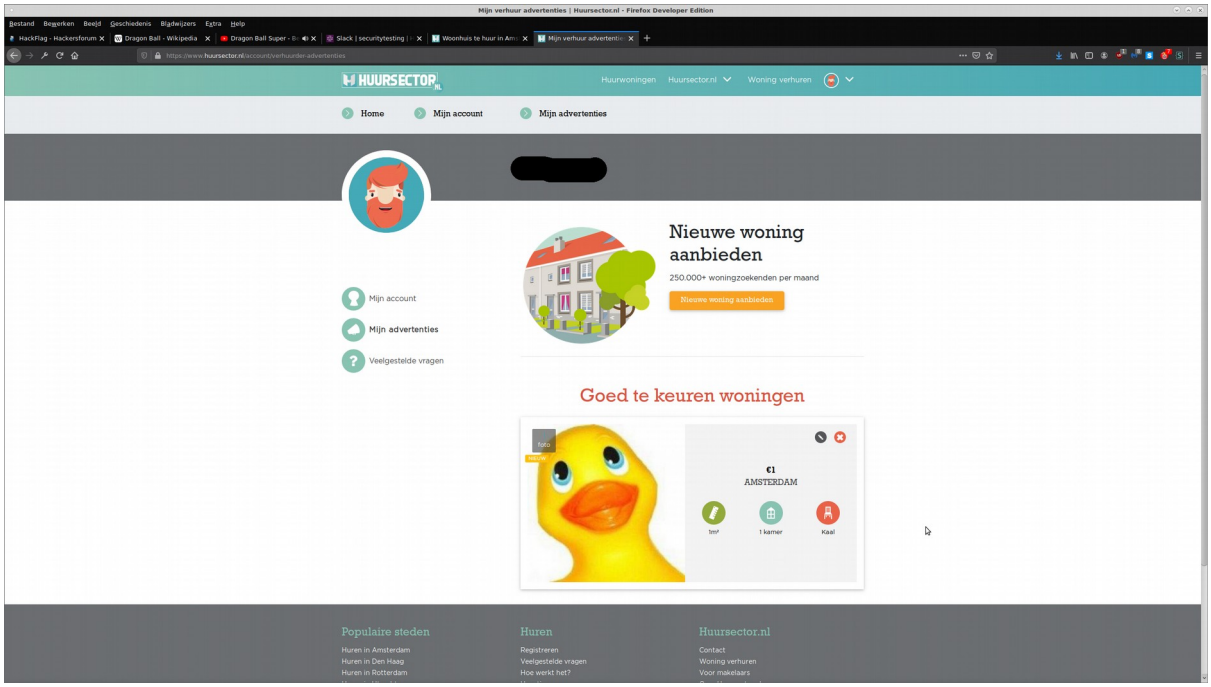
Om deze lek te verifiëren moet u eerst ingelogd zijn met een premium users en naar de webpagina “mijn advertenties” gaan.
U moet nu een advertentie aanmaken en terug naar de “mijn advertenties“ pagina.
Als de advertentie is aangemaakt, het huursector team heeft de advertentie geaccepteerd en hij staat in de “aangeboden woning” kunt u deze advertentie openen.



Als u dat heeft gedaan komt u op uw advertentie en in de url staat een nummer.



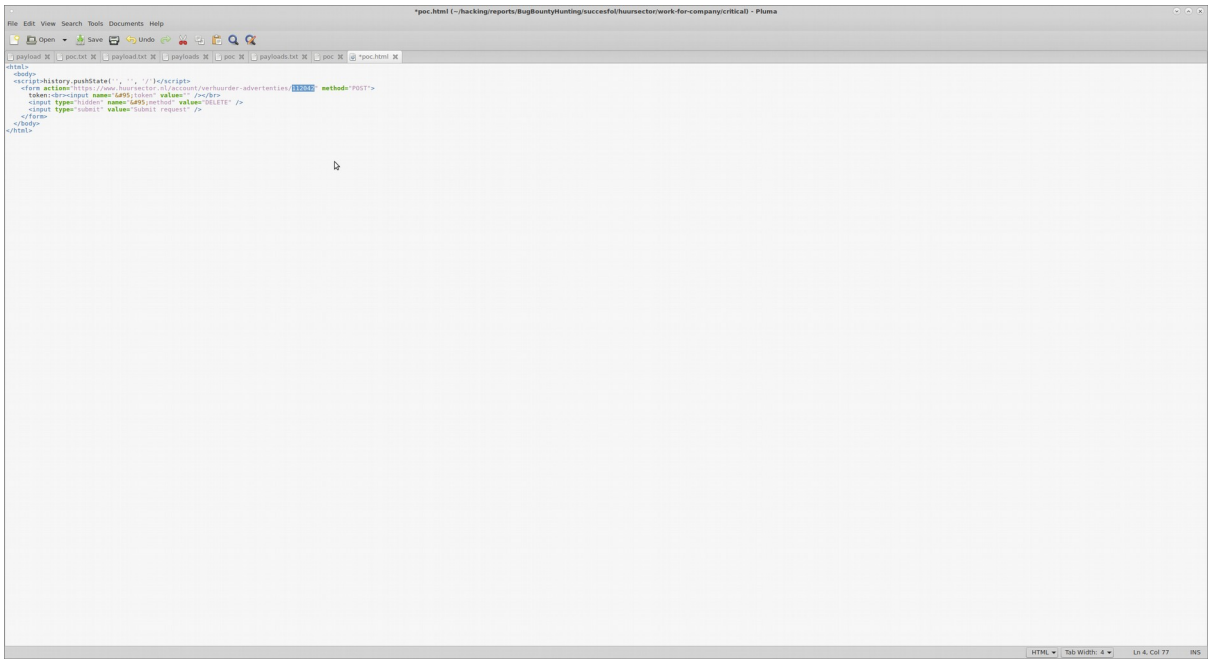
kopieer dit nummer en sla dit ergens even op want dit hebben we straks nodig.
Nu open de tweede premium account (de hacker account) en maak daar ook een advertentie aan, maar hij mag nog niet goedgekeurd worden.



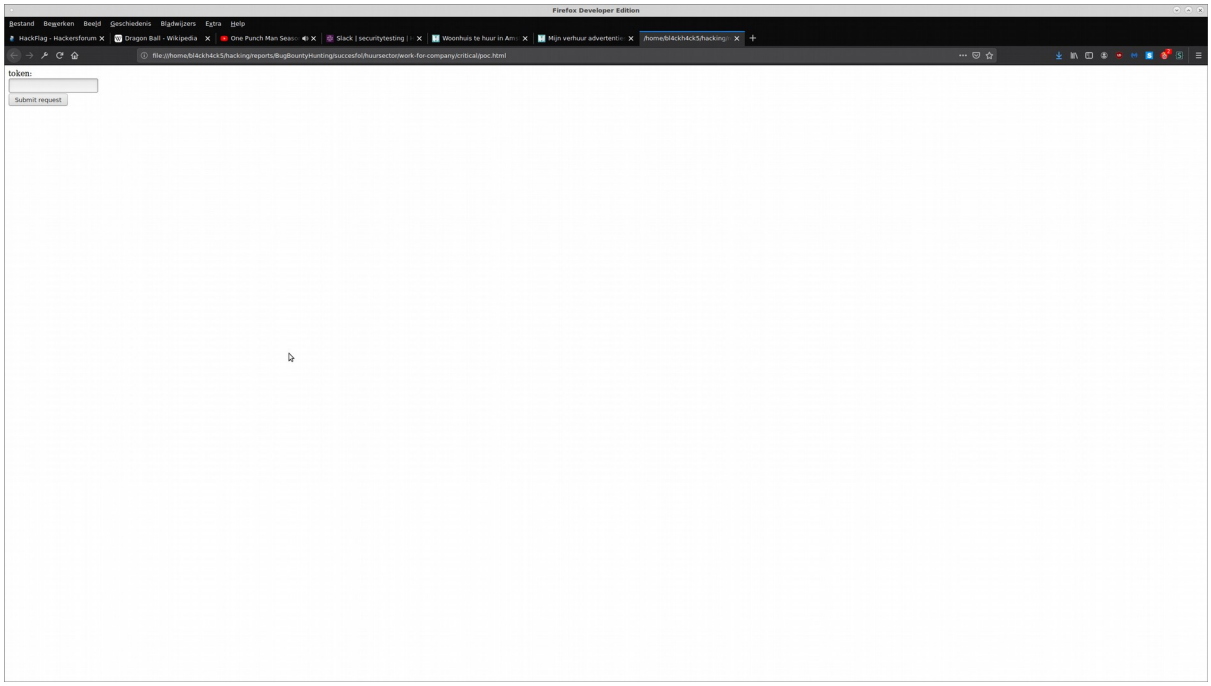
nu maak een nieuwe html file met de code die hieronder staat met bijvoorbeeld notepad++.

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.huursector.nl/account/verhuurder-advertenties/
112042" method="POST">
      token:<br><input name="&#95;token" value="" /></br>
      <input type="hidden" name="&#95;method" value="DELETE" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

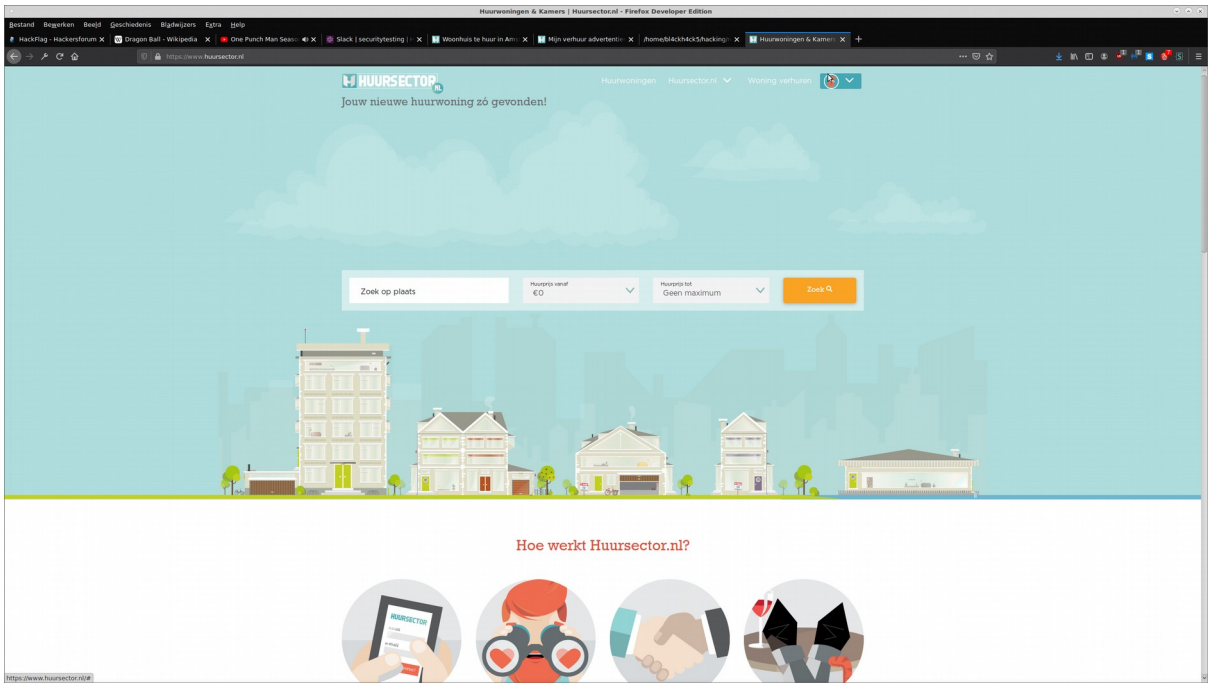
Dan verander het nummer 112042 met het nummer van de advertentie die we weg willen gooien (dat was dat nummer dat we van straks opsloegen) en sla de html file op.



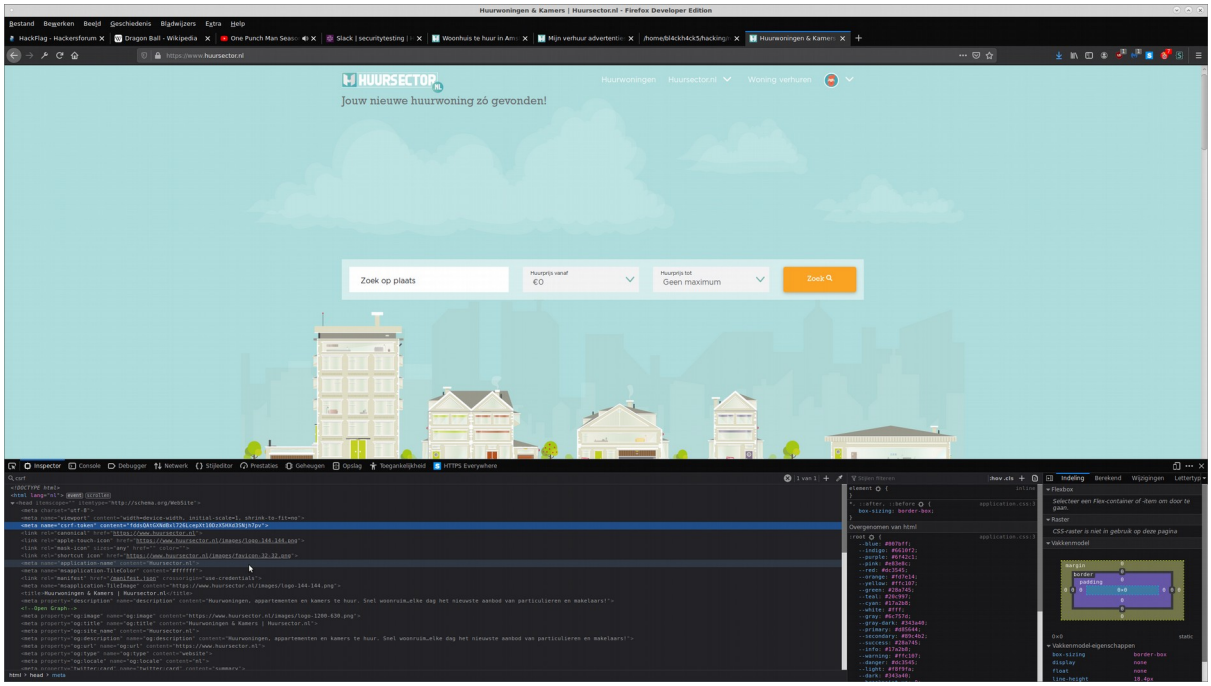
Nu open deze html file in een nieuwe tab in firefox naast de “hackers” account.
Je zult nu een knop en een veld zien.



Nu open nog een nieuwe tab in firefox en ga naar de hoofdpagina https://www.huursector.nl/

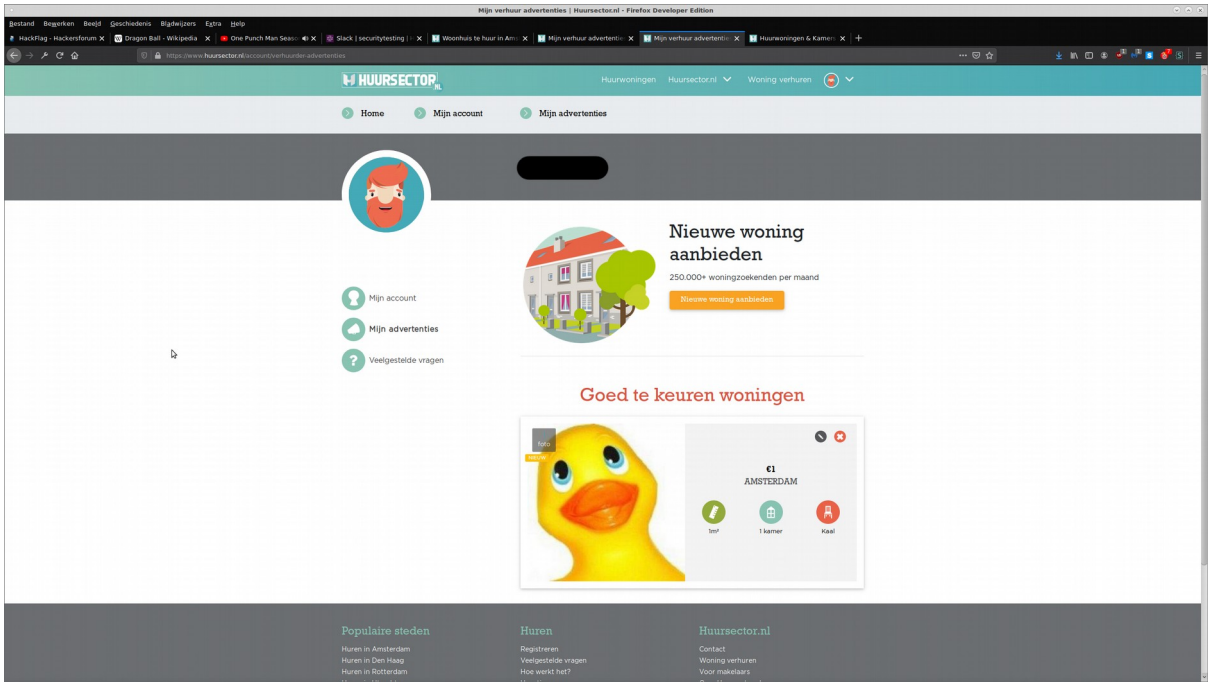


Daar open elemental inspect (rechtsklik staat ergens in dat menu) en zoek naar “csrf-token”
Je zult een meta tag zien die csrf-token heet waar in content een random zin staat. kopieer exact wat er in content staat tussen de aanhalingstekens. (een spelfout en het mislukt)

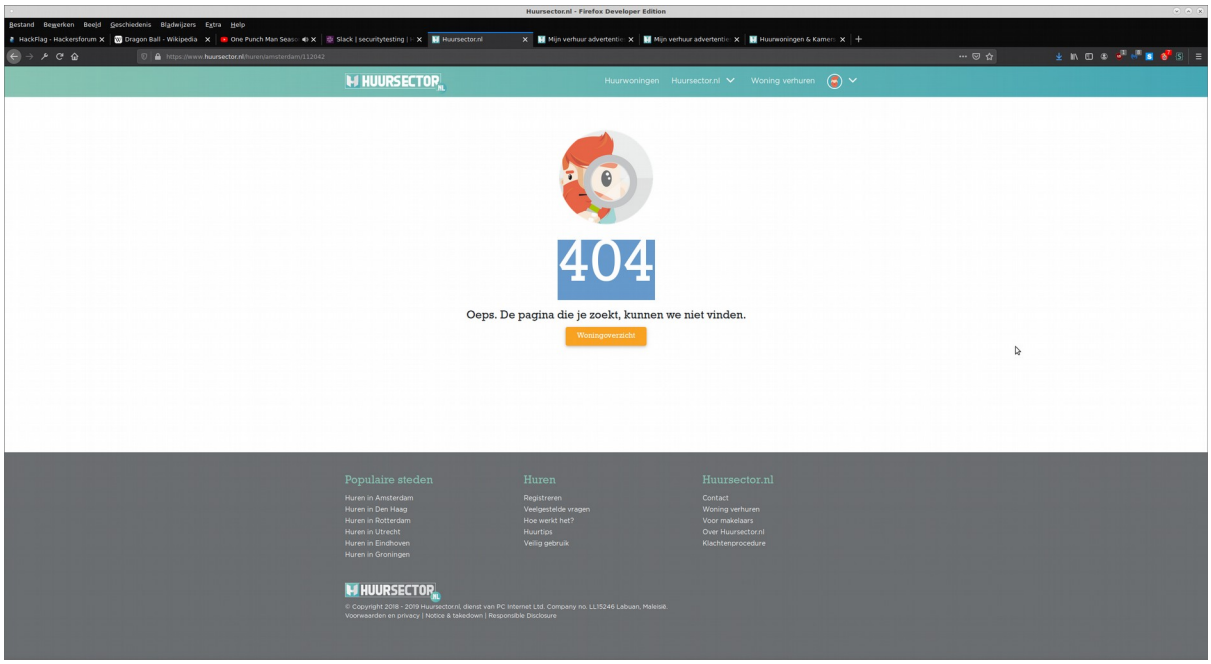


als je dat hebt gekopieerd ga terug naar de html file in een andere tab en plak in het veld de code die je net kopieerde en dan druk op submit.

Als het goed ging kom je terug in de “mijn advertenties” pagina.
Als je niet op die pagina komt heb je mogelijk iets fout gedaan en ben je niet in de verhuurder profiel geweest toen je starten of je maakten een tik fout toen je de token kopieerde en plakten (dat merk je door een session error of je komt op een andere pagina.)



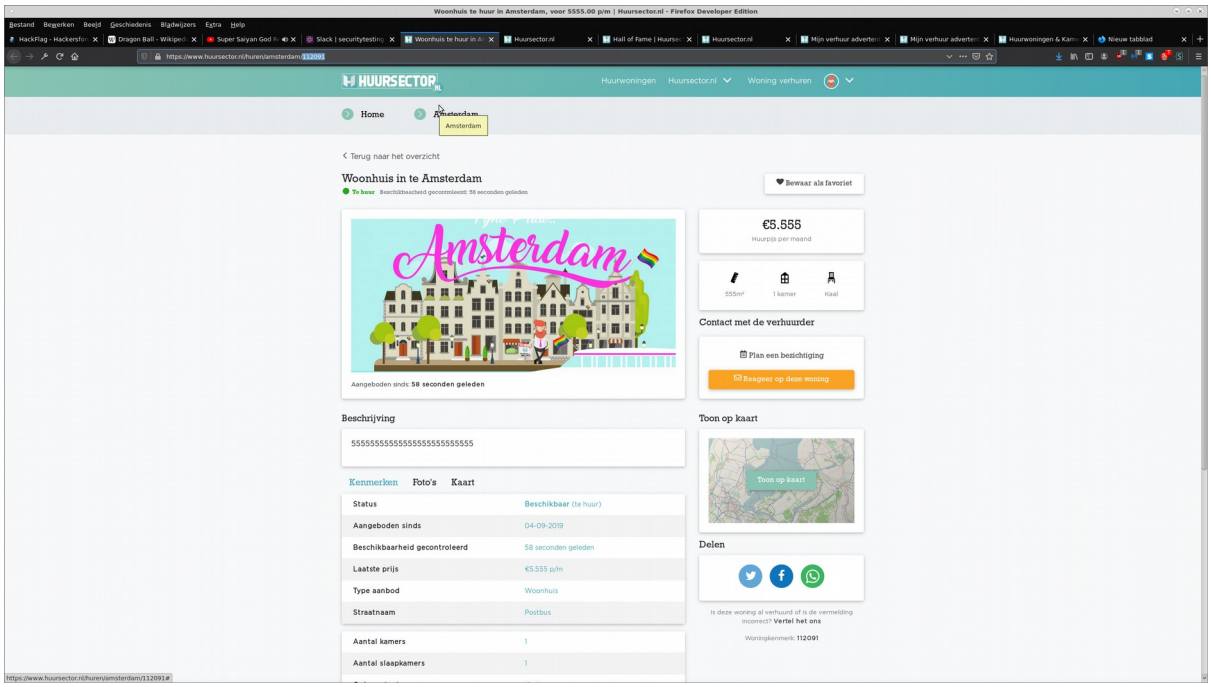
als je nu terug gaat naar de advertentie die je wilden weggooien zul je merken dat deze nu weg is.



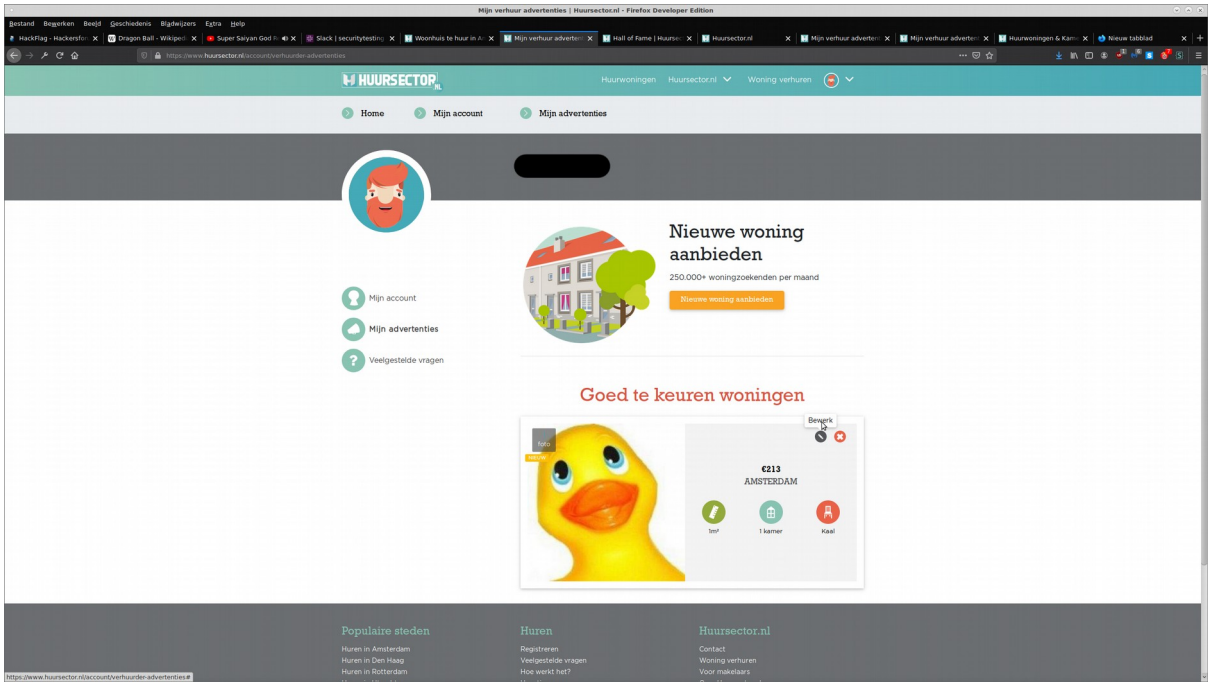
1.2. Insecure direct object reference in advertentie bewerken leidt tot verwijdering van iemand anders advertentie.

Tijdens mijn onderzoeken op 4 September kwam ik er achter dat als je een advertentie aanmaakt met een premium account die nog niet is goedgekeurd, als je die dan bewerkt en dan in de url het nummer van de advertentie verandert naar een andere advertentie die niet van jouw is.
Dan kun je als je de advertentie dan opslaat hem laten verdwijnen.

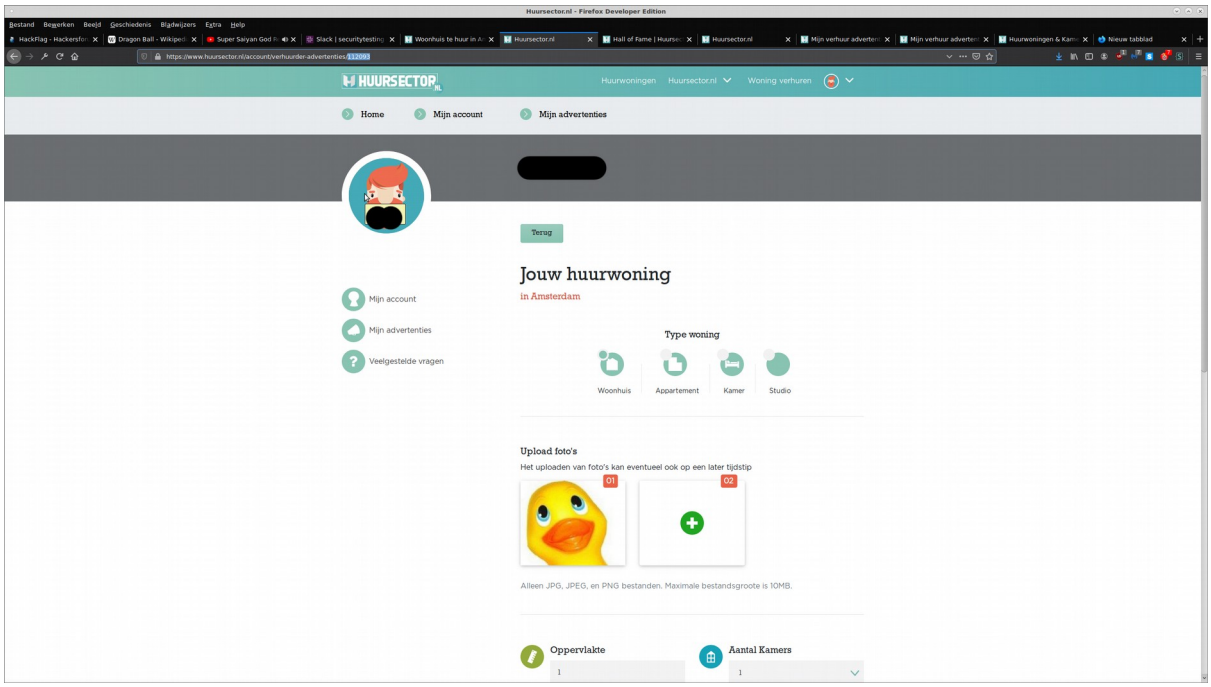
Om deze lek te verifiëren moet u eerst een advertentie hebben die is gemaakt met een premium user.
Ga dan naar die advertentie.
Dan kopieer je het nummer die in de url staat en slaat dat op voor later.



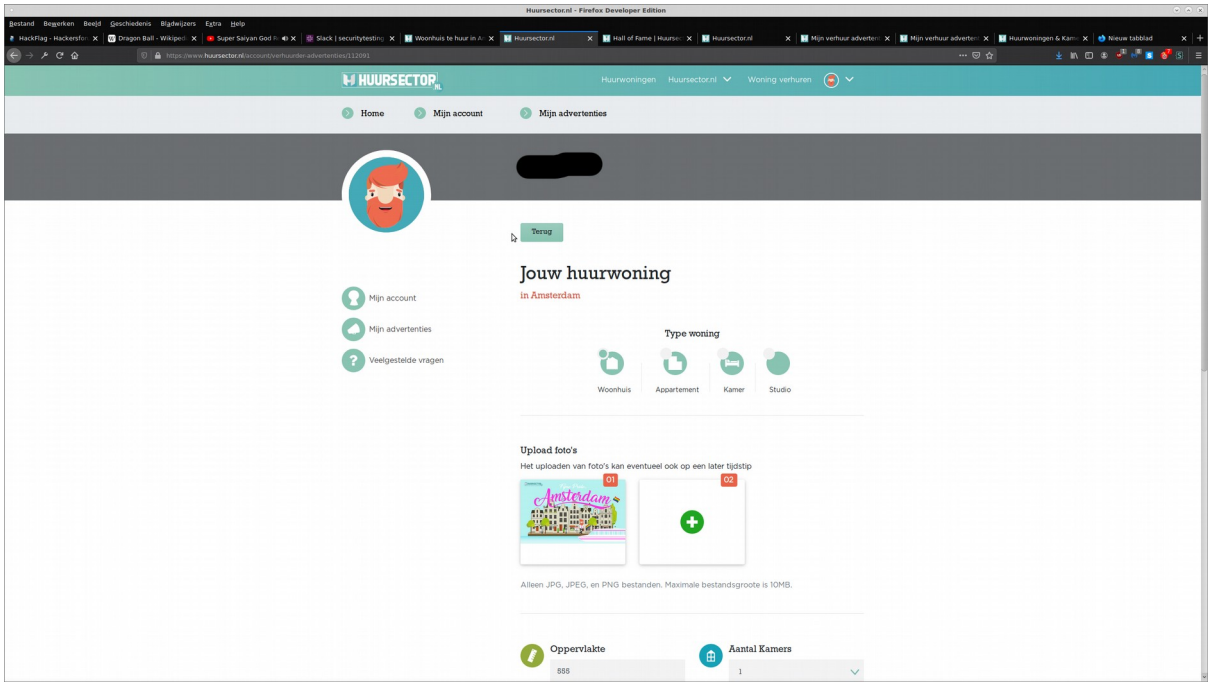
Nu log je in met een andere account die niet deze advertentie had gemaakt (hackers account) en maak je een nieuwe advertentie aan, maar die nog niet goedgekeurd is.
Ga dan naar de “mijn advertenties” sectie en druk daar bij de advertentie die je had gemaakt op bewerk.



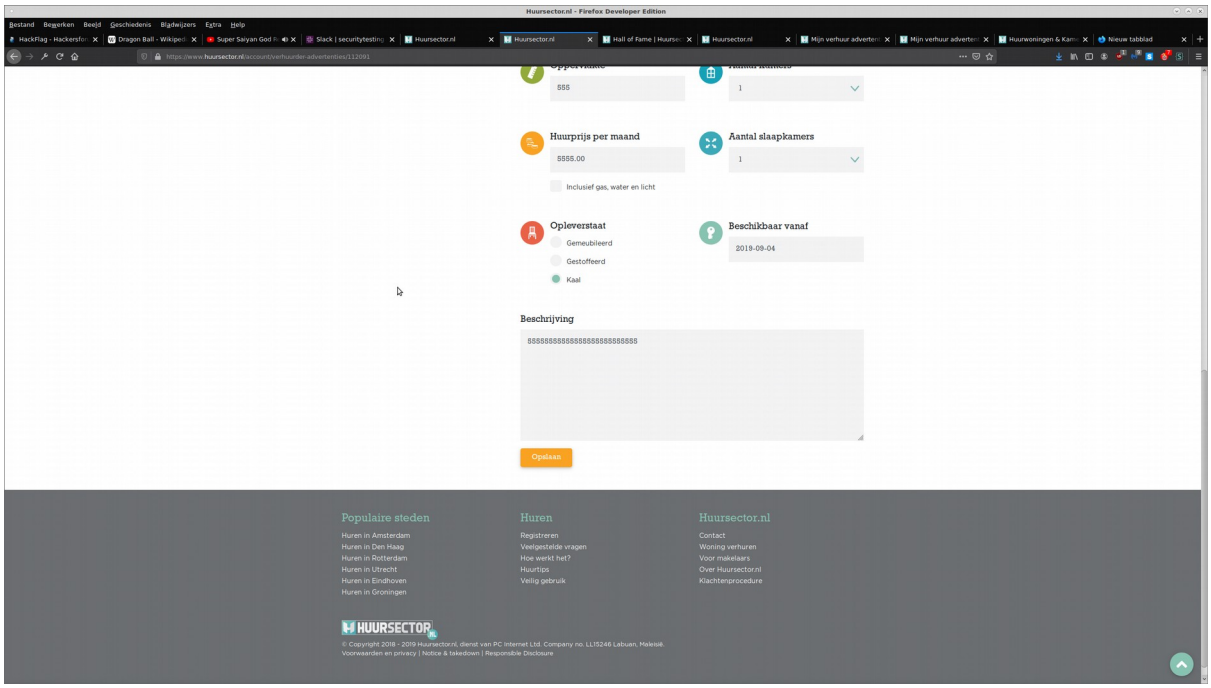
Nu je op de bewerk pagina bent zul je merken dat er in de url een nummer staat.



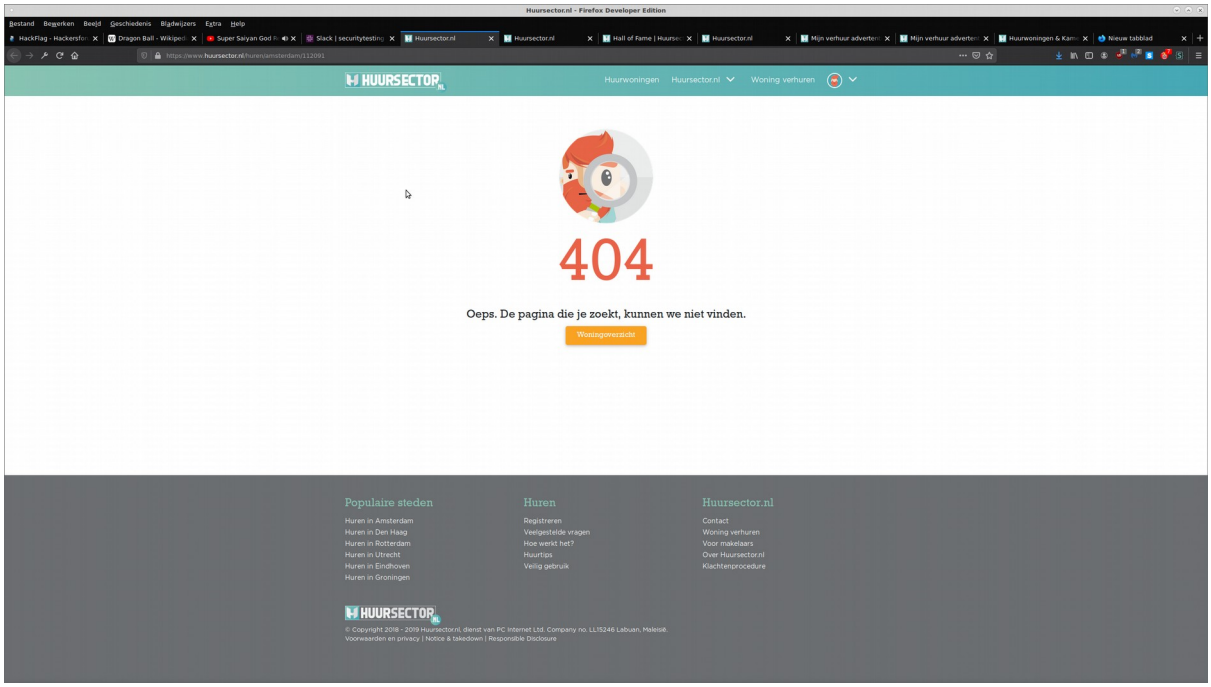
Verander dat nummer naar het nummer dat we hadden opgeslagen (het advertenties nummer van de advertentie die we willen wissen)
als de foto hetzelfde wordt als de foto van de advertentie die we willen wissen heb je tot nu toe alles goed gedaan. (lek van zijn eigen)



scroll nu naar beneden en in de beschrijving plaats 1 extra teken (niet zeker of dit moet) en druk op opslaan.



Als je op opslaan hebt gedrukt en dan terug gaat naar de advertentie die we wilden verwijderen zult u merken dat hij verdwenen is.

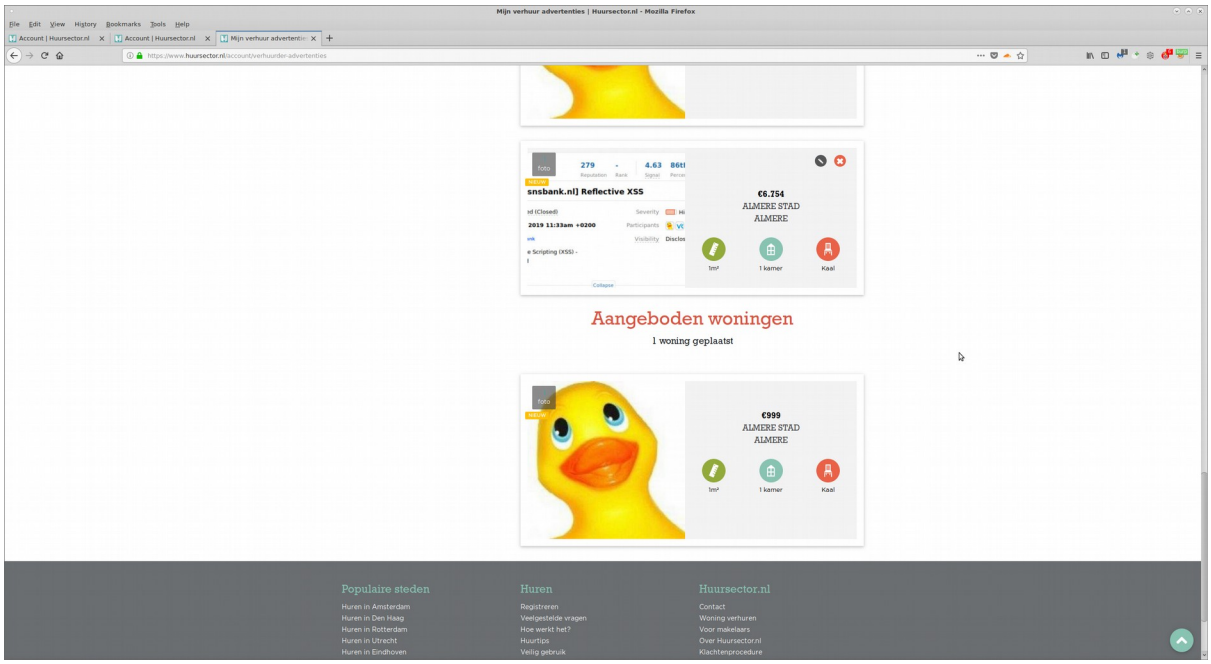


2. Hoge prioriteit

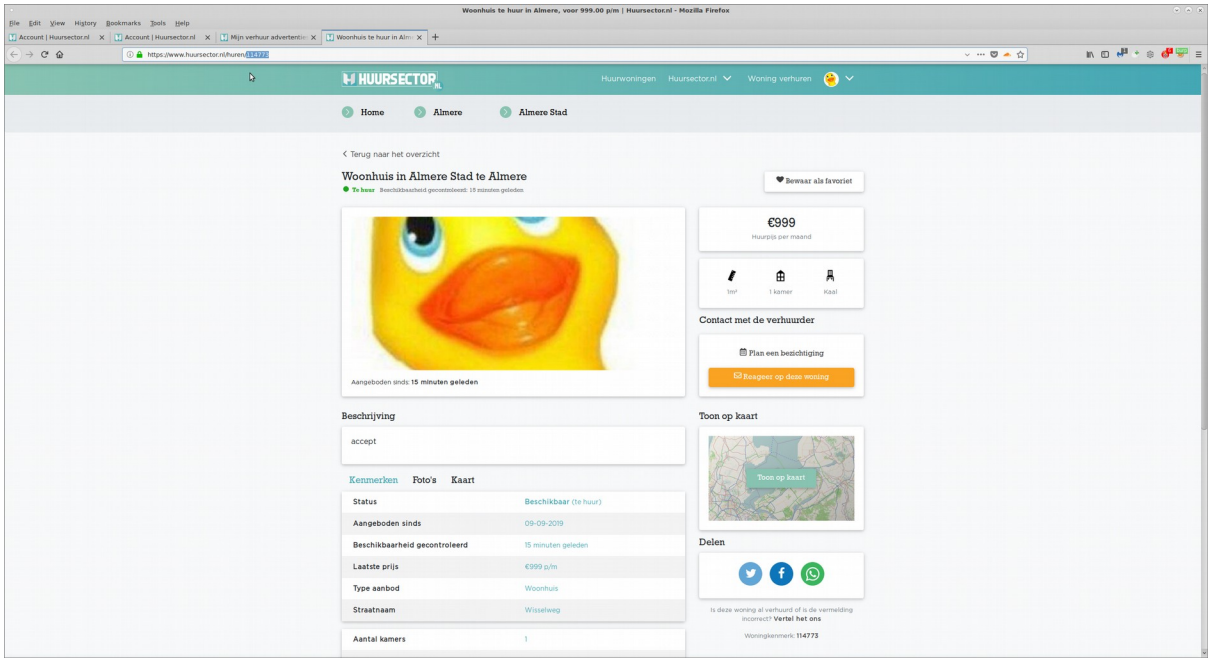
2.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van al geaccepteerde advertentie.

Tijdens mijn onderzoeken op 9 September kwam ik er achter dat als je een advertentie aanmaakt met een premium account die al aangeboden is, dat het mogelijk is om de aangeboden woning te verwijderen door het request op te sturen van het verwijderen van een nog niet aangeboden advertentie, maar dat je dan het advertentienummer vervangt met een advertentie die al aangeboden is.
Dit maakt het mogelijk om een advertentie te verwijderen die al aangeboden is ook al hoor ik dit niet te kunnen.

Om deze lek te verifiëren moet u eerst ingelogd zijn met firefox en 1 advertentie hebben die aangeboden is.

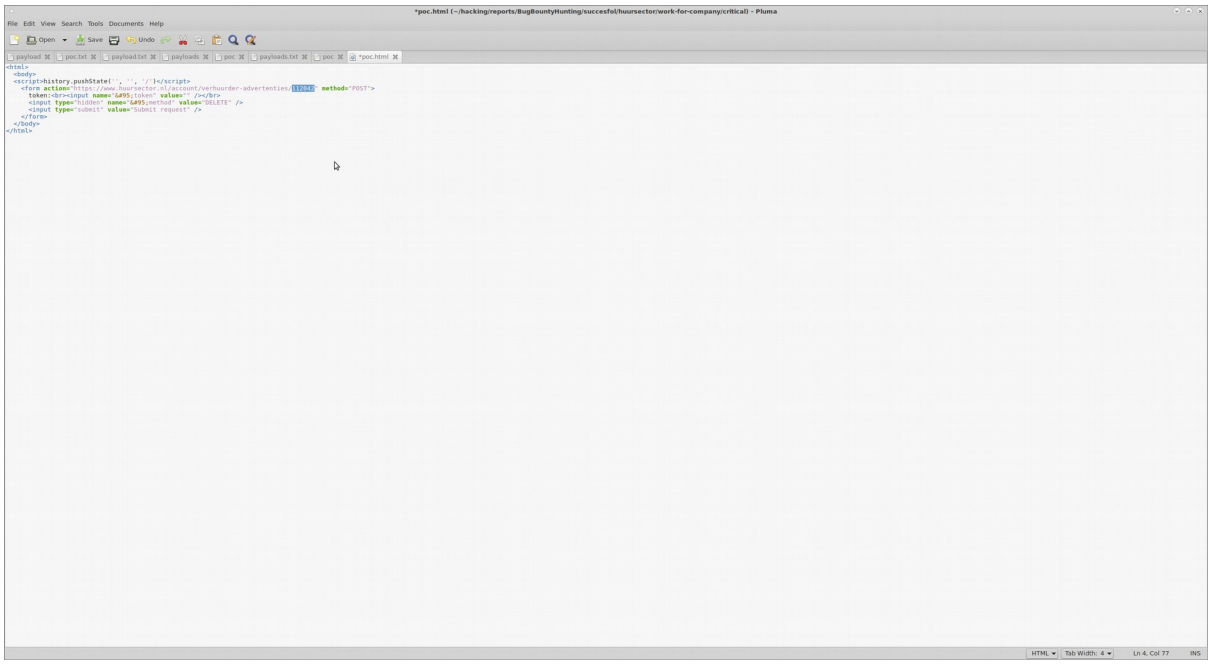


Nu open de aangeboden woning en kopieer het advertentienummer in de url en sla het ergens op.

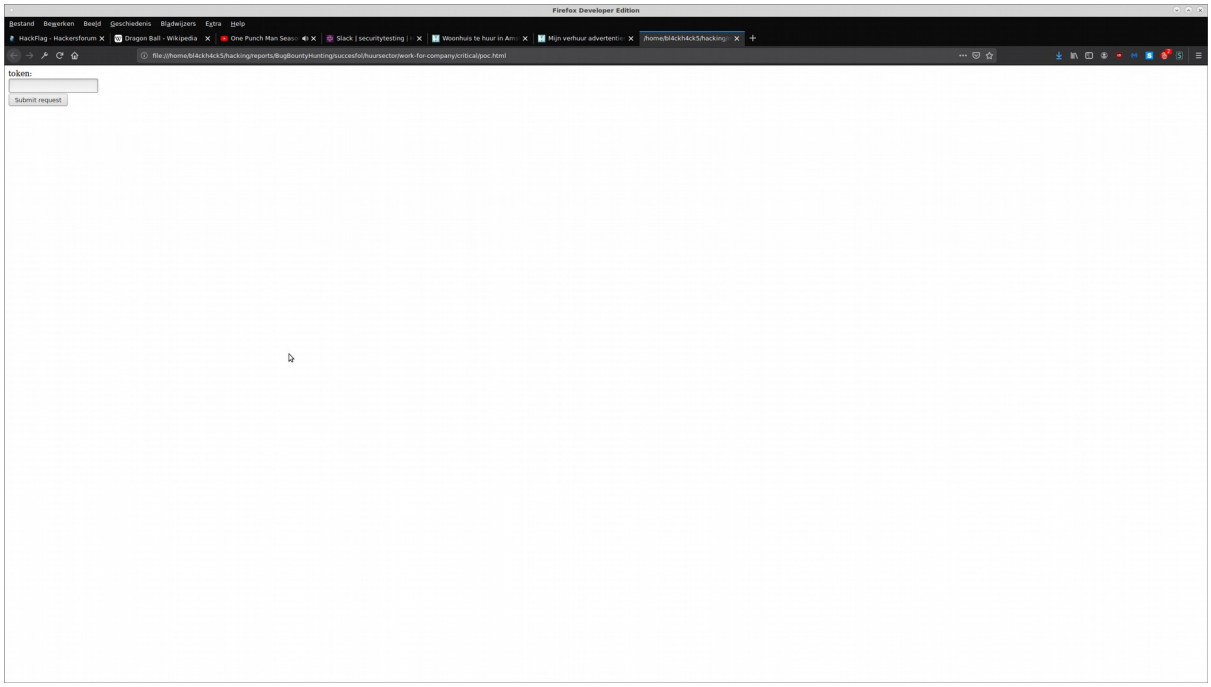


Nu maak een html file met de code hieronder en verander de 112042 naar het advertentienummer dat we net opsloegen en sla de html file op.

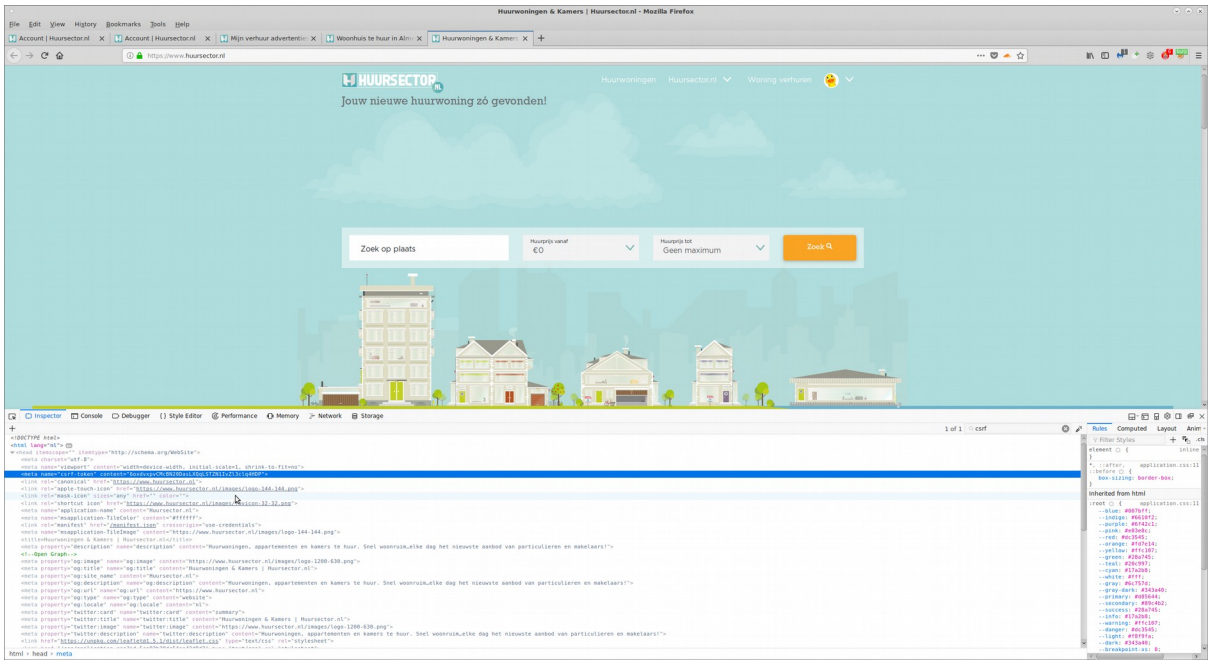
```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.huursector.nl/account/verhuurder-advertenties/
112042" method="POST">
      token:<br><input name="&#95;token" value="" /></br>
      <input type="hidden" name="&#95;method" value="DELETE" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



Nu open de html file in een nieuwe tab en je zult een veld zien met een knop.

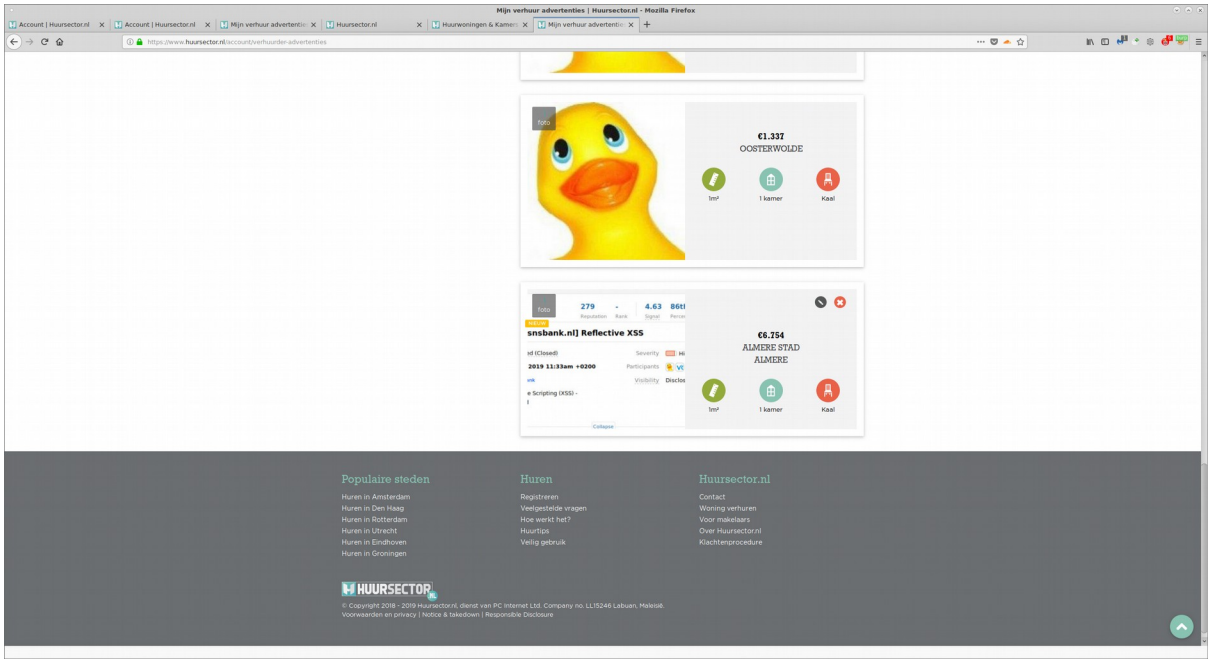


Open nu nog een nieuwe tab en ga naar de webpagina https://www.huursector.nl.
Open daar elemental inspect en zoek voor een meta tag genoemd csrf-token.
kopieer wat er tussen content staat en plak dat in de html files veld.

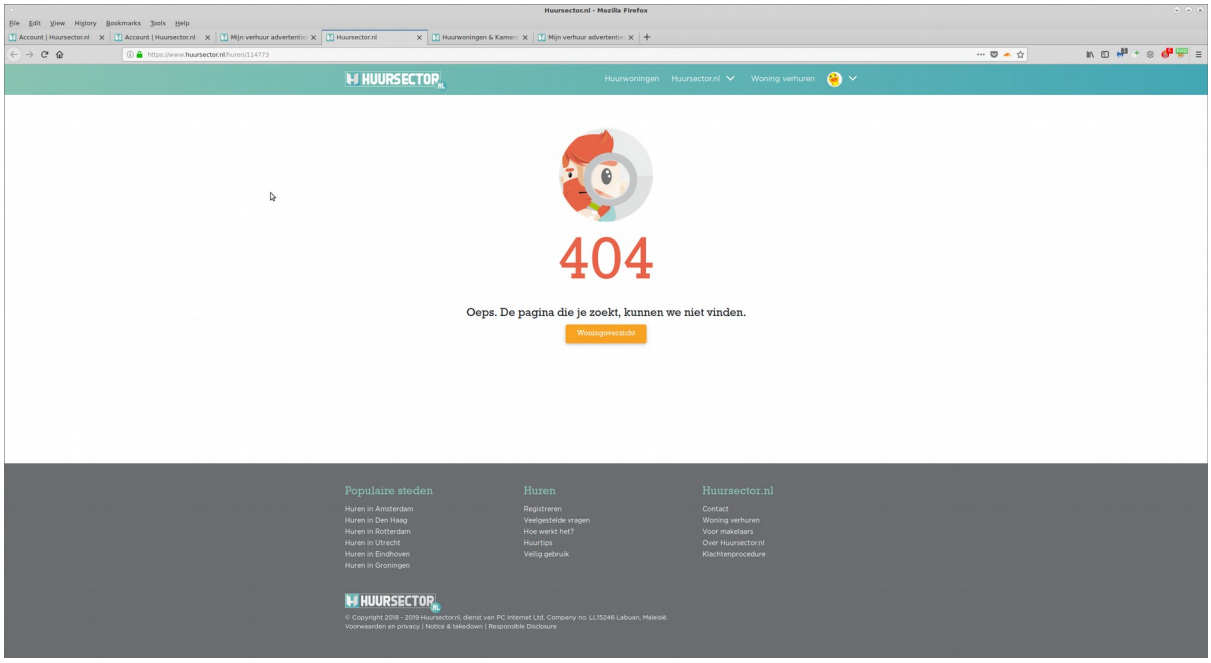

Huurwoningen & Kamers | Huursector.nl - Mozilla Firefox
HUURSECTOR
Jouw nieuwe huurwoning zó gevonden!
Zoek op plaats
Zoek


Firefox Developer Edition
token:
Submit request

Druk nu op submit.
Je komt nu terug op de mijn advertentie pagina en je zult snel merken dat de aangeboden woning weg is.
Als dat niet is gebeurt dan is er iets fout gegaan en is het mogelijk mislukt.



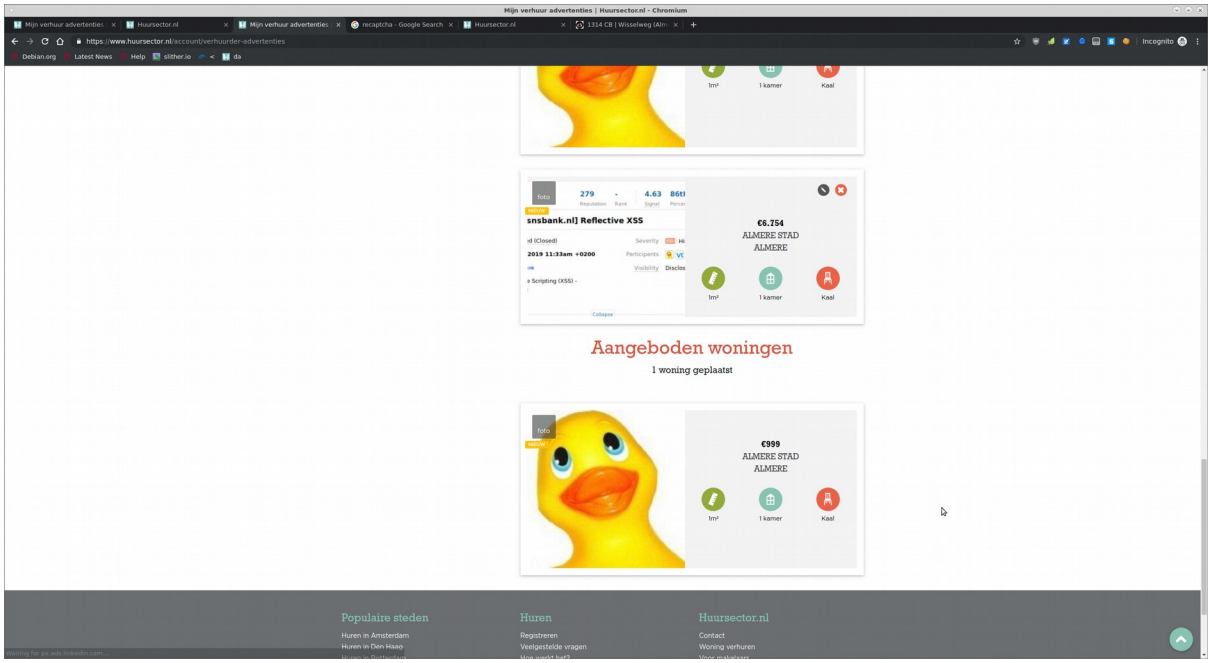
Als je nu terug gaat naar de advertentie die je wilden verwijderen zul je merken dat deze weg is.



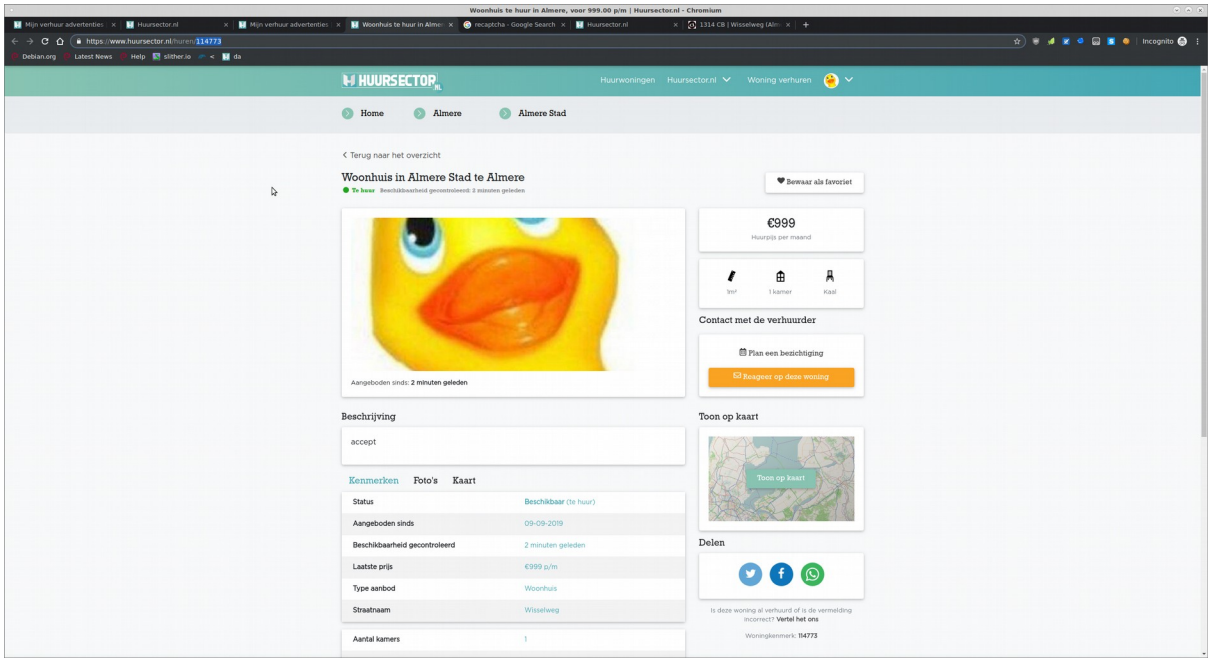
2.2. Insecure direct object reference in bewerken leidt tot verwijdering van al aangeboden advertentie.

Tijdens mijn onderzoeken op 9 September kwam ik er achter dat als je 2 advertenties aanmaakt waar een is al aangeboden en de andere staat in de wacht dat het mogelijk is om de aangeboden advertentie te verwijderen door de nog niet goedgekeurde advertentie te bewerken en als je op de bewerk pagina komt in de url het advertentienummer te vervangen met een advertentie van een al goedgekeurde advertentie.
En als je het dan opslaat wordt de aangeboden woning verwijdert.

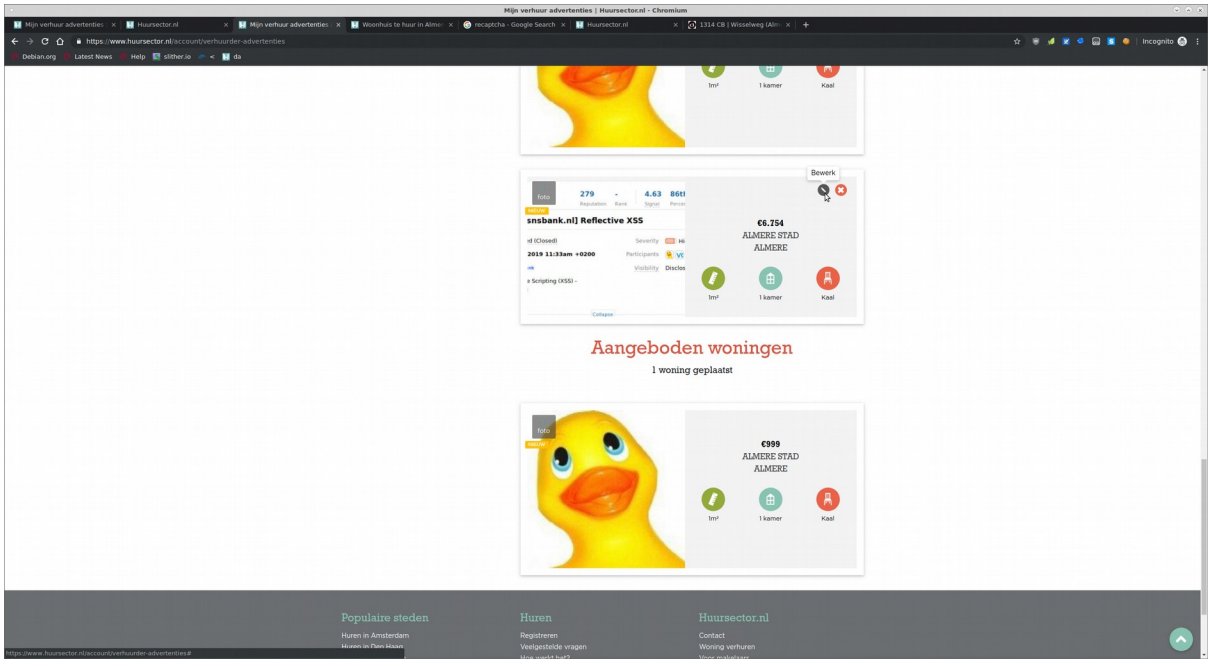
Om deze lek te verifiëren moet je 1 premium account hebben waar je 1 aangeboden woning hebt en een woning die in de wacht zit.



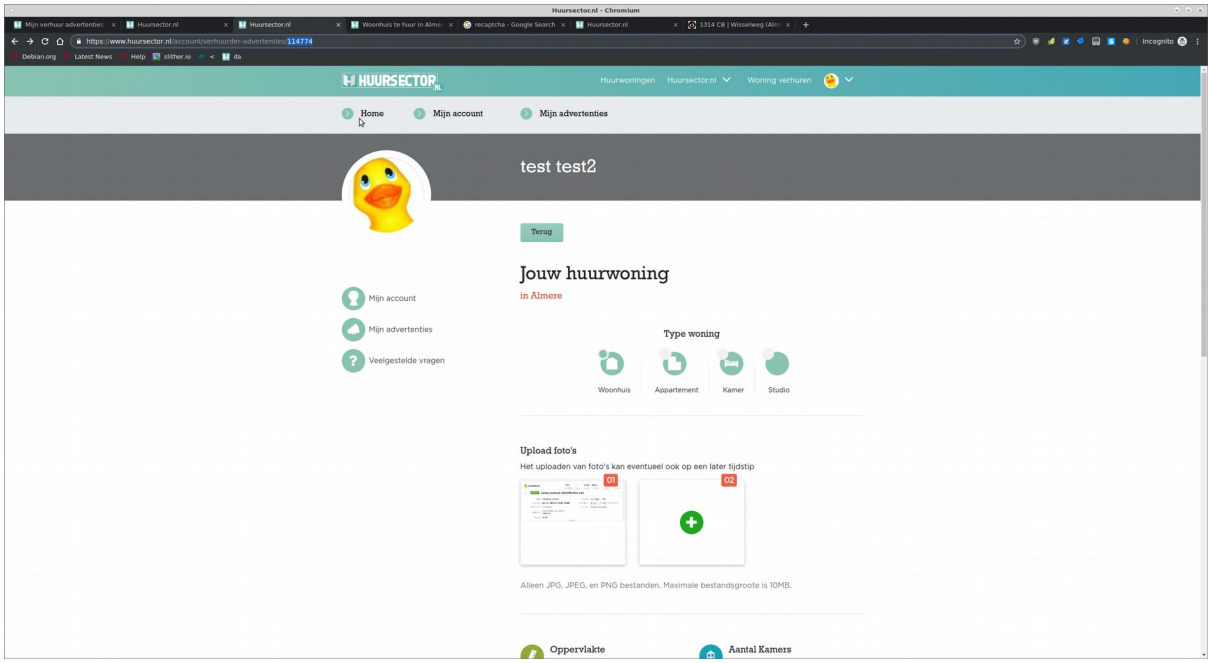
Open nu de aangeboden woning en kopieer het advertentienummer in de url en sla dat ergens op.

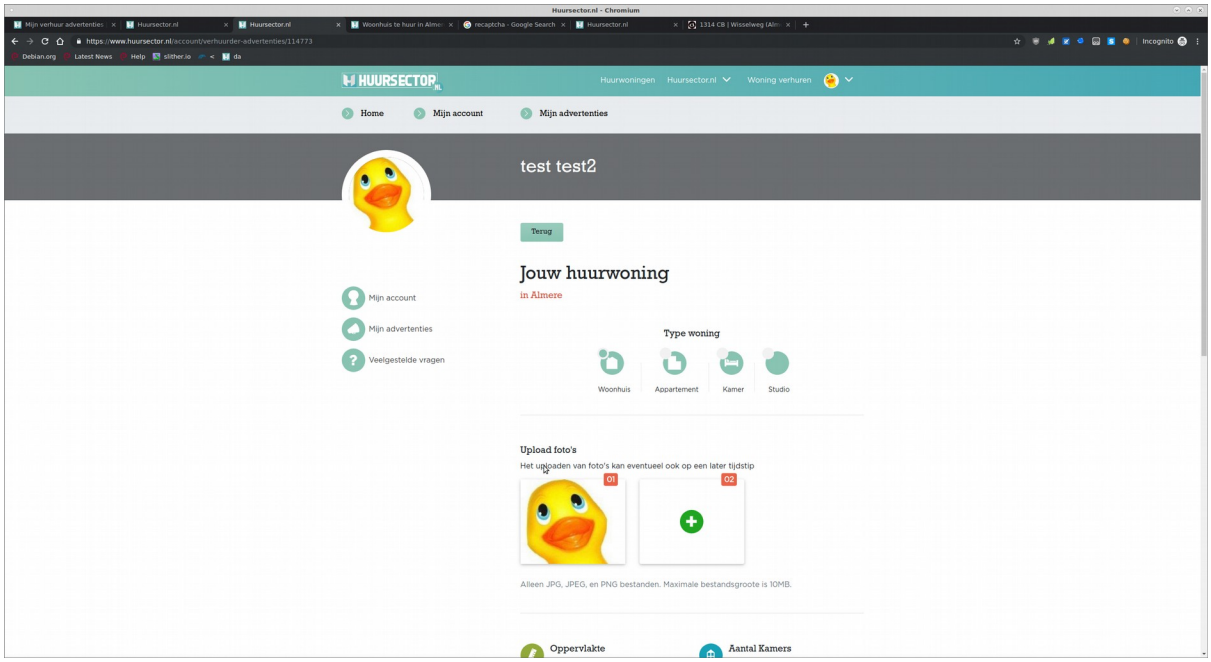


Nu ga terug naar de de mijn advertentie webpagina en druk op bewerk bij de nog goed te keuren woning.

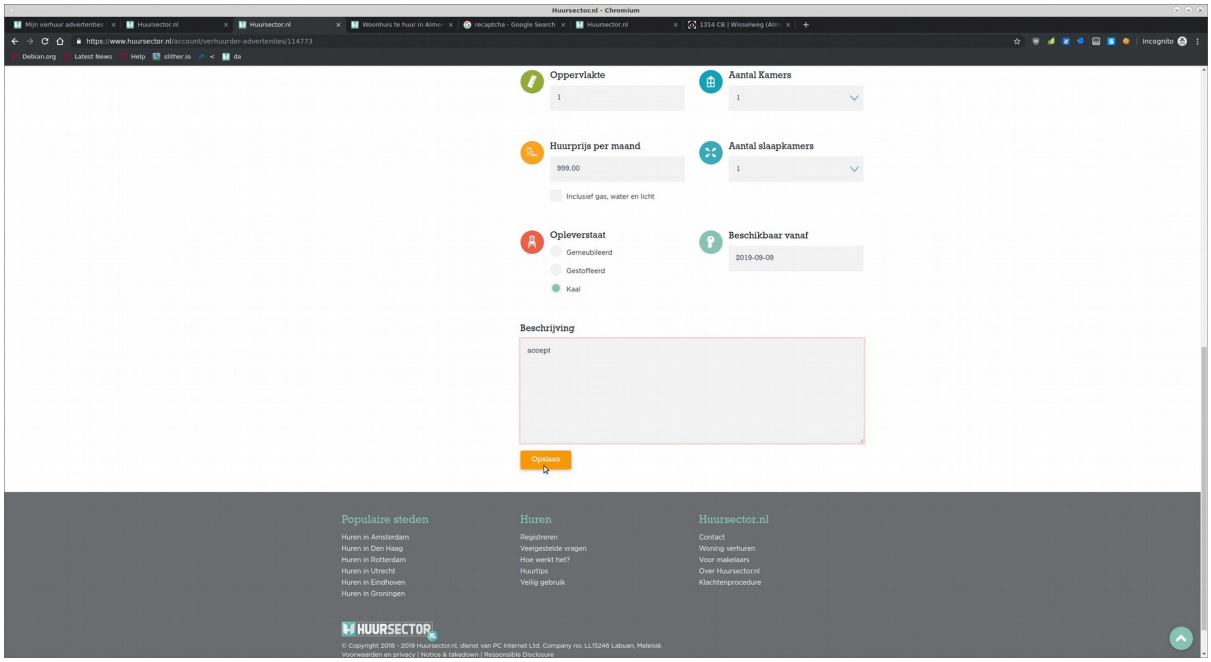


Nu bij de bewerk pagina verander het advertentienummer in de url naar het advertentienummer dat we net opsloegen en druk op enter.
Je zult al snel merken dat de foto verandert.

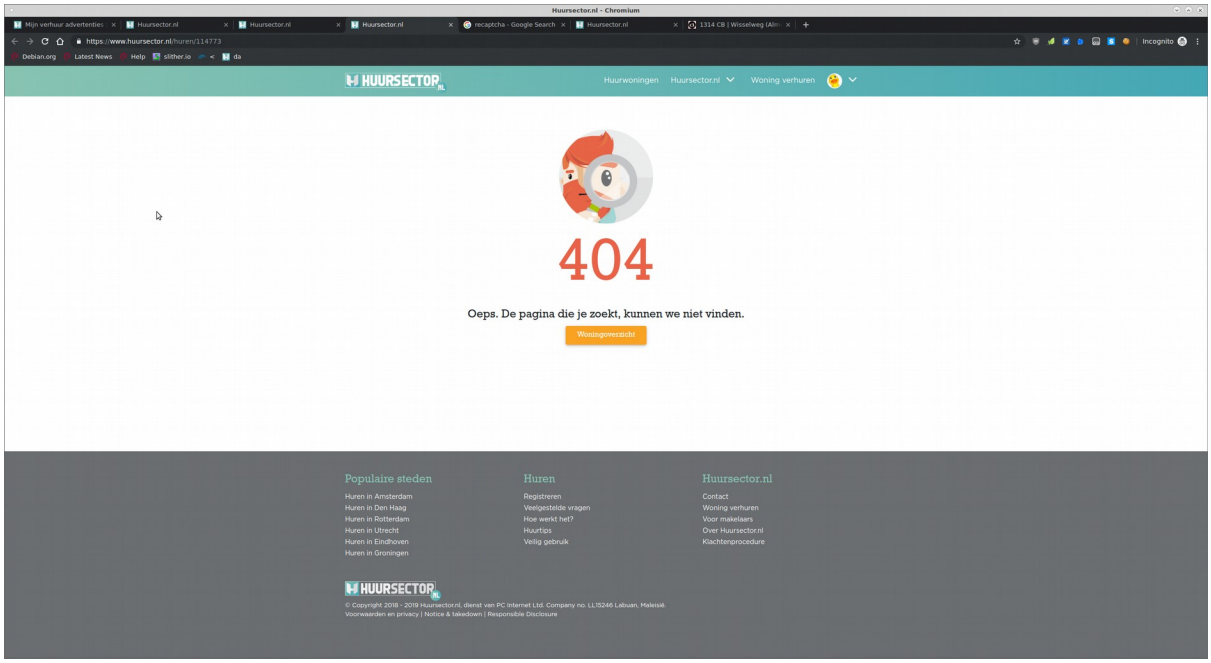




Nu ga helemaal naar beneden en druk op opslaan.



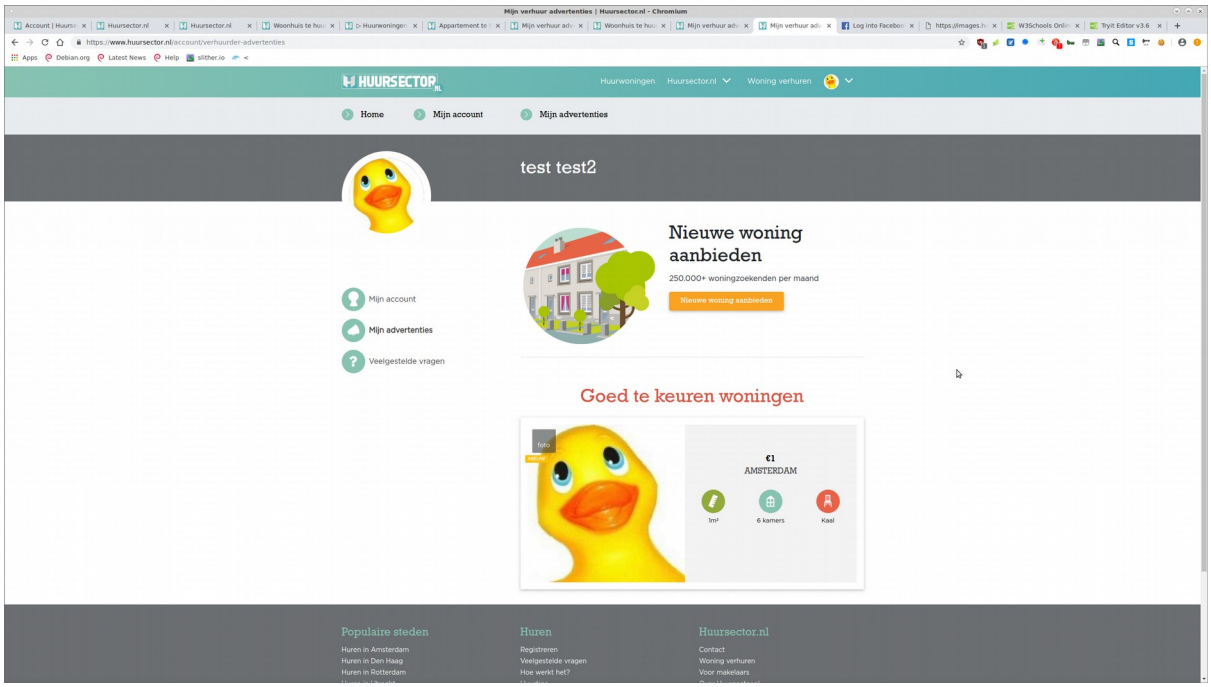
Je wordt nu helemaal naar boven gescrolled.
Als je nu terug gaat naar de aangeboden advertentie merk je dat deze advertentie nu weg is.



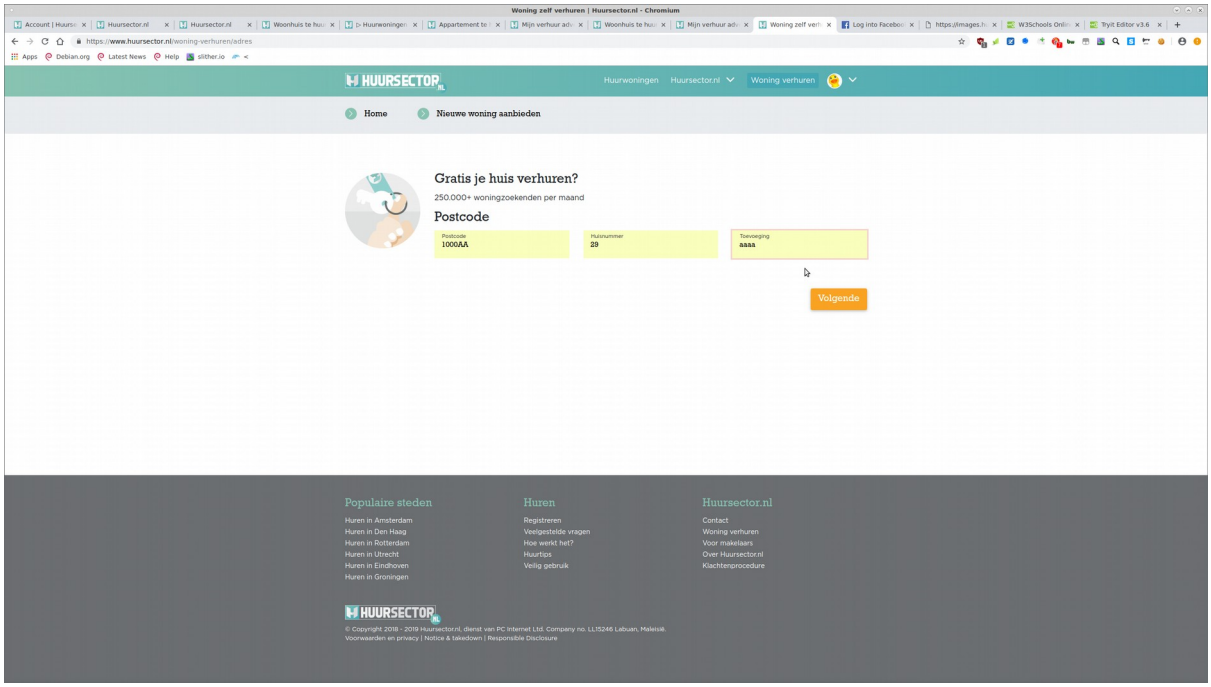
2.3. Stored cross site scripting door middel van het bewerken van een woning voordat het geaccepteerd is.

Tijdens mijn onderzoeken op 1 September kwam ik er achter dat als je een nieuwe woning aanbiedt met een premium account en tijdens de woning in de acceptatie fase zit bewerkt. Dan krijg je stored xss als je een script tag stuurt in de Beschrijving wanneer je het bewerkt.

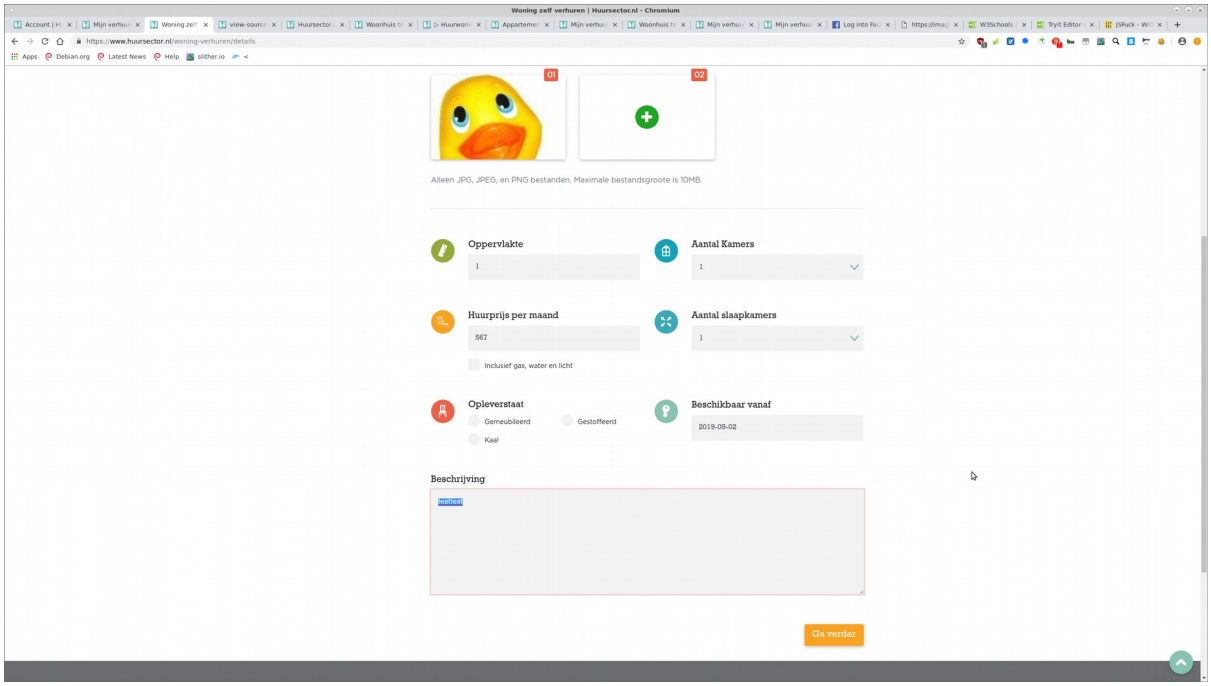
Om deze lek te verifiëren moet u eerst ingelogd zijn met een premium users en naar de webpagina https://www.huursector.nl/account/verhuurder-advertenties gaan.



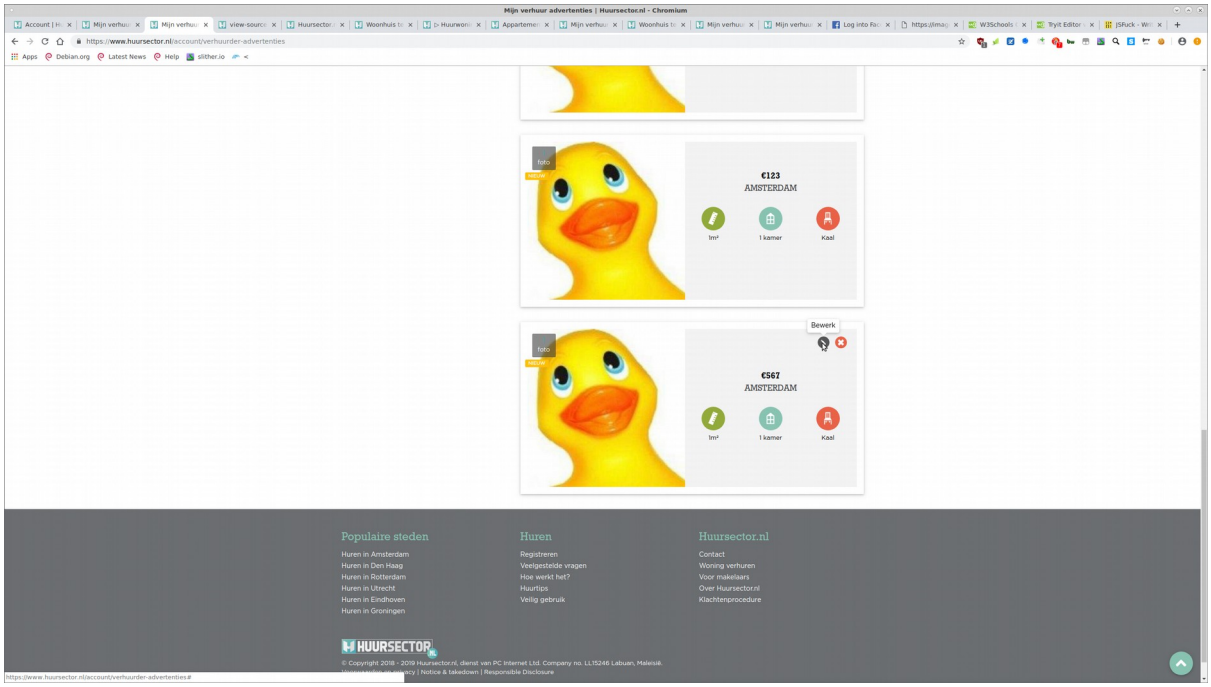
Nadat u op deze webpagina bent gekomen drukt u op “Nieuwe woning aanbieden”.
Je zult nu een echt postcode in moeten voeren. (in deze POC gebruik ik 1000AA met huisnummer 29)



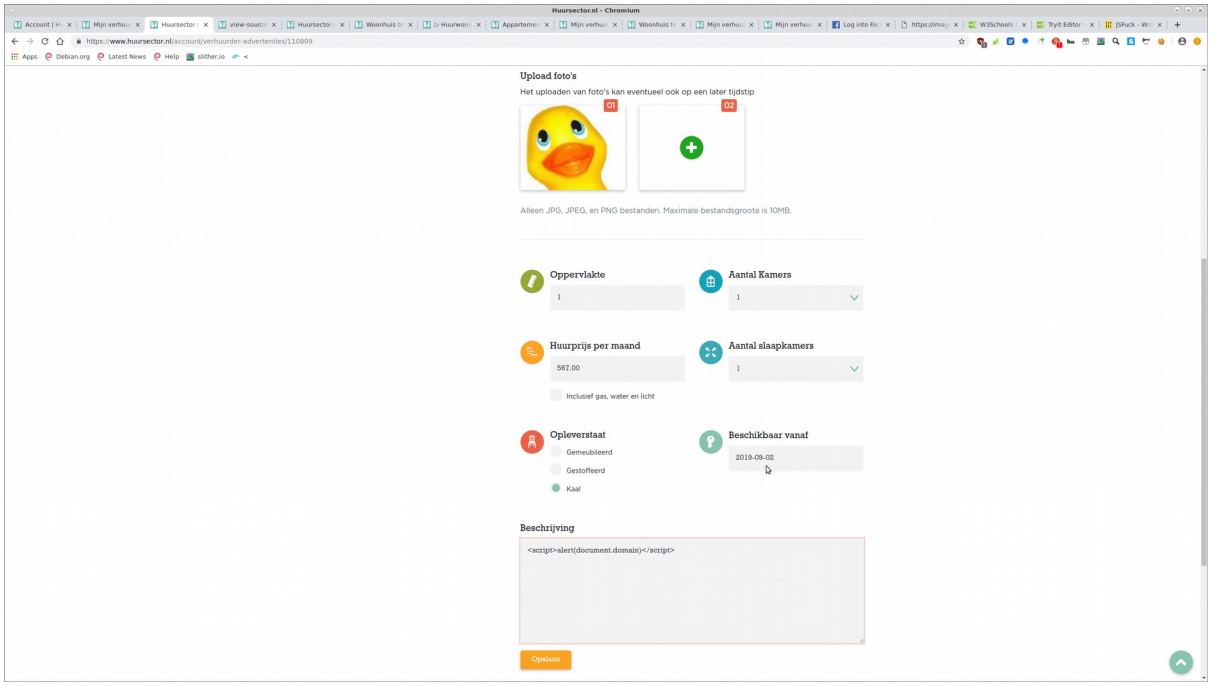
je zult nu op een nieuwe pagina komen; geef daar een foto open en vul alle velden in.



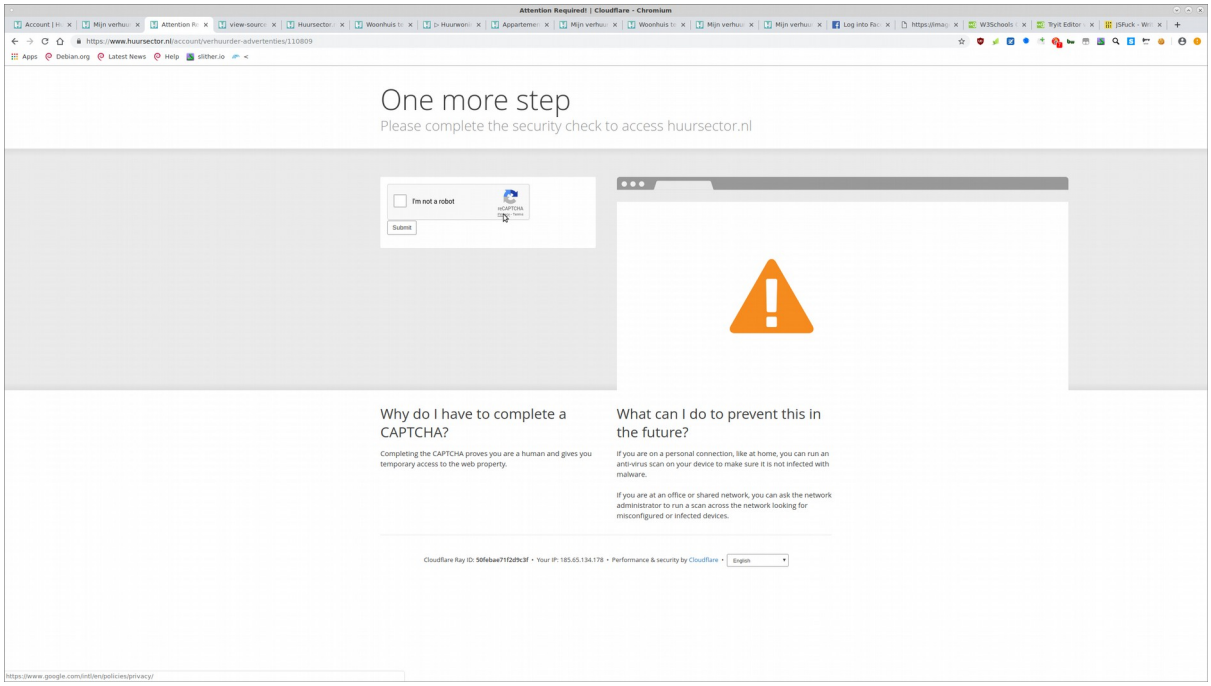
Als u nu op “Ga veder” drukt moet u daarna terug naar de webpagina https://www.huursector.nl/account/verhuurder-advertenties.
Daar gaat u naar uw advertentie die nog niet goedgekeurd is en drukt u op “Bewerk”.



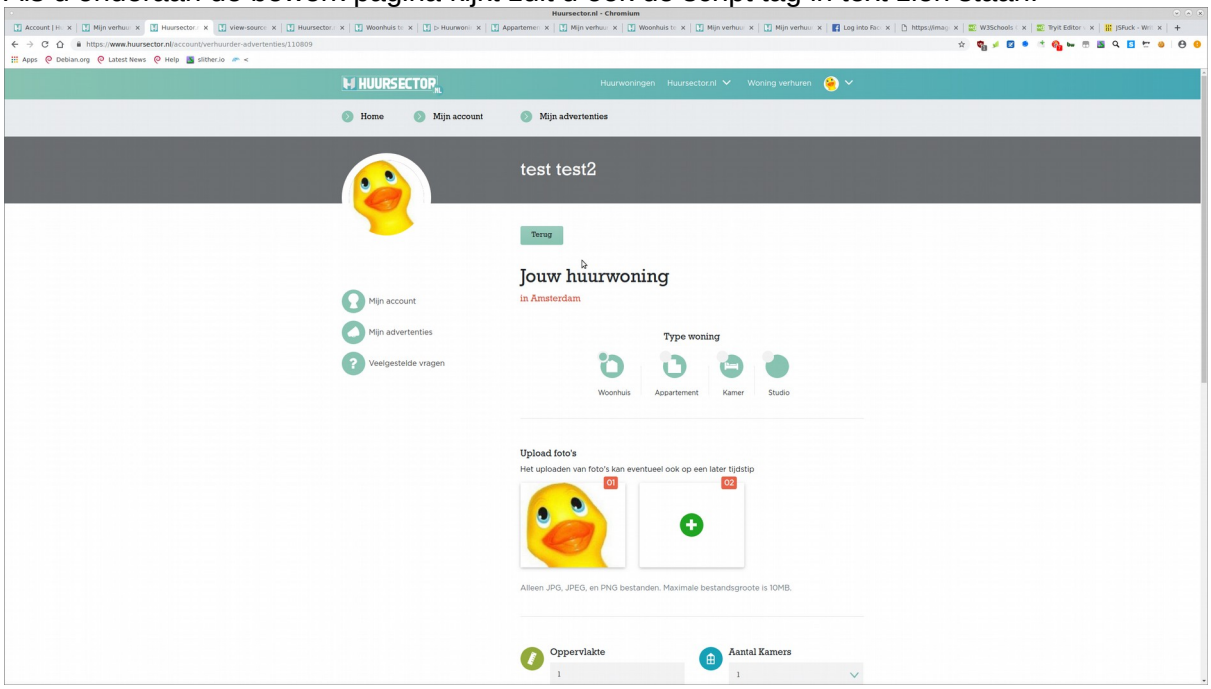
Nu plaats in de Beschrijving een html tag (ik gebruik script tag voor deze poc) en druk op opslaan.



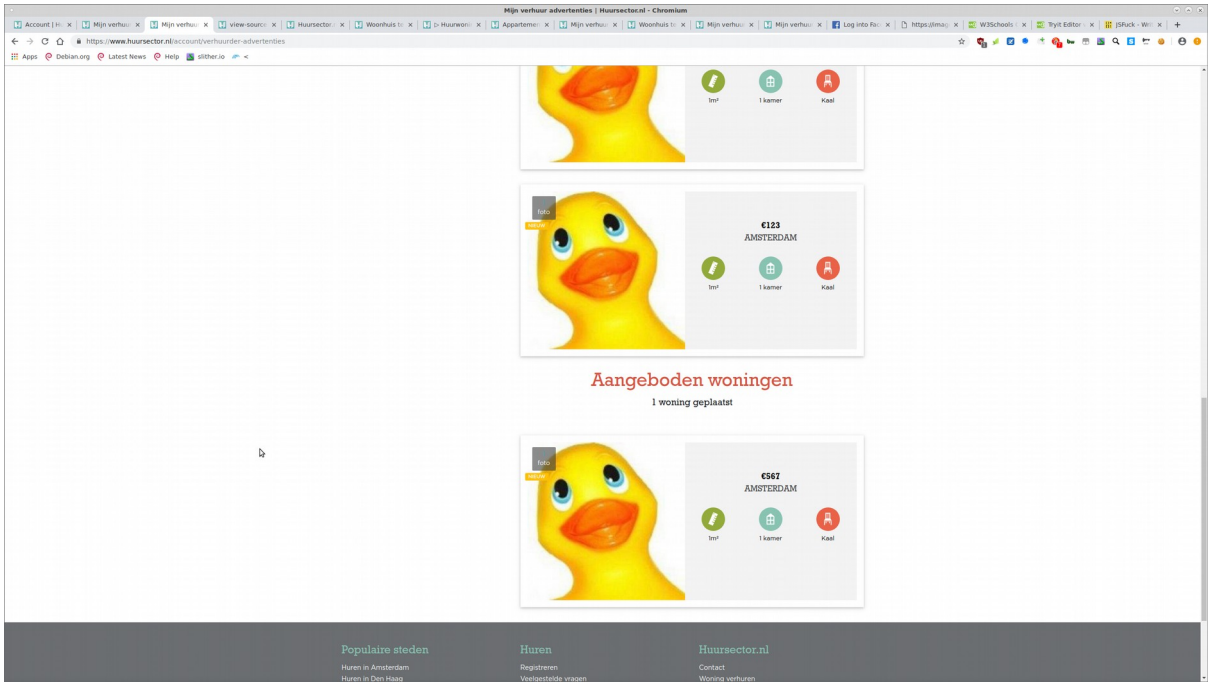
Er is een kans dat uw firewall een waarschuwing geeft; voer de recaptcha in. (als er een blokkade komt gebruik dan een html tag die minder gevaarlijk is zoals een B tag)



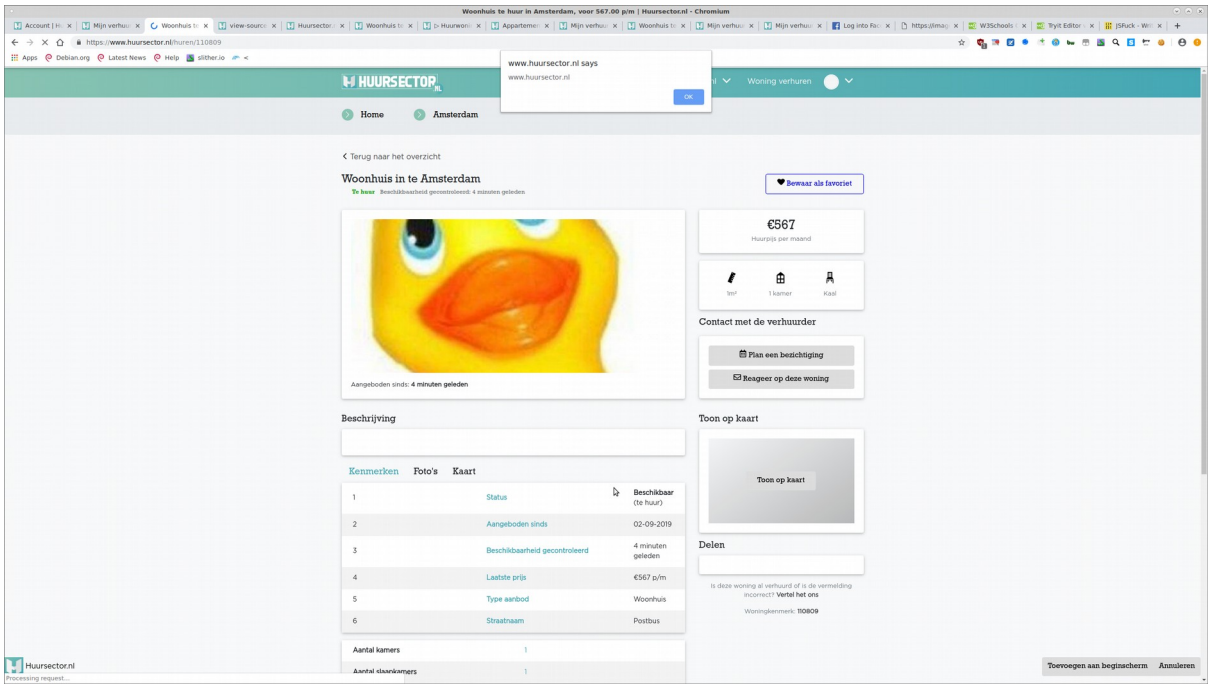
als u deze captcha heeft ingevoerd komt u terug in uw advertentie die u aan het bewerken bent.
Als u onderaan de bewerk pagina kijkt zult u ook de script tag in text zien staan.



U kunt nu op “Mijn advertenties” drukken.
Wanneer deze advertentie dan wordt geaccepteerd (raad aan dat jullie hem accepteren) komt deze in de aangeboden woningen te staan.



Druk nu op uw nieuwe advertentie.
Wanneer u nu op uw nieuwe advertentie komt zult u merken dat de html tag afgaat in de beschrijving.
Omdat ik een script tag met een alert(document.domain) gebruikten gaat deze bij mij af.



Wat ik wel merkten is dat deze lek alleen werkt op premium accounten, dus als u naar dezelfde advertentie gaat met een gratis account gaat deze html tag niet af maar wel met alle premium accounten.
Dit kan dus een zeer goede targeted aanval zijn op premium gebruikers en als ze alleen naar de advertentie gaan wordt hun hele account overgenomen.
Als bewijs laat ik alleen een simpele javascript popup zien maar javascript kan makkelijk de hele account overnemen zonder dat de gebruiker het merkt.

3. Gemiddelde prioriteit.

3.1. 2 reflective xss’en in de facebook autorisatie en google autorisatie doormiddel van malformed url.

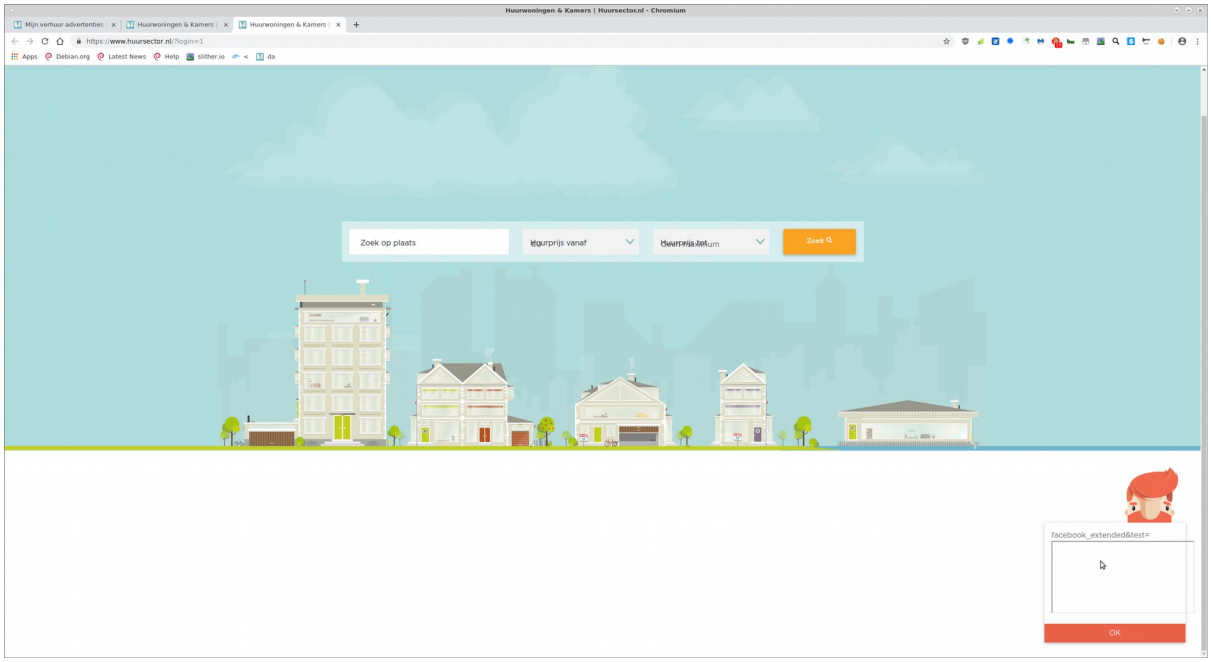
Tijdens mijn onderzoeken op 9 September kwam ik er achter dat als je een malformed url meestuurt in de url van de google of facebook autorisatie dat het mogelijk is om reflective xss te krijgen in het error bericht op https://www.huursector.nl.

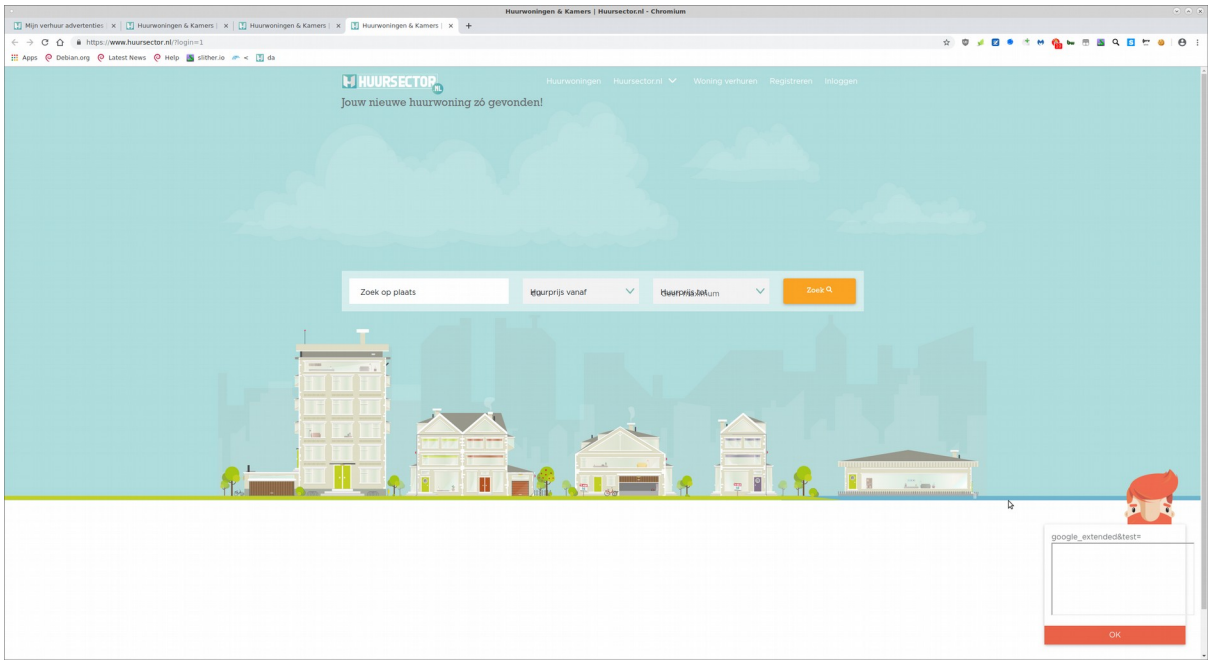
Om deze lek te verifiëren hoeft u alleen naar een van deze 2 webpagina’s te gaan met een niet ingelogde account.

https://www.huursector.nl/inloggen/google_extended&test=%3Ciframe%3E

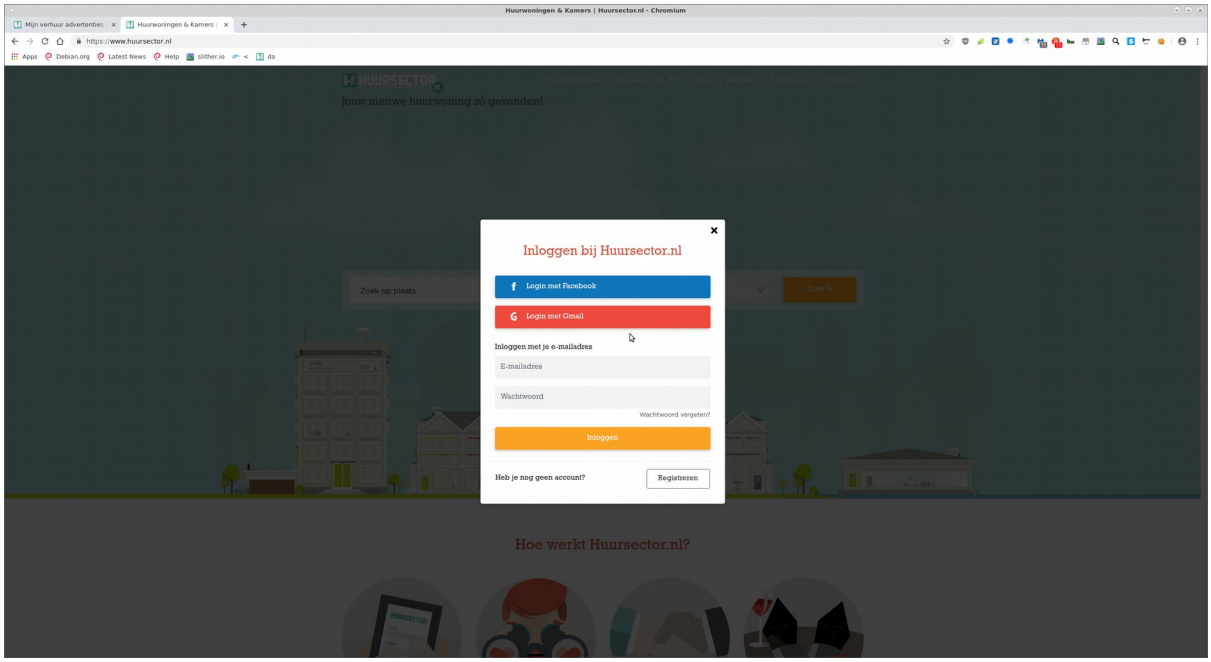
https://www.huursector.nl/inloggen/facebook_extended&test=%3Ciframe%3E

als u op deze webpagina komt wordt je geredirect naar de hoofdpagina en zie je een nieuwe iframe.

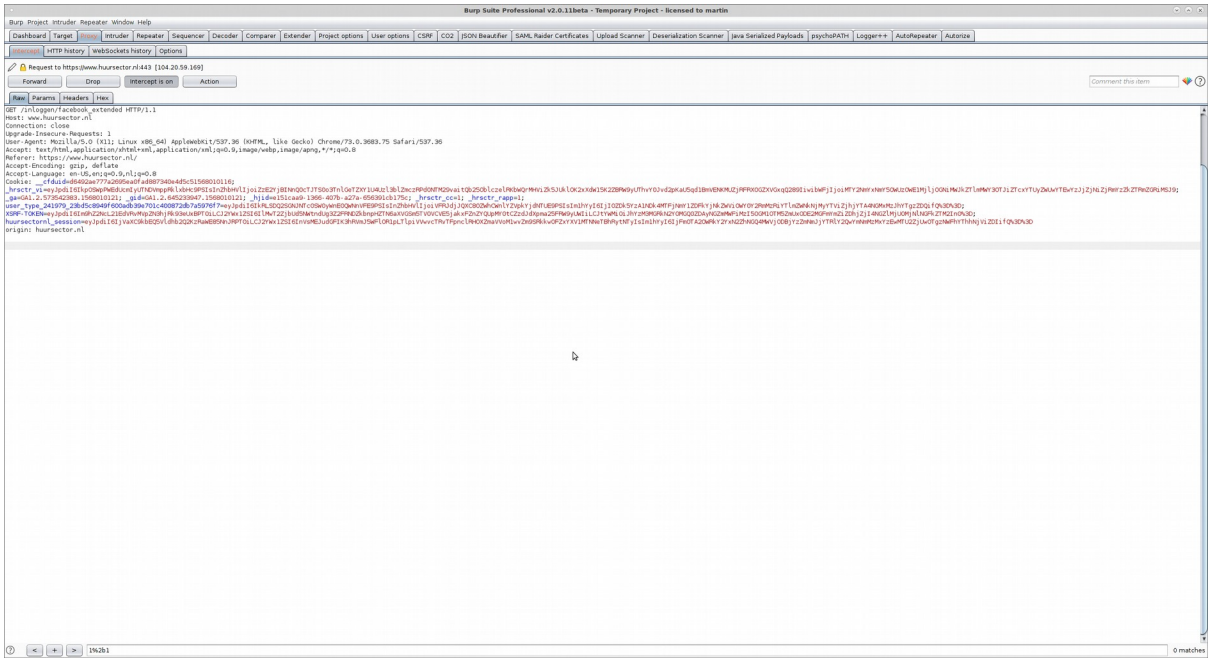




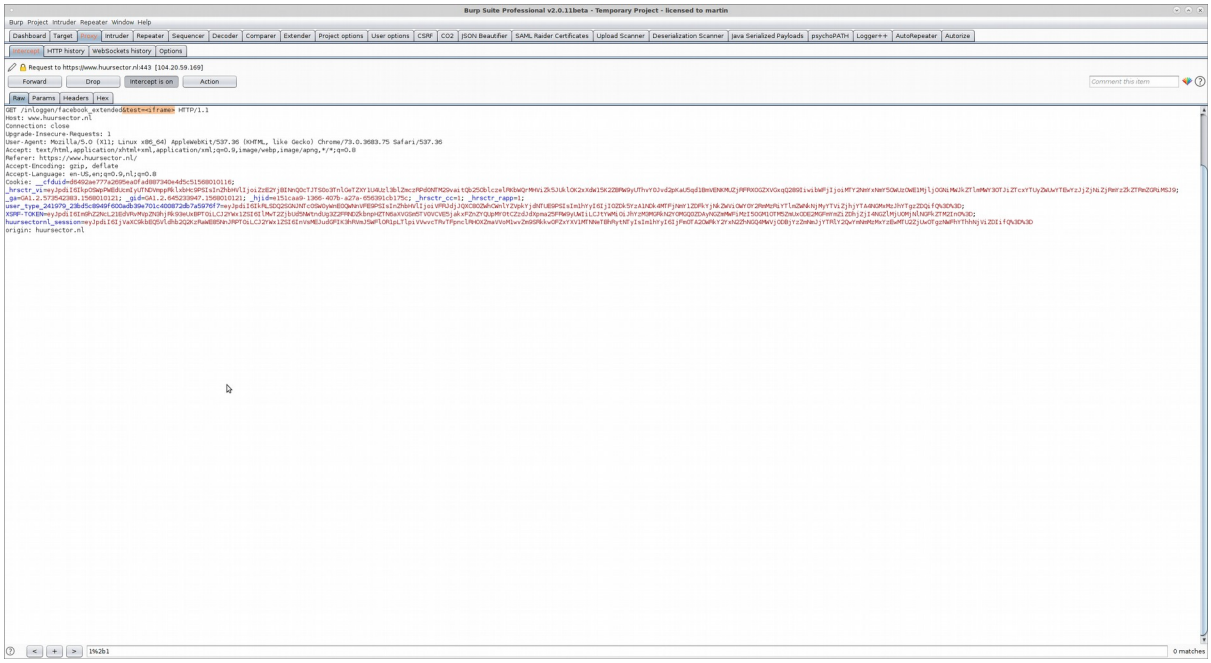
Als we kijken met een interceptie tool kunnen we zien wat er gebreurt (ik gebruik burpsuite)
Wanneer je op de login pagina bent zul je 2 knoppen zien.
Een voor facebook login en de andere voor google login.

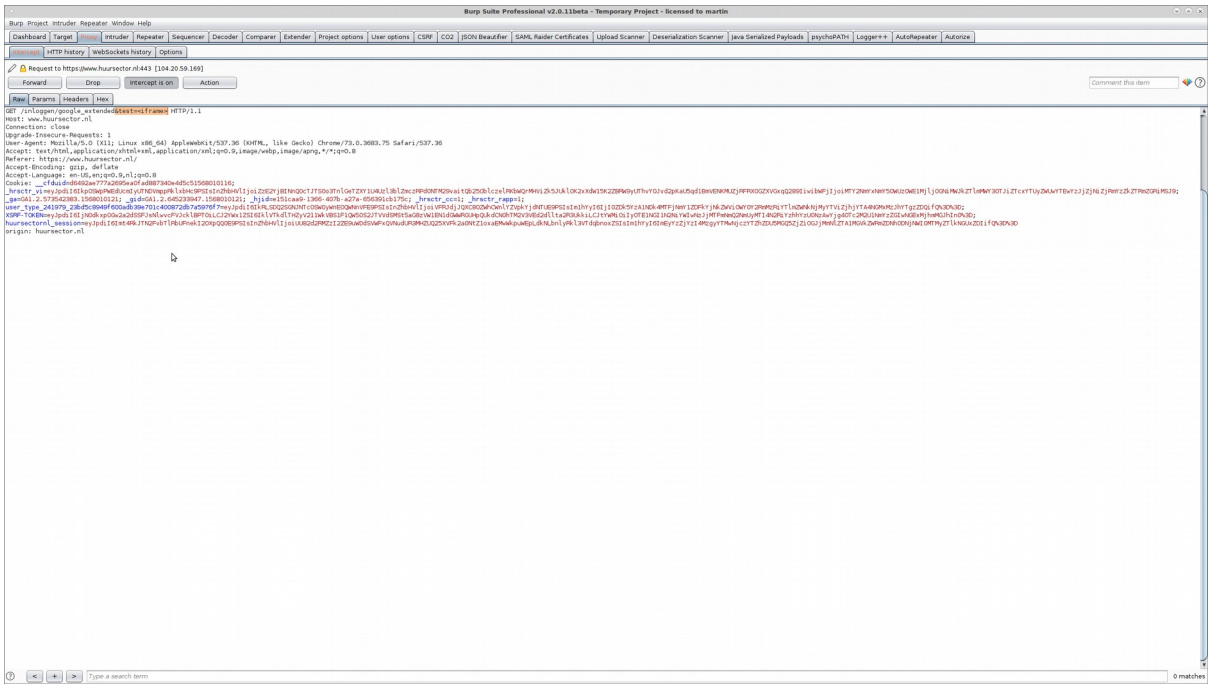


Als je op een van die knoppen drukt stuur je een request naar https://www.huursector.nl/inloggen/*******

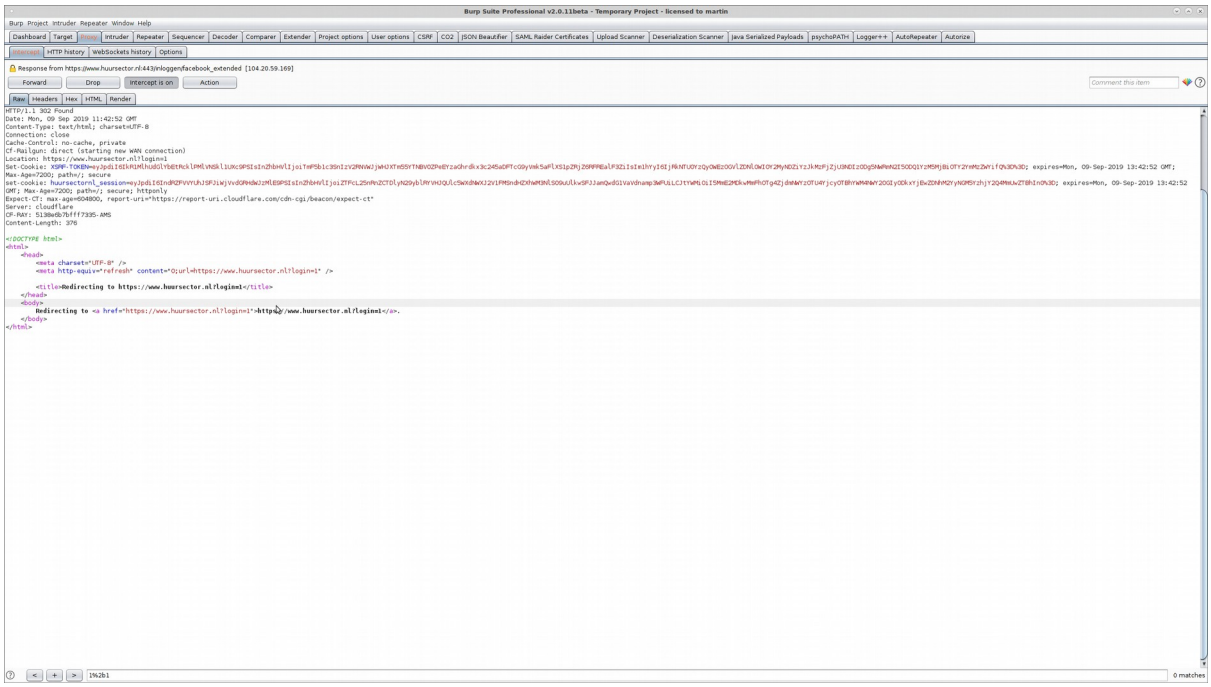


als je daar een malformed url meestuurt door in plaats van met een “?” een parameter te openen in het begin een “&” stuurt als eerste parameter dan veroorzaak je een reflective xss op de hoofdpagina.

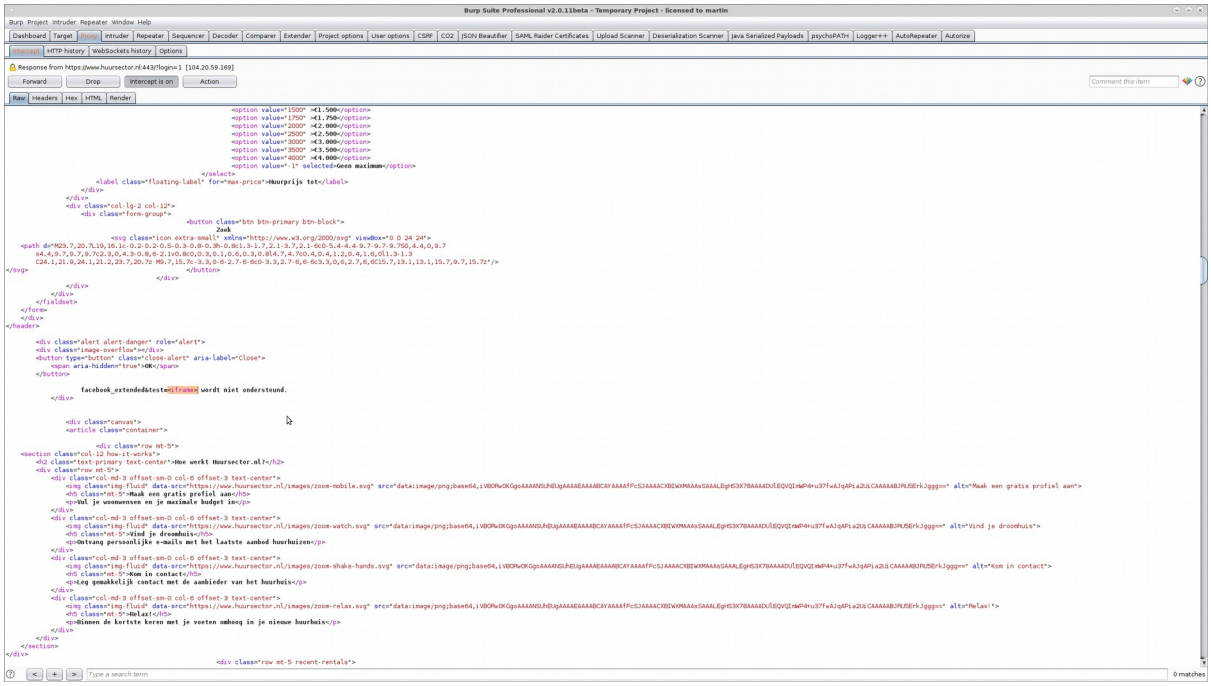




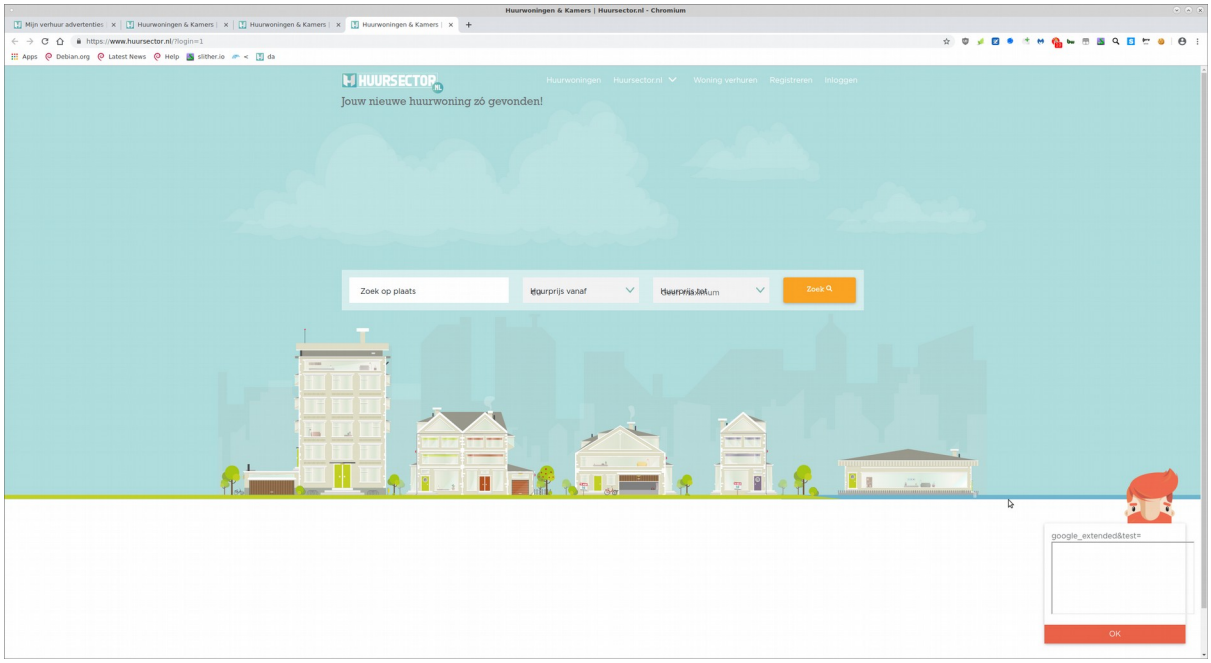
Je krijgt dan een redirect naar de hoofdpagina.



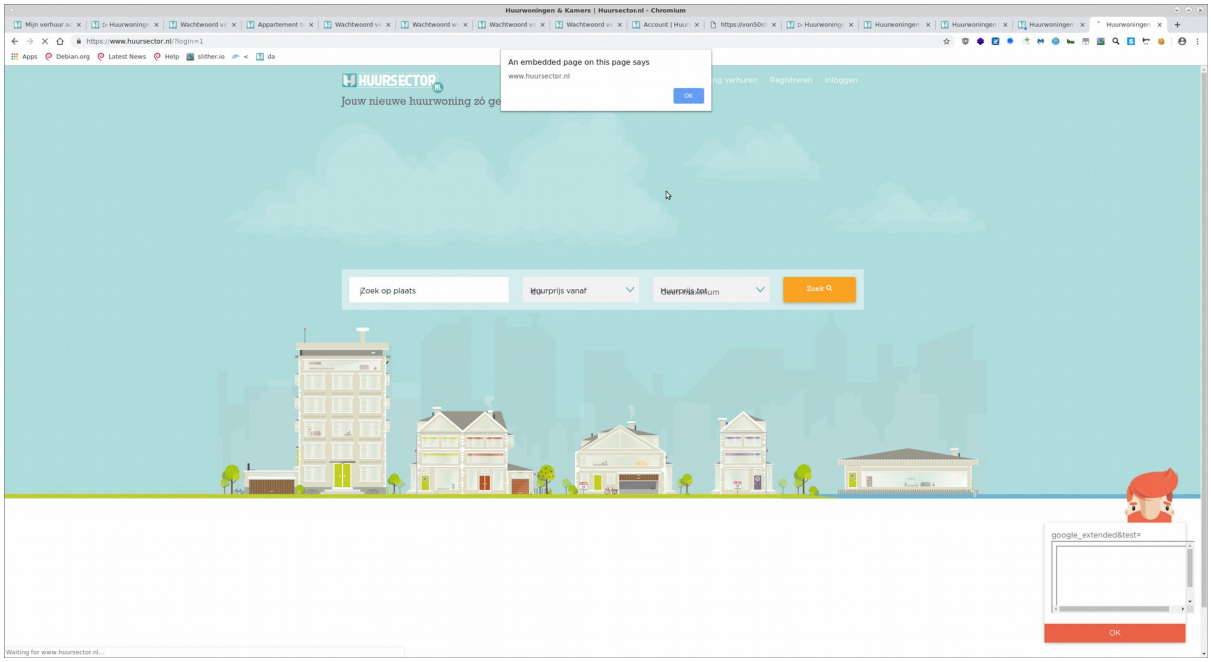
Als je die zou volgen en als je goed zoekt in het response dan zul je een nieuwe iframe tag zien staan in de “wordt niet ondersteund” veld.



Zou je dat zelfde request maken met een browser dan zul je merken dat er een nieuwe iframe op de webpagina staat.



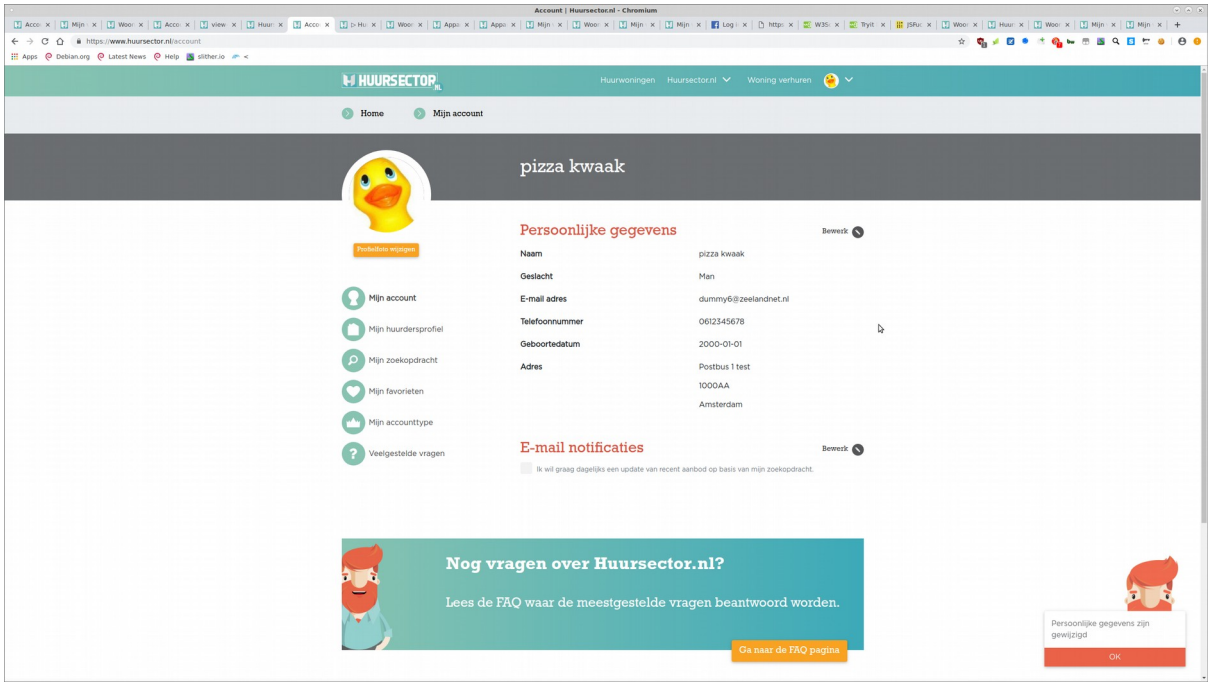
Als je meer tijd spendeert in de exploit dan kun je door een dubbele iframe te maken met een dubbele srcdoc event en dat allemaal html encode kun je de firewall bypassen en elk soort code sturen.
Als je wat extra css code meestuurt kun je deze iframe verbergen en als de user dan gaat inloggen kan de hacker de username en password stelen zonder dat de user het merkt.



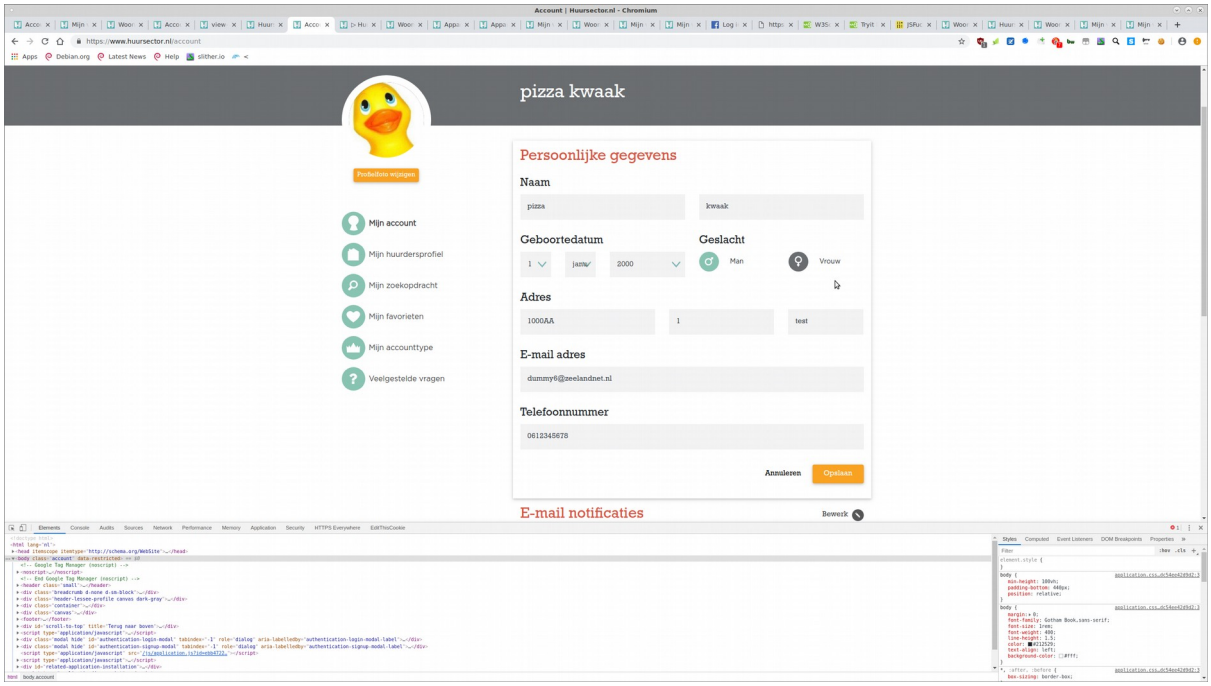
3.2. Bypass om een naam van een premium account aan te passen zonder dat de user dit hoort te kunnen.

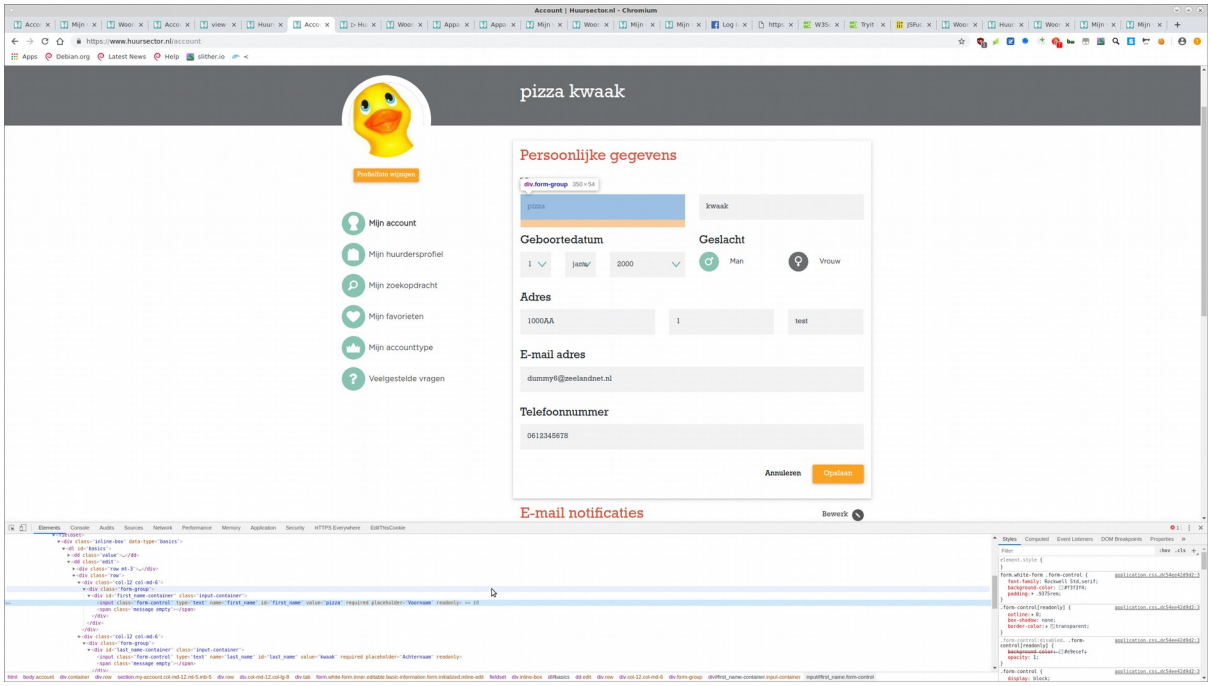
Tijdens mijn onderzoeken op 1 September kwam ik er achter dat als je de html code aanpast van de voor- of achternaam in de settings pagina van een premium user en verwijdert de “readonly” uit de code.
Dan is het mogelijk om de voor- en achternaam aan te kunnen passen ook al hoort een premium user dit recht niet te hebben.

Om deze lek te verifiëren moet u eerst ingelogd zijn met een premium users en naar de webpagina https://www.huursector.nl/account gaan.

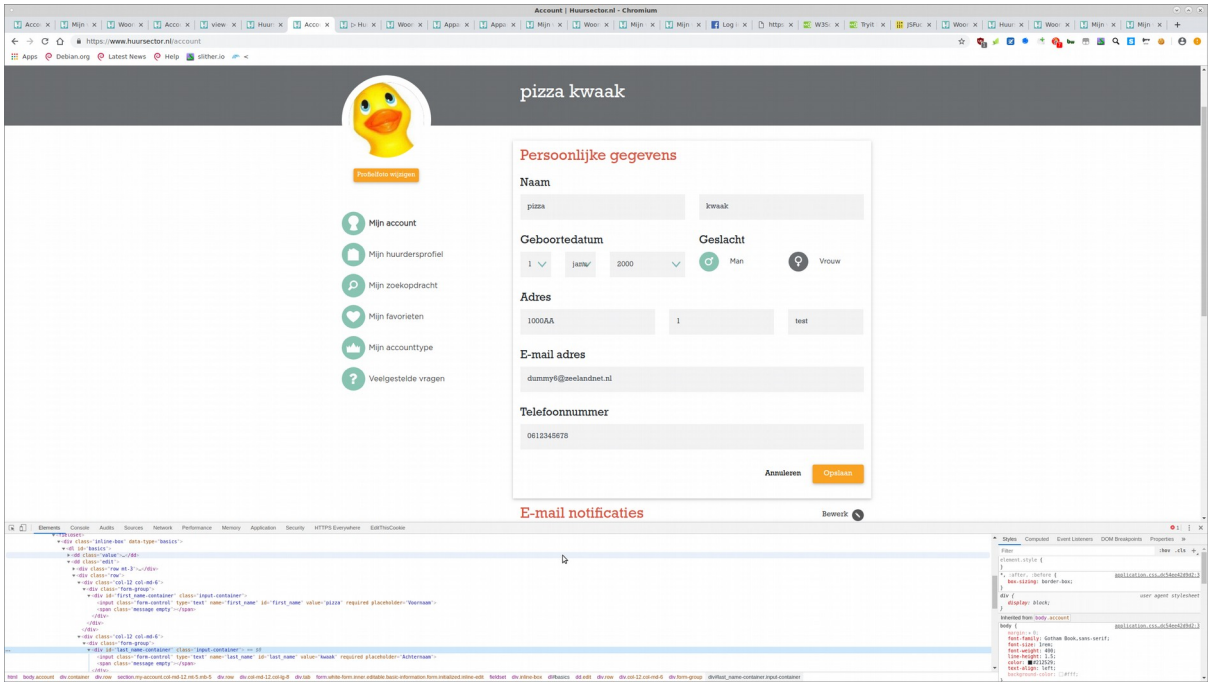


Daarna bij de 2 velden bij “Naam” open met elemental inspect de code waar de html tags “input” staan.

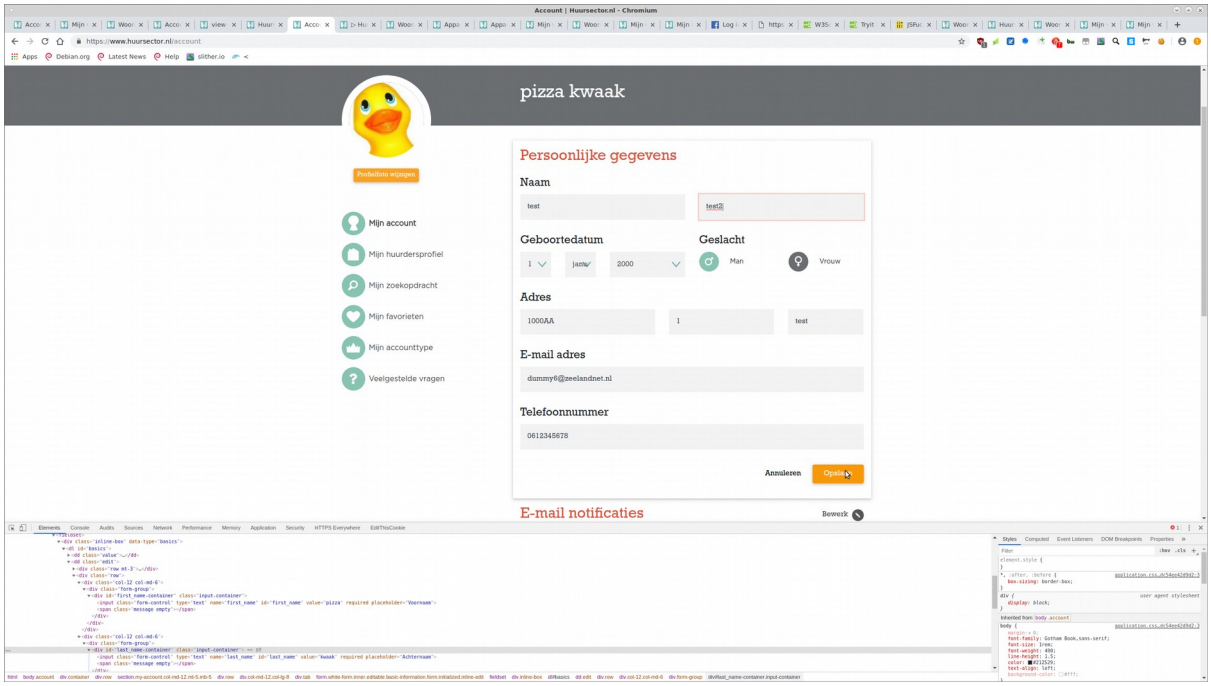




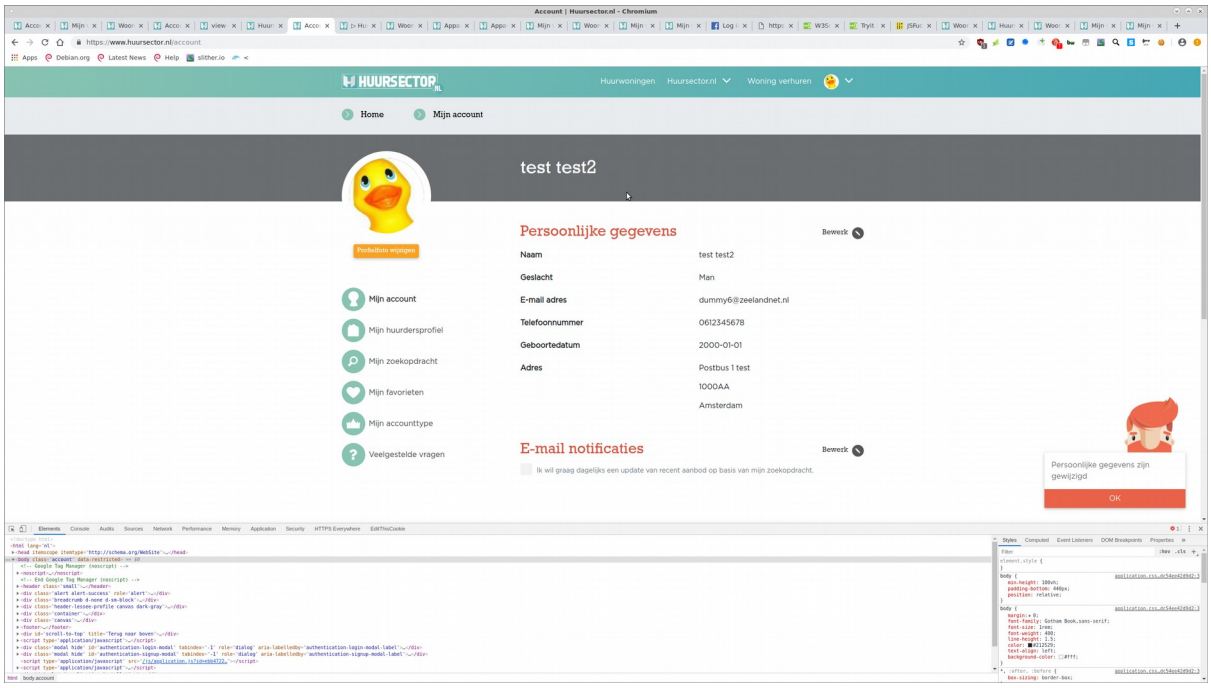
Daar in de code zult u bij beide “readonly” zien staan.
Verwijder die 2 texten uit de code en sla het op door naast de tags te drukken.



Nu kunt u bij de voor en achternaam de gegevens aanpassen.
Voor deze “proof of concept” gebruik ik als voornaam “test” en als achternaam “test2”.



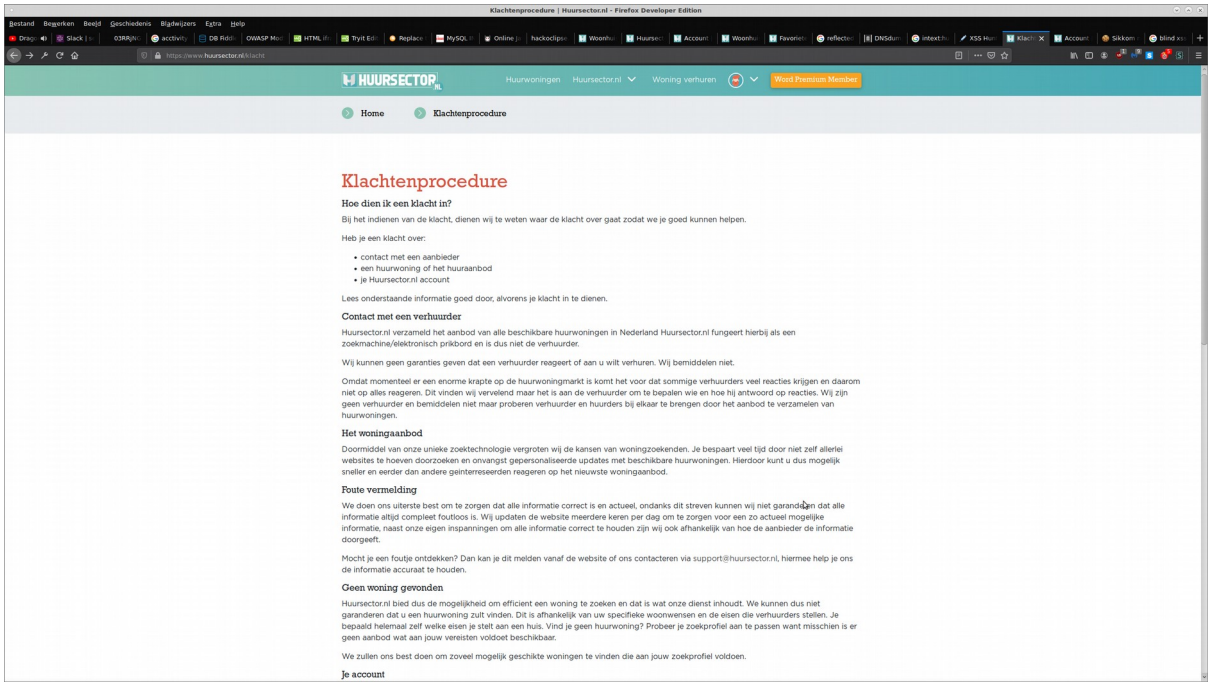
Als u nu op opslaan drukt zult u merken dat uw voor en achternaam zijn verandert.



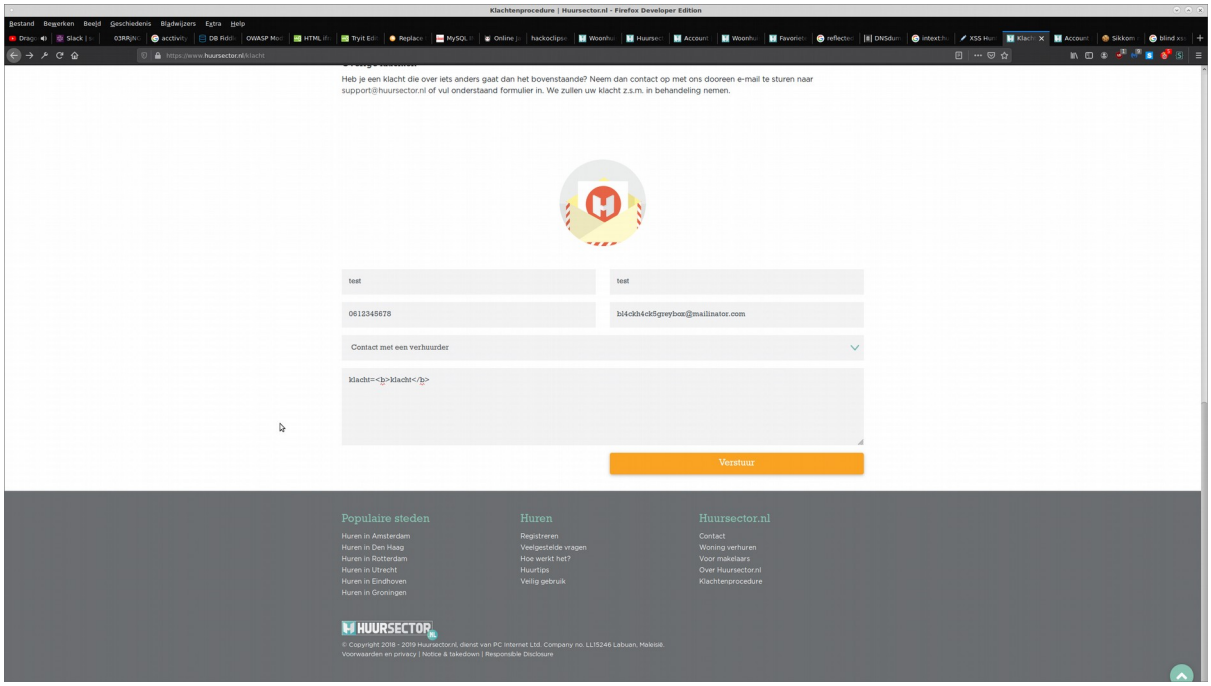
3.3. Klachten die worden ontvangen worden niet escaped voordat ze worden verstuurt.

Tijdens mijn onderzoeken op 1 September kwam ik samen met [redacted] er achter dat als u een klacht stuurt in het klachtenformulier op de webpagina https://www.huursector.nl/klacht dat deze klacht unescaped wordt verstuurt en als u code meestuurt in de klacht dat deze afgaat in [redacted] mail client.

Om deze lek te verifiëren moet u eerst naar de webpagina https://www.huursector.nl/klacht.



Daar scroll naar beneden en vul alle gegevens in.
Plaats in de klacht zelf een html tag (ik gebruik een B tag want die is niet geblokkeerd door uw firewall)



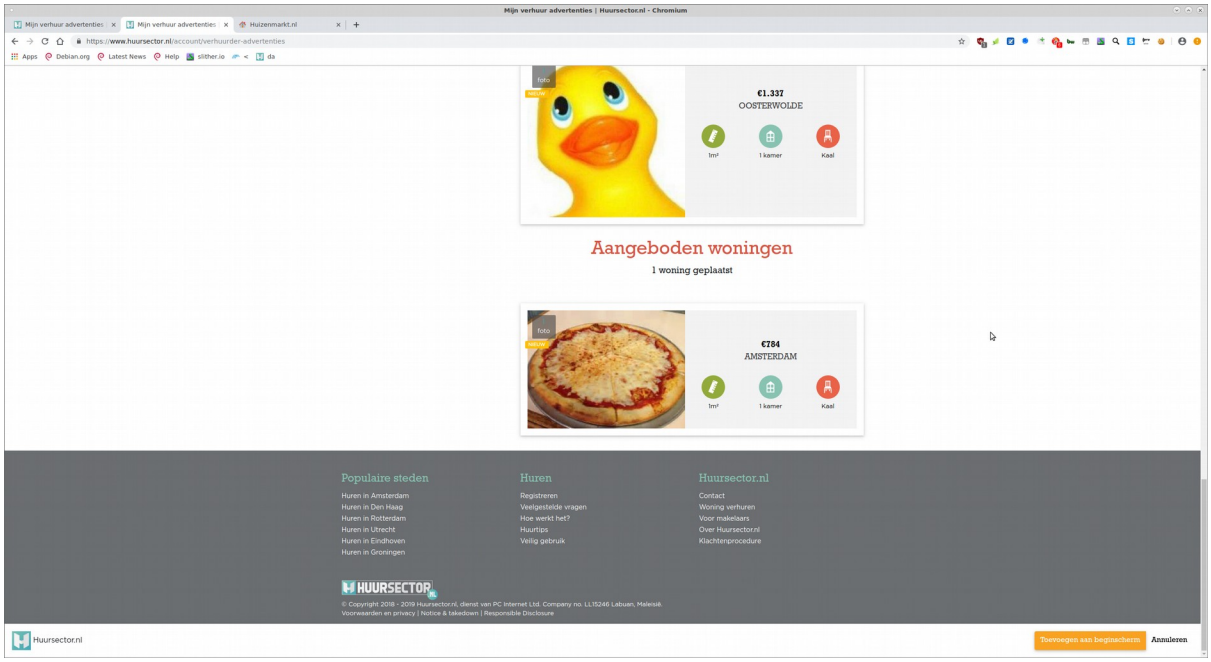
als u alle gegevens heeft ingevuld en de html tag heeft geplaatst in de klacht druk dan op versturen.
U zult nu een berichtje krijgen dat het succesfol verstuurt is.

Als u nu in uw mail kijkt waar de klacht is ontvangen zult u merken dat de html tag is afgegaan en de text bolt is geworden.

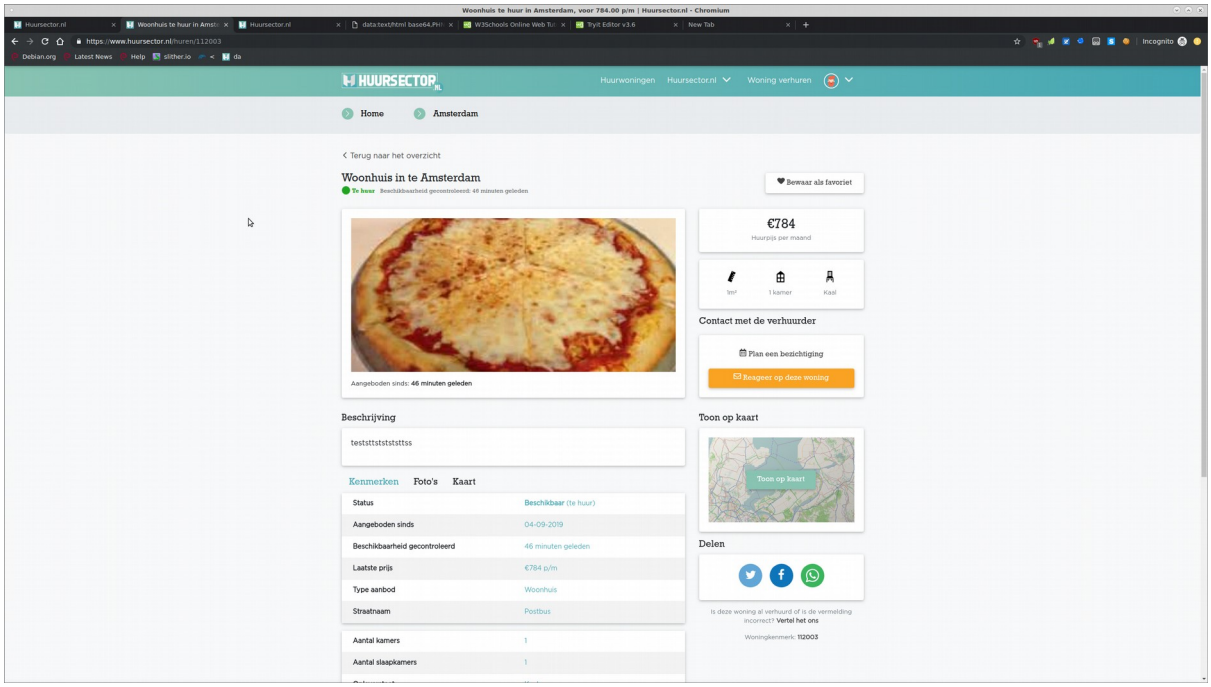
3.4. Reacties die worden ontvangen bij adverteerders worden niet escaped voordat ze worden verstuurt.

Tijdens mijn onderzoeken op 4 September kwam ik er achter dat als u een reactie stuurt naar een adverteerder dat de reactie unescaped wordt verstuurt en als u code meestuurt in de reactie dat deze afgaat in de mail client van de adverteerder.

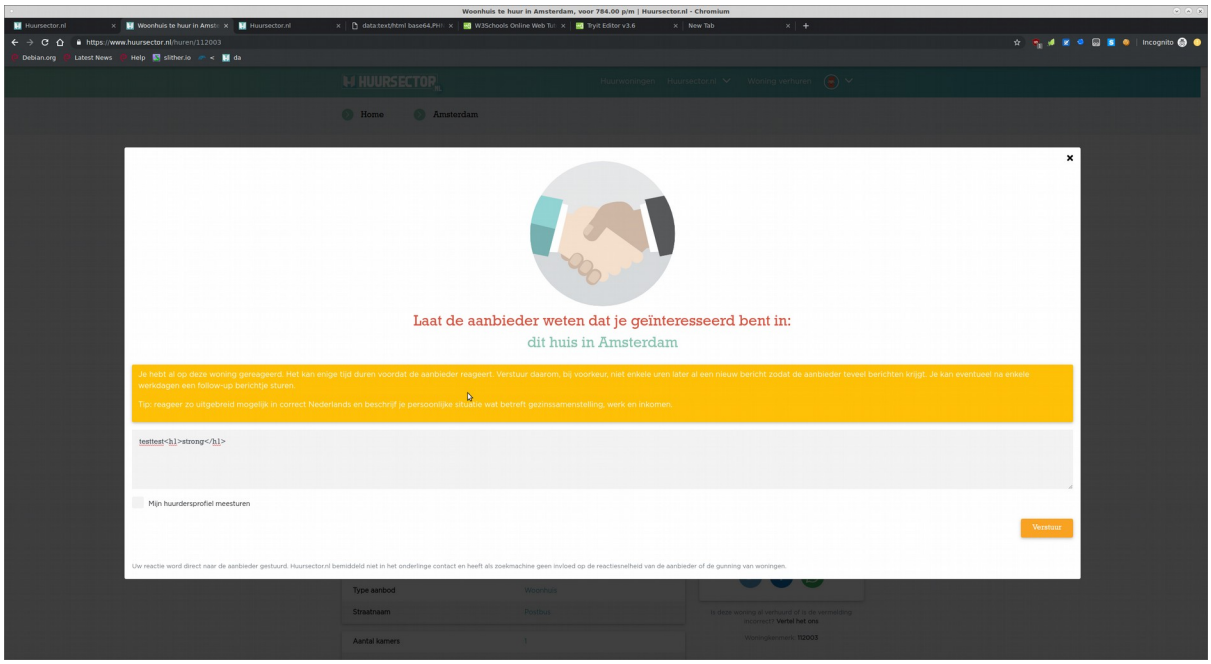
Om deze lek te verifiëren moet u 2 premium accounten hebben waar 1 adverteerde 1 advertentie heeft die is goedgekeurd.



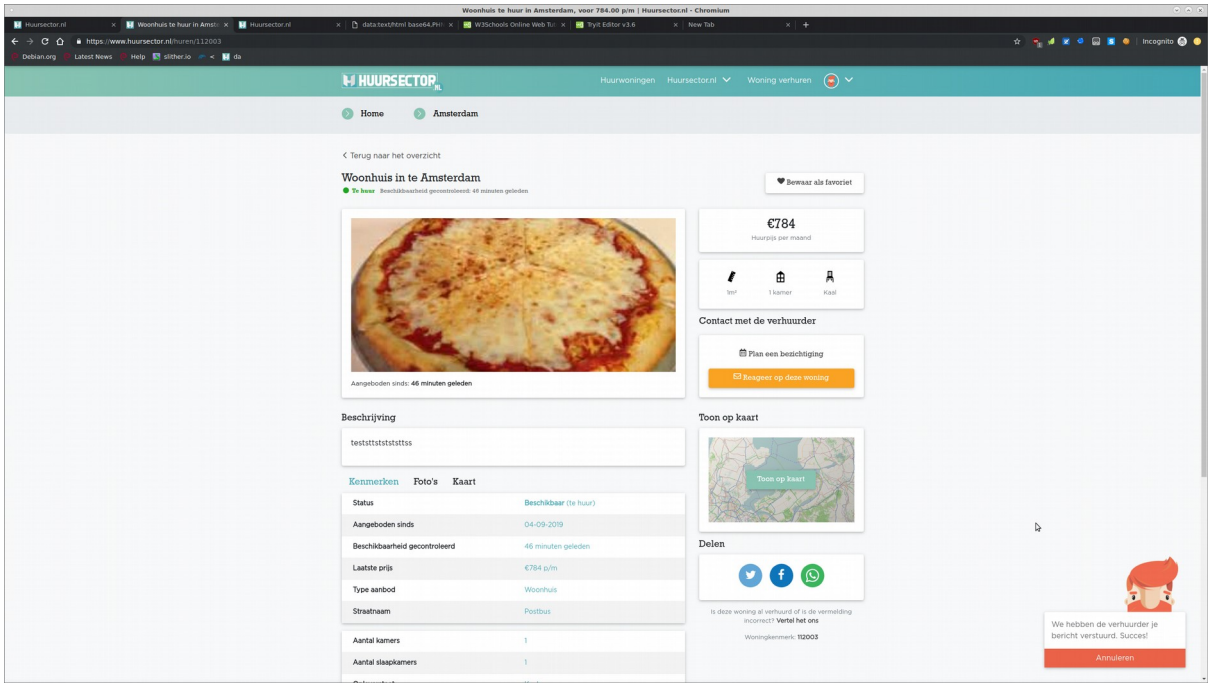
Nu log in op een andere premium user en ga naar deze advertentie.
Daar druk op “reageer op deze woning”



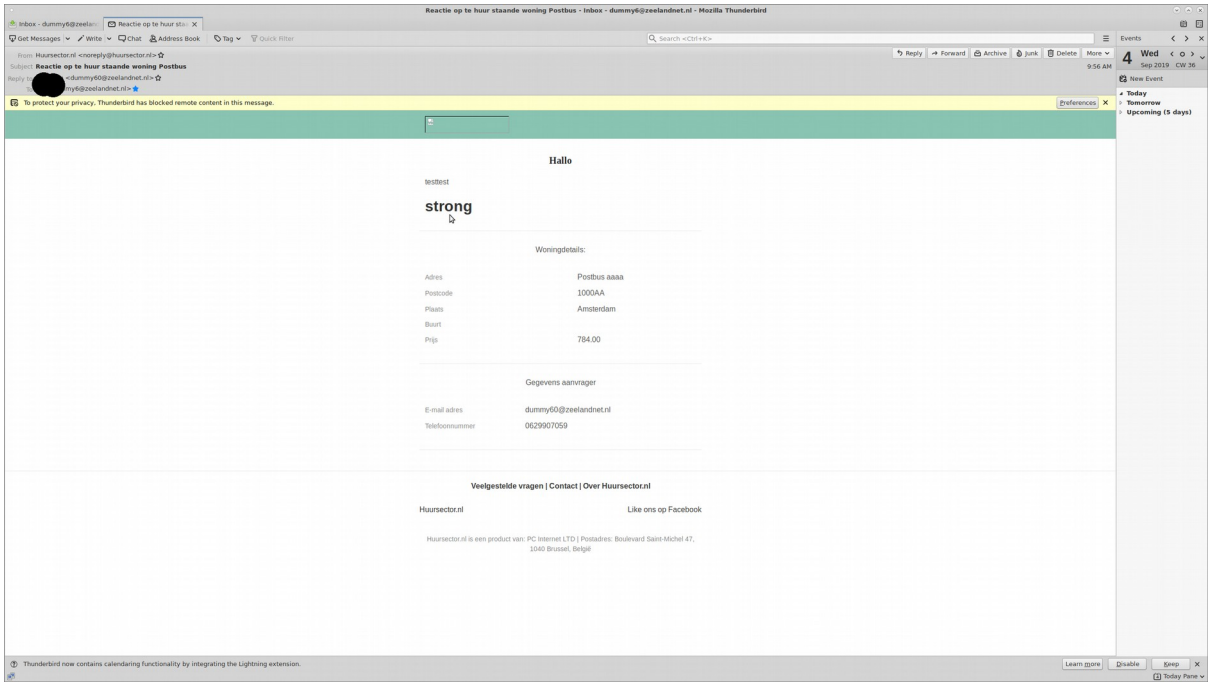
U komt nu op een pagina waar u een reactie kunt sturen.
Plaats in de reactie een html tag en druk op verstuur. (ik gebruik een h1 tag want die is niet geblokkeerd door de firewall)



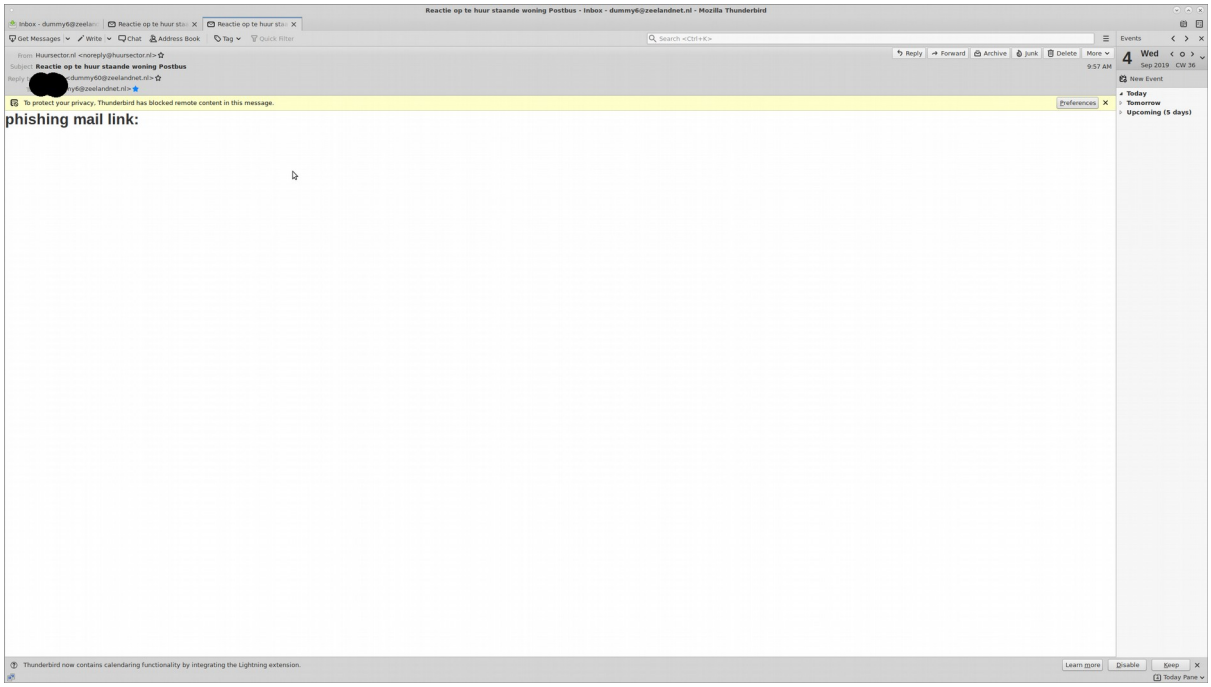
je krijgt nu een bevestiginging dat het bericht is verstuurd.



Als de adverteerder nu de reactie ontvangt in zijn mail zult u merken dat de reactie af is gegaan in zijn mail client.



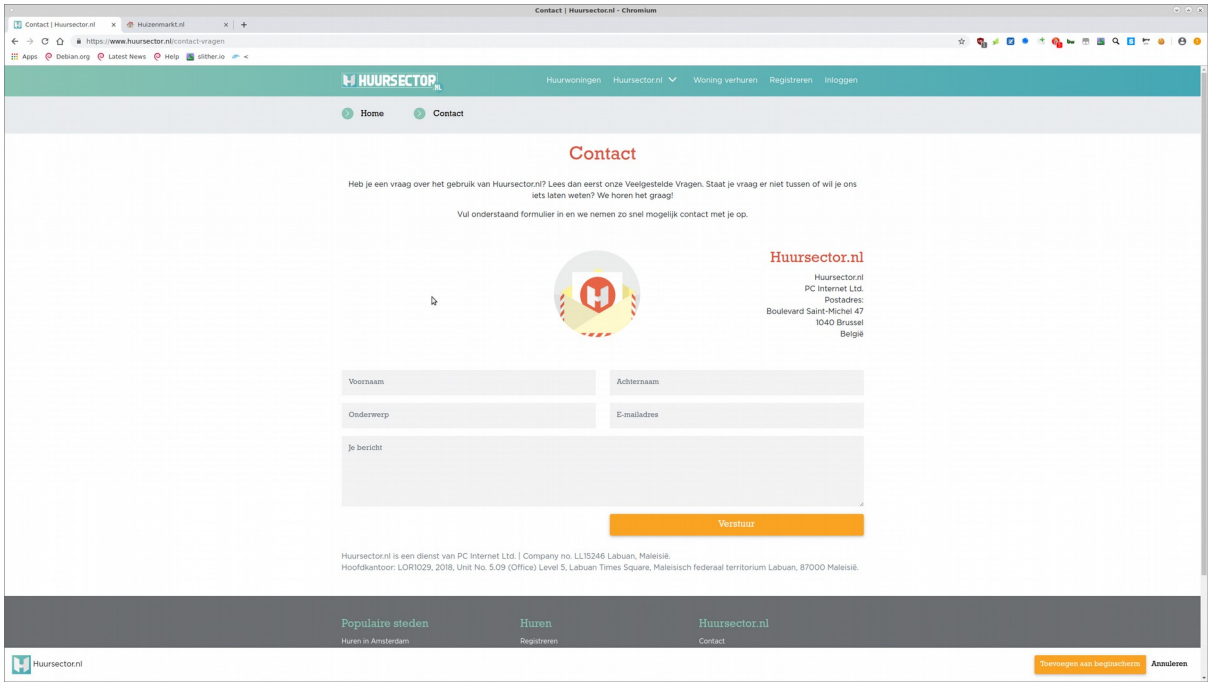
Met een beetje meer puzzelen kun je ook het hele mail herschrijven.



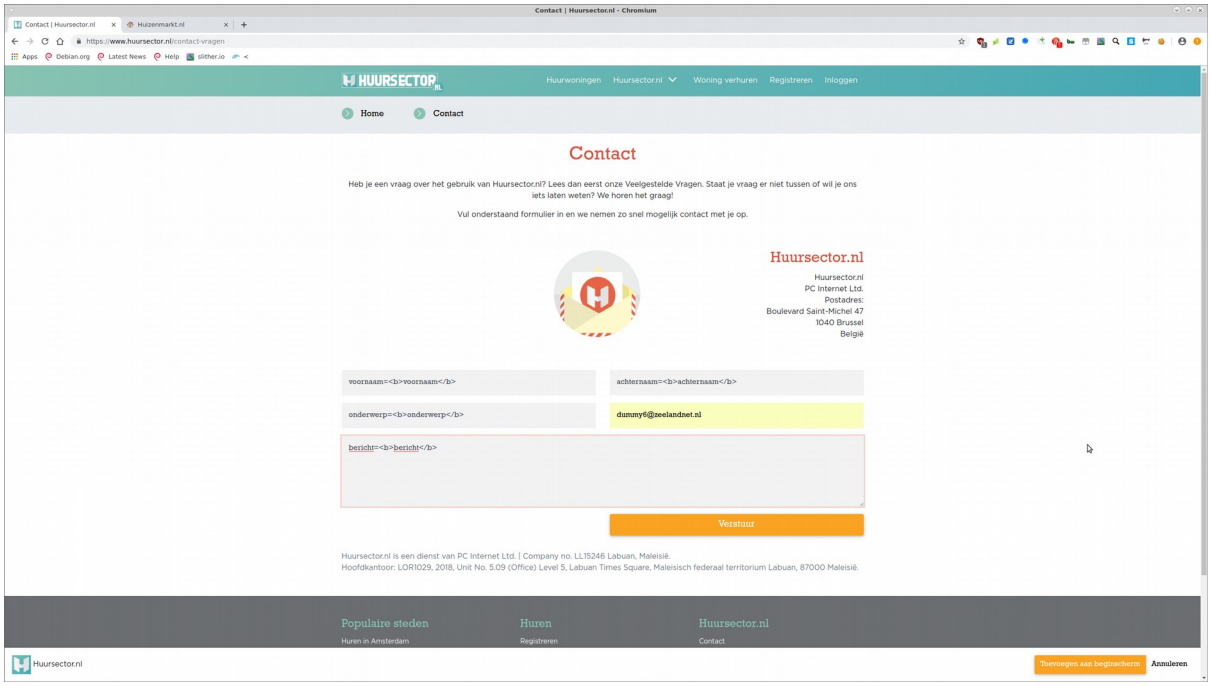
3.5. Berichten die worden verstuurt naar de medewerkers worden niet escaped voordat ze worden verstuurt.

Tijdens mijn onderzoeken op 4 September kwam ik samen met [redacted] er achter dat als u een bericht stuurt in het contactformulier op de webpagina https://www.huursector.nl/contact-vragen dat dit bericht unescaped wordt verstuurt en als u code meestuurt in de bericht dat deze afgaat.

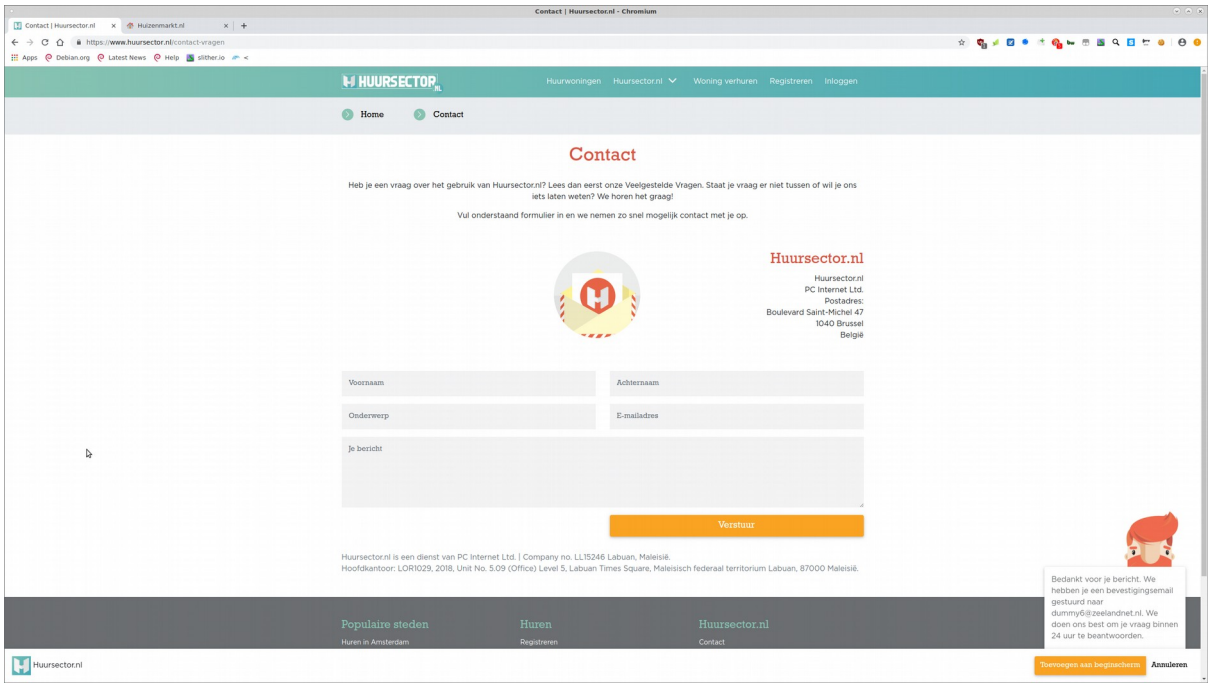
Als u deze lek wilt verifiëren moet u eerst naar de webpagina https://www.huursector.nl/contact-vragen.



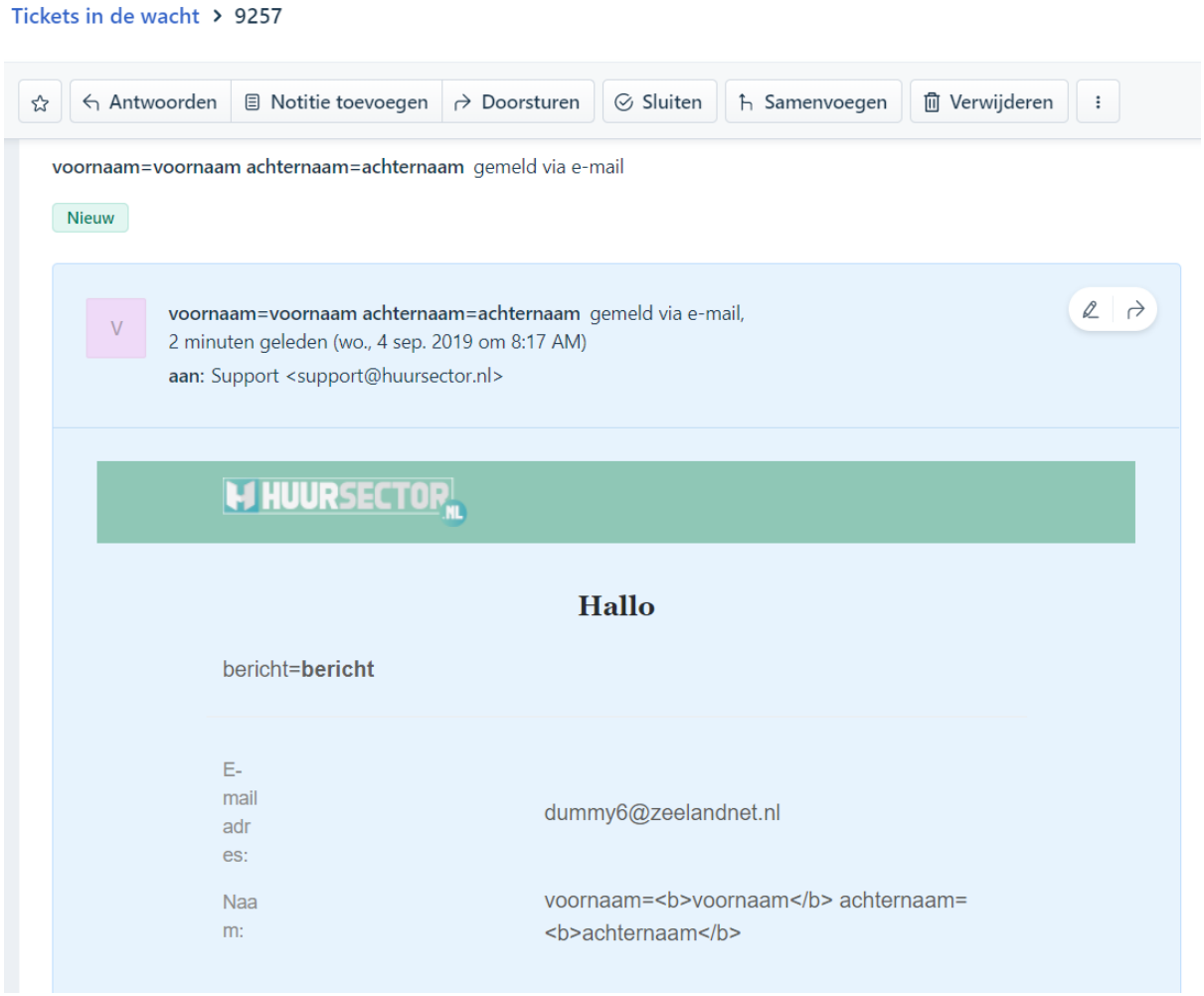
Vul alle velden in maar als laatste veld voer een html tag in zoals de B tag.
En druk op verstuur.



Je zult nu een bevestiging krijgen dat het bericht is verstuurt.



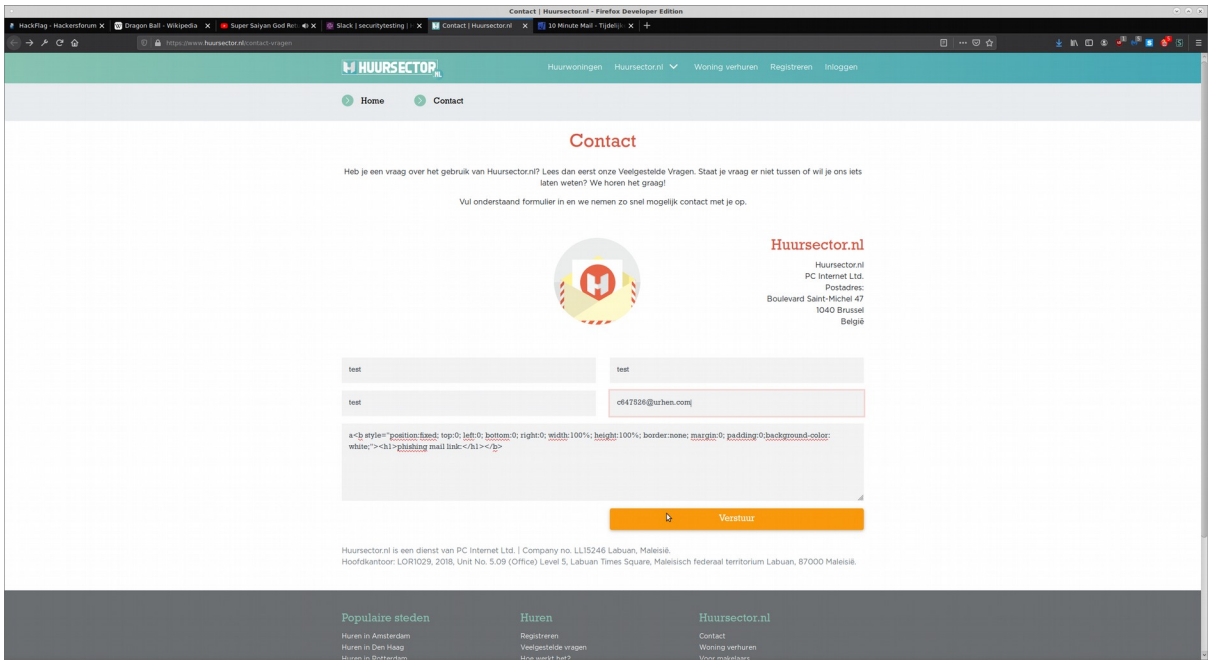
Als de medewerker nu kijkt naar zijn mail merkt hij dat de code is afgegaan in de mail client.



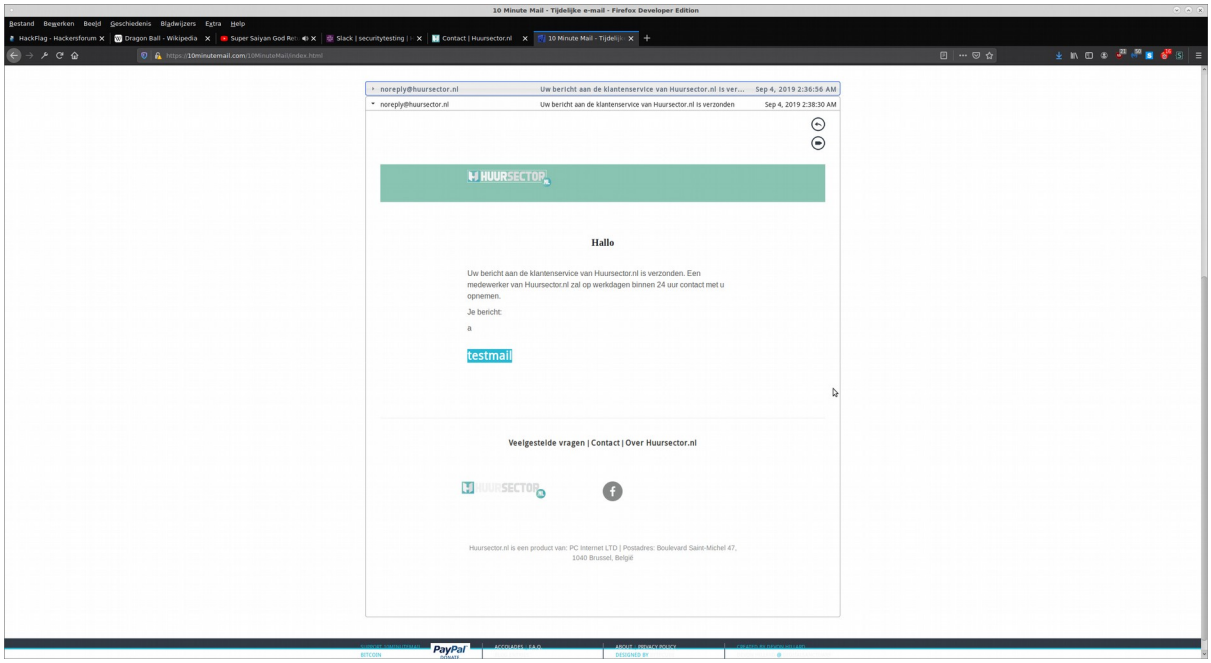
3.6. De bevestigingsmails van het contactformulier worden niet escaped waardoor het mogelijk is om spam te sturen vanaf het huursector domein.

Tijdens mijn onderzoeken op 4 September kwam ik er ook achter dat als u een bericht stuurt in het contactformulier op de webpagina https://www.huursector.nl/contact-vragen dat dit bericht unescaped wordt verstuurt en als u code meestuurt in de bericht dat deze afgaat, maar alle users krijgen een bevestigingsmail binnen en die zijn ook niet escaped.
Dit maakt het mogelijk om spam te laten sturen via het mailadres noreply@huursector.nl naar een mailadres naar keuze.

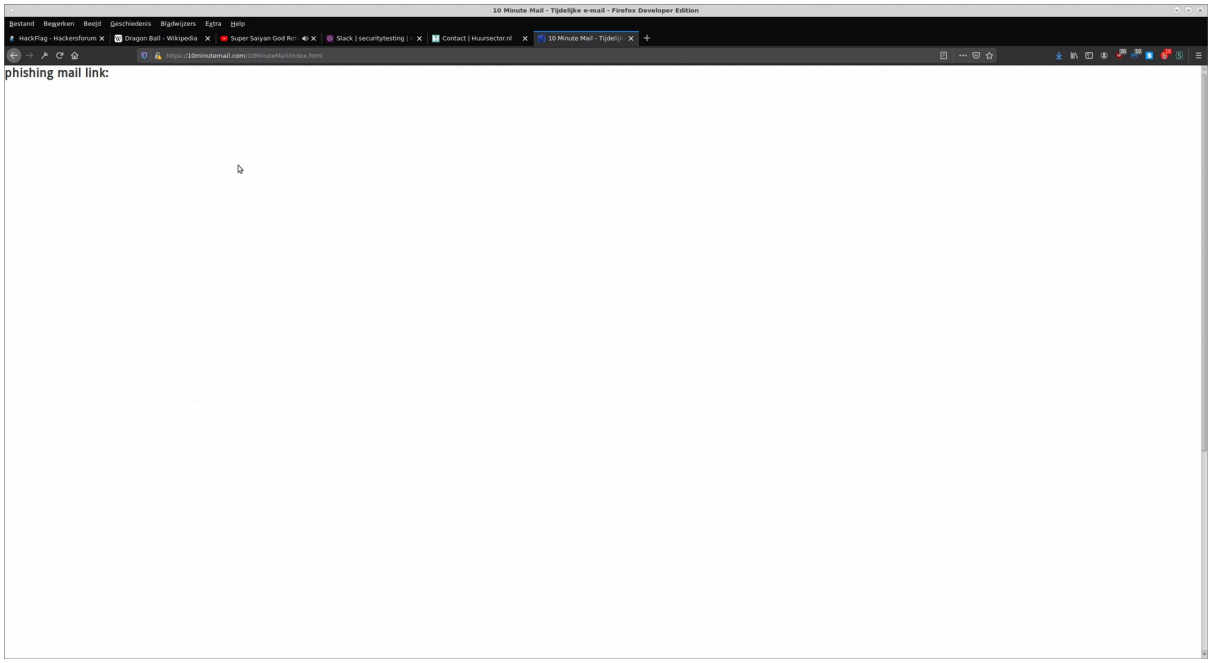
Om deze lek te verifiëren moet je eerst naar de webpagina https://www.huursector.nl/contact-vragen.
Dan volg dezelfde stappen als in 3.4 maar als emailadres kies je het emailadres waar je de spam naartoe wilt sturen.
Voor deze poc gebruik ik een B tag waar met css de pagina full screen is gemaakt.



Als je nu het bericht verstuurt krijgt huursector een bericht, maar ook krijg je een bevestigingsbericht.
Als de user nu kijkt in zijn mail ziet hij dat hij een bevestigings mail ontving.
Als je alleen een simpele h1 tag stuurt zie je dat de text groter is geworden



maar als je hem fullscreen maakt dan is het hele mail herschreven.



Het verschilt per mail client maar roundcube, thunderbird en 10minutesmail.net werken zeer goed met dit.

Dit is een interessante lek want nu kan ik via jullie mailadres spam sturen.
Hier zou ik even een kijkje naar nemen.

4. lage prioriteit.

4.1. Geen rate limiting op contact en klachtenformulier.

Tijdens mijn onderzoeken op 4 September kwam ik er achter dat in het contact formulier (https://www.huursector.nl/contact-vragen) en het klachtenformulier (https://www.huursector.nl/klacht) dat er geen rate limiting zit op het versturen van het bericht.
Hierdoor kun je het bericht over en over sturen waardoor je makkelijk 180 mails kan ontvangen binnen 2 minuten.
Een mogelijke patch is om een recaptcha te implementeren op de klachtenformulier en contact formulier.