Vulnerability rapport over:

https://www.huursector.nl/

HUURSECTOP Huurwoningen Huurwoningen Huurwoningen Huurwoningen
Jouw nieuwe huurwoning zó gevonden!
Zoek op plaats 60 V Hoursy stat Zoek O
Hoe werkt Huursector.nl?

Bedrijf: Hackoclipse Datum: 9 September 2019

Inhoud

1.	Wat is de opdracht3
1.	Zeer hoge prioriteit4
	1.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van iemand anders advertentie
	1.2. Insecure direct object reference in advertentie bewerken leidt tot verwijdering van iemand anders advertentie
2.	Hoge prioriteit14
	2.1. Insecure direct object reference in advertentie verwijderen leidt tot verwijdering van al geaccepteerde advertentie
	2.2. Insecure direct object reference in bewerken leidt tot verwijdering van al aangeboden advertentie
	2.3. Stored cross site scripting door middel van het bewerken van een woning voordat het geaccepteerd is
3.	Gemiddelde prioriteit
	3.1. 2 reflective xss'en in de facebook autorisatie en google autorisatie doormiddel van malformed url
	3.2. Bypass om een naam van een premium account aan te passen zonder dat de user dit hoort te kunnen
	3.3. Klachten die worden ontvangen worden niet escaped voordat ze worden verstuurt37
	3.4. Reacties die worden ontvangen bij adverteerders worden niet escaped voordat ze worden verstuurt
	3.5. Berichten die worden verstuurt naar de medewerkers worden niet escaped voordat zeworden verstuurt
	3.6. De bevestigingsmails van het contactformulier worden niet escaped waardoor het mogelijk is om spam te sturen vanaf het huursector domein45
4.	lage prioriteit47
	4.1. Geen rate limiting op contact en klachtenformulier47

1. Wat is de opdracht

Het testen van mogelijke kwetsbaarheden van de website:



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.



•		W	oonhuis te huur in Amsterdam, voor 500.	00 p/m Huursector.nl	I - Chromium	* * *
🚺 Mijn verhuur advertenties 🗴 🚺 Woonhuis te huur in Amste 🗴 🍈 Huizen	markt.nl	× +				
← → G L ■ https://www.nuursector.ni/nuren/u12042 Ⅲ Apps @ Debian.org @ Latest News @ Help Sither.io < ③ d	a					x, d = _ d = d = d = d
			Hu	urwoningen Huur	sector.ni 🗸 Woning verhuren 🧁 🗸	
		🔊 Home 🕥 Amsterda	ım			
		< Terug naar het overzicht				
¢		Woonhuis in te Amsterda	m I minsten geleden		♥ Bewaar als favoriet	
		ił4ckh4ck5	279 - 4.63 86th Reputation Rank State	22.50 94t Impact Perce	€500 Huurpis per maand	
		(#4920227) [www.snsbank. State • Resolved (Closed) Disclosed July 10, 2019 11:33a	nl] Reflective XSS Severity 🛄 High (m +0200 Participants 🔒 😿	7 ~ 8.9) (Manage collaborato	Inst I karner Kosl	
		Reported To de Volksbank Weakness Reflected	Visibility Disclosed	(Limited)	Contact met de verhuurder	
		Bounty \$1.000 Aangeboden sinds: 2 minuten geleden	Collapse		🛱 Plan een bezichtiging Si Reageer op deze woning	
		Beschrijving			Toon op kaart	
		dfghnt				
		Kenmerken Foto's Kaar	rt		Toon op kaart	
		1	Status	Beschikbaar (te huur)		
		2	Aangeboden sinds	04-09-2019	Delen	
		3	Beschikbaarheid gecontroleerd	2 minuten geleden		
		4	Laatste prijs	€500 p/m		
		5	Type aanbod	Woonhuis	Is deze woning al verhaurd of is de vermelding incorrect? Vertel het ons	
		6	Straatnaam	Postbus	Woningkenmerk: 112042	

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.

		Mijr	vernuur advertenties Huursector.nl - Firefox Devel	oper Edition		() () () () () () () () () ()
Bestand Bemerken Beeld G HackFlag Hackersforum X	eschiedenis Bladwijzers Eatra Help 10 Dragon Ball - Wikipedia 🗙 🤒 Dragon Ball Super - Bi 🐠 🗙 🎼	🛿 Slack securitytesting F 🗙 🛛 🔢 Woonhuls te hui	ur in Ams 🗙 🔢 Mijn verhuur advertentie 🗙 🕂			
	A https://www.huursector.nl/account/verhuurder-adverter	inties			🖾 🕁	👱 in d s 🖑 🖑 🕱 💕 (S) 😑
		HUURSECTOR				
		🕥 Home 💿 Mijn account	Mijn advertenties			
		Min accurit Min accurit Min advertantes Velgenstedde vragen		Nieuwe woning aanbieden 25.000° woningzoekenden per maan 26.000° woningzoekenden per maan		
			Goed te ke	euren woningen		
				Cl AMSTERDAM (a) (b) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	Ņ	
		Populaire steden Huren in Amsterdam Huren in Rotterdam Huren in Rotterdam	Huren Registeren Veelgestelde wagen Hoe werkt het?	Huursector.nl Contact Woning verhuren Voor makelaars		

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.

	Firefox Developer Edition		(* (* (*)
Bestand Bewerken Beeld	jeschindenis Bigdwiljzers Egtra Help		
🕴 HackFlag - Hackersforum 🗙	o Dragon Ball - Wikipedia 🗴 💆 One Punch Man Seaso: 40 X 🔯 Slack I securitytesting I : X 👖 Woonthuis te huuri in Am: X 👖 Mijn verhuur advetentii: X 🥻 homebäldskhidsfinaskingii: X +		
(e) → ⊁ C @	file () file () file () hashing hearts BugBourty Hunting successful humseter/work-for company (critical) goc.tem	🗟 습	🛓 IN 🗊 🕸 🖷 🛤 🍯 🕄 🗏
token:			
Submit request			
	4		
	~		

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 "csrftoken"

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.)

	Mijn ver	huur advertenties Huursector.nl - Firefox Developer	Edition		(*) (*) (X)
gestand Begerken Beejd Geschiedenis Bladwijzers Egtra Help ≹ HackFlag - Hackersforum X 😨 Oragon Ball - Wikipedia X 🔹 One Punch Man Seaso: € X	👳 Slack securitytesting H 🗙 🛛 🔝 Woonhuis te huur in	Ams 🗴 🔝 Mijn verhuur advertentie: 🗙 🔝 Mijn verhuu	ar advertentie: 🗙 📲 Huurwoningen & Kamer: 🗙 🕇 🕂		
(€) → / C ⊕ (0) ● https://www.huursector.nl/account/verhuurder-adve	itenties			… ☺ ☆	± n o ≎ 📲 📲 s 💕 S ≡
		Huurwoningen Huur	ector.nl 🗸 Woning verhuren 😨 🗸		
	🕥 Home 🚫 Mijn account	Mijn advertenties			
þ	Min accurt Min advertentis Min advertentis		euwe woning nbieden 000 woningsokenden per maand rever tennig ankonen		
		Goed te keu	ren woningen		
			CI AMSTERDAM CO DO I NAMOR AGA		
	Populaire steden Huren in Amsterdam Huren in Rotterdam Huren in Rotterdam	Huren Registeren Vedgestelde vagen Hoe werkt het?	Huursector.nl Contet Woning verturen Voor mäelaars		

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.

voor 5555.00 p/m | Huursector.nl - Firefox E

Ga dan naar die advertentie.

Dan kopieer je het nummer die in de url staat en slaat dat op voor later.

ዶሮድ	https://www.huursector.nl/huren/amsterdam/112091				v … ⊠ ☆	¥ N O 0 🔮 📲 🖬
		H HUURSECTOP				
) Home Amsterdam				
		< Terug naar het overzicht				
		Woonhuis in te Amsterdam • Te huar Beschildbaarheid geocetroleezt: 55 soor	onden geleden	• Bewaar als favoriet		
		Ams	terdams	€5,555 Huurpisper maand		
			TI AA	555m ² 1 kamer Kaal		
				Contact met de verhuurder		
		Aangeboden sinds: 58 seconden geleden		E Plan een bezichtiging		
		Beschrijving		Toon op kaart		
		555555555555555555555555555555555555555				
		Kenmerken Foto's Kaart		Toon op kaart		
		Status	Beschikbaar (te huur)			
		Aangeboden sinds	04+09-2019	Data		
		Beschikbaarheid gecontroleerd	58 seconden geleden	Deten		
		Laatste prijs	€5.555 p/m	🕑 🗗 🔕		
		type aanbod Straatnaam	Woonhuis Postbus	Is deze woning al verhuurd of is de vermelding		
		Aantal kamers		Incorrect? Vertel het ons Woningkenmerk: 112091		
		Autor Autors				

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.

•	Mijn verh	uur advertenties Huursector.nl - Firefox Developer	Edition	
Bettand Begeld Geschiedenis Bigdelijzers Egta Egto It HackFilag HackFilag	ck securitytesting X Woonhuis te huar in A: X enties	Nijn verhuur adverten: 🗙 🔡 Hall of Fame Huursec	🗙 📔 Huursector.el 🛛 🗙 📓 Mijn verhuur adverten: 🗙	🖬 Mijn verhuur adverte:: X 📓 Huursoningen & Kam:: X 🚯 Nieuw tabbiad X 🕞 🏠 👱 🖍 🗊 🌚 🖓 👫 🛒 💕 🧐
	M HUURSECTOR	Huurwoningen Huur	sector.nl 🗸 Woning verhuren 🥃 🗸	
	🕥 Home 💿 Mijn account	Mijn advertenties		
	Min account Min account Min advertentes Vergestede vragen	Ni aa 200	euwe woning inbieden 000+ woningzeekenden per maand rever wedag aablieden	
		Goed te keu	ren woningen	
			CONSTRUCTION CONST	
Lings Sweet Namestar All Construction Sweet and Lings	Populaire steden Huren in Amsterdam Huren in Detterdam	Huren Registeren Verigestelde vragen Hoe werk het?	Huursector.nl Centect Woning verburen Voor makelaars	

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

Nummerter el - Eirefex De

Bestand Besperken Beeld Geschiedenis Bladwijzers Egtra Help ≹ HackFlag - Hackersfor: X 😨 Dragon Ball - Wikiped: X 😨 Super Salyan God P: 40 X 🖉 Slack securitytesting: X	🖬 Woonhuis te huur in A- 🗴 📓 Huursector.nl 🛛 🗴 🖬 Hall of Rame Huursec: 🗙 📓 Huursector.nl	🗴 📓 Mijn verhuur adverten: X 📓 Mijn verhuur adverten: X 📓 Huurwoningen & Kans: X 🚯 Nieuw tabblad 🛛 X 🕂
(€ → / C û		✓ ··· ♡ ☆ ± M □ ● ♣ ⁰ № ■
M HUURS	ECTOR _{NL} Huurwoningen Huursector.nl V V	Voning verhuren 💿 🗸
📎 Ноте	S Mijn account S Mijn advertenties	
() Min acc	Jouw huurwoning	
Mijn adv	vertenties Type woning	-
(?) Veriges	Viconhuis Appurtement Kamer	Studo
	Upload foto's Het uploaden van foto's kan eventueel ook op een ister tijstist Oor op	
	Alten JPG, JPEG, en PNO bestanden, Maximale bestandigroo	te № 1048. I Kamers

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)

	Huursector.m - Firefox Developer Edition
gestand Begerken Beejd Geschiedenis Bigdeijters Egtra Help 2 HackFilge - Hackersfor: 🗙 🔯 Dragon Ball - Wikiper: X 📴 Sper Seiyan God 🗉 🐠 X 🔡 Stack securitytesting X 📗 Woorhuis te huur in A - X	🛛 Haursectorel 🛛 x 🖬 Hall of Fame (Haurse: x) 📓 Haursectorel x 📓 Mijn verbaar adverter: x 📓 Mijn verbaar adverter: x 📓 Mijn verbaar adverter: x 📓 Haurseoningen & Kam: x 👌 Neuw tabblad 🛛 x +
(€) → /² C* A (0) A https://www.huursector.nl/account/ver/huurder-advertentiles/112091	
M HUURSECTOR _M	Haurwoningen Haursectorni V Woning verhuren 🧿 V
💿 Homo 💿 Mijn account	Ø Mijn advertenties
	e Terug
	Iouw huurwoning
Mijn account	in Amsterdam
Min advertenties	
	Type woning
? Vergestelde vragen	Viconhuis Ageartement Kamer Studio
	Inlad folds
	Het spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto's kar eventueel ook op een laker tijdstip Image: Spleaden van foto:
	Oppervlakte
	885 1 1

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

Huursector.nl - Firefox Develope

<u>B</u> estand Be <u>m</u> erken Beeld <u>G</u> eschiedenis Bl <u>a</u> dwijzers Egtra <u>H</u> elp				
👌 HackFlag - Hackersfon: 🗙 🛛 👹 Dragon Ball - Wikiped: 🗙 📄 🖬 Super Salyan God R. 🛛 🗙 🖉 Slack securitytesting: 🗙 📲 Huursector.nl	X 🔢 Huursector.nl 🛛 X 🔡 Hall of Fame Huurs	e:: 🗙 🛛 🔣 Huursector.nl 💦 🗙 🔛 Mijn verhuur adve	rten: 🗙 📔 Mijn verhuur adverten: 🗙 📗 Huurw	ningen & Kama 🗙 👌 Nieuw tabblad 🛛 🗙 🕇 🕂
(€ → / C û (0) ▲ https://www.huursector.nl/account/verhuurder-advertenties/112091				👱 in co 👁 🖑 📲 💕 (S) 😑
	O opportunito			*
	555	1 ~		
	Huurphis per maand	Rantal slaapkamers		
	5555.00	1 ~		
	Inclusief gas, water en licht			
	Copieverstaat	P Beschikbaar vanaf		
	Gemeubileerd	2019-09-04		
	Gestoffeerd			
A	Kaal			
	Beschrijving			
	855555555555555555555555555555555555555			
				1
		4		
	Opslaan			
Populaire steden				
Huren in Den Haag Muran in Dottarriam	Veelgestelde vragen Hoe werkt het?	Woning verhuren Voor makelaars		
Huren in Eindhoven Huren in Groningen				
li: Copyright 2019 - 2019 Haursectorni, die				
وكالالالية التلوي التيكي الشروع ومنها والمتعاد المرتب المتلا وليتنا				

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.

Ele Edit View History	Bookmarks Jools Help	Woonhuis te	huur in Almere, voor 999.00 p/m Huur	ector.nl - Mozilla Firefox		
Account Huursector.nl	X Account Huursector.nl X Min verhuur advertenti	🗉 X 🚺 Woonhuis te huur in Alm: X 🕂			v 🖾 🛧 🔿	n n 📲 + a 🚚 📟 :
<u></u>		M HUURSECTOR	Huurwoning	ien Huursector.ni 🗸 Woning verhuren 😩 🗸	·	
		Home Almere	Almere Stad			
		< Terug naar het overzicht				
		Woonhuis in Almere Stad te Alm • Te huur Seechtkisaacheid gecontmoerd: 15 minnten ge	lere	♥ Bewaar als favoriet		
		0	-	€999 Huurpis per maand		
				1 🖻 🛱 Im ⁴ I kamer - Kaal		
				Contact met de verhuurder		
		Aangeboden sinds: 15 minuten geleden		Plan een bezichtiging		
		Beschrijving		Toon op kaart		
		accept				
		Kenmerken Foto's Kaart		Toon op kaart		
		Status	Beschikbaar (te huur)	State 1		
		Aangeboden sinds	09-09-2019			
		Beschikbaarheid gecontroleerd	15 minuten geleden	Delen		
		Laatste prijs	€999 p/m			
		Type aanbod	Woonhuis			
		Straatnaam	Wisselweg	Is deze woning al verhuurd of is de vermelding incorrect? Vertel het ons		
		Aantal kamers	1	Woningkenmerk: 114773		

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/</th></tr><tr><td>112042" method="POST"> token: <input name="_token" value=""/> <input name="_method" type="hidden" value="DELETE"/> <input type="submit" value="Submit request"/> </form></body></html>

File Edit View Search Tools Documents Help	*poc.html [-/hacking/reports/BugBountyHunting/succesfol/huursector/work-for-company/critical] - Pluma	* * X
S Di Coen - A Save Di Go Undo 🛷 🔟 💈 🖹 🖸 🕼		
i pavload M i poc.ht M i pavload.ht M i pavloads M i poc. M i pavloads.ht M i poc. M @ *poc.htm	il X	
<pre>shall coop </pre>		
4		
	HTML • Tab Width: 4 •	Ln 4, Col 77 INS

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 <u>https://www.huursector.nl</u>. 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.

File Edit View History	Rockmarks Tools Help	Huurwoningen & Kamers Huursector.nl - Mozilla Firefox		* * X
Account Huursector n)	Account Huursectorn X Nin verbaur advectention X	Weenhuis te buur in Alm: X T Buuryseelingen & Kamer: X +		
	https://www.huursector.nl		··· 😇 🔶 습	IV (D 🖬 . 🔅 💁 🙈 🗏
		HUURSELIUK		
		Jouw nieuwe huurwoning zó gevonden!		
		,		
		Haurprijs vanaf Haurprijs tot		
		Zoek op plaats E0 Geen maximum Zoek 9		
	_ L			
Console	Debugger () Style Editor @ Performance @ Memory > Netw	ork 🖨 Storage		8-6800e×
+			1 of 1 csrf	Rules Computed Layout Anim -
<html lang="nl"> (D)</html>				v Hiter Styles + 10 .cs
<pre>w chead itenscopes** itentype</pre>	"http://schema.org/WebSite">) Inthe
«neta nane="viewport" con	ent="width=device-width, initial-scale=1, shrink-to-fit=no">			*, ::after, application.css:11 ::before 0 {
	<pre>https://www.hursector.nl"></pre>			box-sizing: barder-bax:
<pre>k rel="apple-touch-ic clink rel="apple-touch-ic</pre>	n' Bref='https://www.busrsector.nl/images/logo.144.144.png">			Inherited from html
k rel="shortcut icen"	href="https://www.huursector.nl/images/Wwicen-32-32.org">			:root (explication.css:11
<neta content="Huursector.nl" name="application-n</td><td>me"></neta>			blue: #007bff:	
<pre></pre>	"/manifest.isen" crossorigin="use-credentials">			purple: #6142c1;
<nets content="https://www.huursector.nl/images/logo-144-144.png</td><td></td><td></td><td>pink: #el3elc;</td></tr><tr><td><pre><title>Huurwenlopen 5 Kan <neta property=" descripti"<="" nane="msapplication</td><td>TileImage" pre=""></nets>	<pre>rs Huursector.nt n' name="description" content="Huurwoningen, appartementem en kamers</pre>	te huur. Snel woonruim.elke dap het nieuwste aanbod van particulieren en makelaars!">		orange: #fd7e14;
«1Open Graph>				green: #280745;
<pre> cneta propertys"og:image" cneta propertys"og:title"</pre>	name="og:image" content="https://www.huursector.nl/images/logo-1200-0 name="og:title" content="Huurwaningen & Kamers Huursector.nl">	an bul.>		teal: #28(997)
«meta property»"og:site_m	me" content="Mursector.nl">			white: #fff;
<pre>emeta property*'og:descri conta propert</pre>	tion" name="og:description" content="Buurwoningen, appartementen en i	amers te huur. Snel woonruim…elke dag het nieuwste aanbod van particulieren en makelaars!">		gray: #6c7576;
«seta property» ogitype"	ame="opitype" content="website">			primary: #085644;
«seta property="ogilocale	name="og(locale" content="nl">			secondary: #89c4b2; success: #28a745;
<pre> deta property='twitter:t</pre>	tle" name="twitter:title" content="Haurwoningen & Kamers Haursector	<16.		info: #17a2b8;
<meta ;<="" content="https://www.huursector.nl/images/</td><td>ogs-1280-633.png*></td><td></td><td> danger: #0:3545;</td></tr><tr><td><pre></td><td><pre>com/leafletal.5.1/dist/leaflet.css' type=" css'="" name="twitter:image" pre="" property="twitter:1</td><td>age" rel="stylesheet" text=""/>	enten en samers te nuur, smet wommruim.eine oag met nieuwste aansoo van partituiteren en MakéläärST'>		Light: #f8f9fa;	
html > head > meta				breakpoint.as: 0;
mann - means - mieta				())

- Firefox Developer Edition		~ ~ x
🕴 HackFlag - HackEng - Ha		
	··· 🖾 🕁	± in © ⊕ ● ● ■ 6 *5 =
token: Januar Januarian Januari		
Submit request		
4		

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.

File Fulit Minus Misters	Paralamente Tarde Mala		Huursector.nl - Mozilla Firefox			· · · ·
Account Huursector.nl X	Count Huursectorn X] Mijn verhuur advertentie: X	Huursector.nl X Huurwoningen & Kamer	X] Mijn verhuur advertentie X +			
← → ♂ ☆	A https://www.huursector.nl/huren/114773				😇 📥 🏠	n ⊡ 📌 + ⊜ 🖑 🖤 ≡
		H HUURSECTOR	Huurwoningen Huurs	sector.ni 🗸 Woning verhuren 🌘) ~	
	4					
			404			
		Oeps. De	pagina die je zoekt, kunnen we n	iet vinden.		
			Woningoverzicht			
		Populaire steden Huren in Amsterdam Huren in Den Haag Huren in Rotterdam	Huren Registreen Veelgestelde vragen Hoe werkt het?	Huursector.nl Contact Woning verhuren Voor makelaars		
		Huren in Utrecht Huren in Eindhoven Huren in Groningen	Huurtips Veilig gebruik			
		HUURSECTOR Copyright 2018 - 2019 Huursectorni, dienst van PC Inte Copyright 2018 - 2019 Huursectorni, dienst van PC Inte Voorwaarden en privacy Notice & takedown Responsit				

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.

	Mijn verhuur advertenties Huursector.nl - Chr	romium	· · · · · · · · · · · · · · · · · · ·
🖬 Mijn verhuur advertenties 🗴 📓 Huursector.nl 🛛 🗴 🖬 Mijn verhuur advertenties 🗴 📳 Woonhuis te huur in Alme: 🗴 📀 reca	sptcha - Google Search 🗴 📘 Huursector.nl	× 👩 1314 CB Wisselweg (Alm. × 🕂	
			al 🗮 al 🗮 🔿 🖓 🗮 💩 Lineannite 🗛 1
The second se			H 🐡 💭 🗙 👻 🔤 💁 🚺 incognito 🤯 :
🥙 Debian.org 🖗 Latest News 🥀 Help 📓 slither.io 🛷 < 📓 da			
	All started		
		Im ² I kamer Kaal	
		Bauad	
	279 - 4.63	86ti 🔍 🔇	
	Reputation Rank Signal	Perces	
	anshank pil Reflective YSS		
	shabanking kenective A33	66.754	
	id (Closed) Severity	ALMERE STAD	
	2019 11:33am +0200 Participants	ALMERE	
	A Visibility	Dista	
	a Resisting (VER)		
	a scipting (cash-		
		Im ² I kamer Kaal	
	Cottapoe		
	Aangebo	oden woningen	
	1 v	voning geplaatst	
	foto		
	THE OWNER OF THE OWNER	€999	
		ALMERE STAD	
		ALMERE	
	All and and a		
		Im ² I kamer Kaal	
والمتحد والمتحد والمتحري والمحري المرجع المتحد والمتحد والمحد والمحد والمحد والمحد والمحد والمحد والم			
Populaire steden			
ropalate steden			
Huren in Amsterdam			
ettos://www.huarsector.nl/account/verbraurder-advertenties#			
	MAB washt har?	TOAR MITCH SHE	

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.

Mijn verhuir advententies ×	x 🔢 Woonhuis te huur in Alme- x 💿 recaptchi	a - Google Search x 🖿 Hoursectarul x 🔮 1131 (21) (Waarloog (Alic: x +
		Huurwoningen Huursectorni V Woning verhuren 🤗 V
	Nijn account	Ø Mijn advertenties
		test test2
		Reng
		Jouw huurwoning
	Mijn account	in Almero
	Mijn advertenties	Type woning
	vengestende vragen	Vitoorhuis Appartement Kamer Studio
		Upload foro's He uploader van foto's kan eventueel ook op een later tijdstip
		Alleen JPG, JPEG, en PNG bestanden. Maximale bestandsgroote is 10MB.
		🕜 Oppervlakie 👝 Aantal Kamers .
Millin verhuur sovertentie: x Millinursector el x Millinursector el	x Woonhuis te huur in Alme: x @ recartch	Nuursectoral - Chronium ○ ○ △ ▲
← → C △ ▲ https://www.huursector.nl/account/verhuurder-advertenties/114773		tr 😻 🚽 🗶 🏶 📄 🕱 ♦ Incognito 😋 ‡
		Huurwoningen Huursectorni V Woning verhuren 🤗 V
	🕥 Home 🕥 Mijn account	Mijn advertenties
		test test2
		Terug
		Jouw huurwoning
	Mijn account	in Almere
	Mijn advertenties Veelgestelde vragen	Type woning O Accurtement Kamer Studio
		Upload foto's Het uigsaden van foto's kan eventueel ook op een later tijstsp International foto skan eventueel ook op een later tijstsp International foto skan eventueel ook op een later tijstsp International foto skan eventueel ook op een later tijstsp
		🕜 Oppervlakte 💦 Aantal Kamers

•		Huursector.nl - Chromium		(v) (x) (x)
🔢 Mijn verhuur advertenties 🗴 🔛 Huursector.nl 🛛 🗴 🔛 Huursector.nl	🗴 🛐 Woonhuis te huur in Almer 🗴 👩 recaptcha - Google Si	earch 🗴 🔝 Huursector.nl 🛛 🛛 🛪 🧕		왜 비행히 물건에 웃던 방문에 부가가 만나 도망하며 여기 비행하게 비행
← → C ☆ i https://www.huursector.nl/account/verhuurder-advertenties/114773				🖈 🤴 💋 🔽 🤷 😡 🗾 Incognito 💮 🗄
🤨 Debian.org 🔮 Latest News 🔮 Help 🔣 slither.io 🥟 🤜 🔢 da				
	^	Oppervlakte	Aantal Kamers	^
		- pp	•	
		1	1	×
	A	Huurprijs per maand	Aantal slaapkamers	
		999.00	• ·	× ·
		Inclusief gas, water en licht		
		Onlanation		
		Opteversiaat	Beschikbaar vanaf	
		Gemeubileerd	2019-09-09	
		Gestoffeerd		
		Kaal		
	Beer	And Index of		
	Besc	anijving		
	aco	ept		
	or	psiaan		
		4		
	Huren in Den Haag Veelge Huren in Datterdam Hon w	estelde vragen	Woning verhuren	
	Huren in Utrecht Huurti	ips	Over Huursector.nl	
	HUURSECTOR			
	© Copyright 2018 - 2019 Huursector.nl, dienst van PC Internet Ltd.			
	voorwaarden en privacy (Nouce & takedown (Nesponsible Discie	osare		

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

		Huursector.nl - Chromium		· · ·
 Mijn verhaur advententies x M Haursector.nl x M Haursector.nl → C C A https://www.haursector.nl/huren/114773 Deblan.org 0 Latest News 10 Help S sitter: 0 = < M da 	x 📕 Huursector.nl 🛛 🗙	🕲 recaptcha - Google Search 🗴 📘 Huursector.nl	× 🔯 1314 CB Wisselweg (Alm: × +	st 👻 🖋 🗶 D 😡 🕱 🐠 Incognito 🚱 :
	H HUURSECTOP,		Huursector.nl 🗸 Woning verhuren 🤗 🗸	
Ŀ		404 Opps. De pagina die je zoekt, kunnen	we niet vinden.	
	Populaire steden Haren en Ansterdam Haren Bon Haag Haren Bon Hade Haren Bouteden Haren en Userdt Haren Henderber Haren en Genergen Henderber Hende	Humen Registrean Verlagsstälde wegen noor werk her? Haartos Verlag gebruik Verlag gebruik Sonia ven PC intervert Lit. Schwart Halenak doort (Responselie Dachwart	Huursector.nl Cortes Wormekens Vormekens Over Aussectors Reichterenochue	

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 <u>https://www.huursector.nl/account/verhuurder-advertenties</u> gaan.

Mijn verhuur advertenties Huursector.nl - Chromium 📀						
🚺 Account Huurse x 🚺 Huursector.nl 🛛 x 🚺 Huursector.nl 🛛 x 🚺 Woonhuis te huu 🤉	x 🚺 > Huurwoningen x 🚺 Appartement te 🗆 x	🚺 Mijn verhuur adv 🗴 🚺 Woonhuis te huu 🗴 🚺	🕽 Mijn verhuur advi 🗴 🚺 Mijn verhuur advi 🗴 📑 Log into Facebool 🗴 📋	https://images.h: x 🗱 W3Schools Onlin: x 🗱 Tryit Editor v3.6 🛛 x	+	
← → ♂ ☆ 🔒 https://www.huursector.nl/account/verhuurder-advertenties				x 📬 🖌 🛛 🔹 🖄 🗛 🛏 🗇 🗳 Q 🖬 🗠 🧕	00	
III Apps 🝳 Debian.org 🝳 Latest News 🝳 Help 🧾 slither.io 🛷 <						
	M HUURSECTOR _M	Huurwoningen Huu	rsector.nl 🗸 Woning verhuren 🤗 🗸		Î	
	🕥 Home 💿 Mijn account	Mijn advertenties				
		test test2				
	Mijn account Mijn advertenties Verligestelde vragen		ieuwe woning anbieden 000+ woligzekenden per maand Revers weng aablanke			
		Goed te keu	ıren woningen	Þ		
			AMSTERDAM			
	Populaire steden Huren in Amsterdan Huren in Rotterdan Huren in Rotterdan	Hurren Registreren Verlgestelde vragen Hee werkt het?	Huursector.nl Contact Woring withium Voor makdaara			

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)

Woning zelf verburen Hoursector.nl - Chromium					
🚺 Account Huurse x 🚺 Huursector.nl x 🚺 Huursector.nl x 🚺 Woonhuis te huu x	t 🚺 > Huurwoningen 🗴 🚺 Appartement te 🖂 🗴	🚺 Mijn verhuur adv 🗴 🚺 Woonhuis te huu 🗴 🚺 🕅	Nijn verhuur adv 🗴 🔝 Woning zelf verh 🗴 👔 Log into Faceboo 🗴	🗅 https://images.hii x 😴 W3Schools Onlini x 📰 Tryit Editor v3.6 x 🕇	
← → C ☆ @ https://www.huursector.nl/woning-verhuren/adres				x 🔹 🖌 🛛 🔹 🖄 🖓 🖬 🕾 🔍 🖸 😾 😣 😌	
🛗 Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 🛪					
	M HUURSECTOR	Huurwoningen Huur	sector.nl 🗸 Woning verhuren 🧁 🗸		
	Mome Nieuwe woning a	anbieden			
	Gratis je hu 20.000 voring Postcode 10004	iis verhuren? toosenden per mand 20	towapu ana Vulgendo		
	Popularine staden Haran ia Anderdan Haran Dan Hasa Haran B. Durekt Haran B. Durekt Haran B. Granisen Haran II. Granisen Haran II. Granisen Haran II. Character (J. Barthan M. Barthan C. Granisett 2019 Haranshird, david an P. Workweither an princip (Hottor & Machanin Perg	FUTCON Programmer Weightein Angen Hearting Hearting Verlag petruk Schleren List, Cumpeny nei Listärit Jahouri Helenik deleh Futcher	Hurrnector.nl Contect Woong withoun Ower Haursectord Ower Haursectord Kachtengenoodare		

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

	Woning zelf verhuren Huursector.nl - Chromiur	n	· · ·
🚺 Account H: x 🚺 Mijn verhui: x 🚺 Woning zelf x 🚺 view-source: x 🚺 Huursector: x 🚺 Woonhuis te x 🚺	🕽 þ-Huunwonir 🗙 🚺 Appartemen 🛪 🚺 Mijn verhuur 🛪 🚺 Woonhuis to	🗙 🚺 Mijn verhuur 🗴 🚺 Mijn verhuur 🗙 🛃 Log into Fact 🗴 🗅 https://imag	🗴 🗱 W3Schools 🤇 x 🧱 Tryit Editor 🖓 x 🚻 JSFuck - Writ x 🕂
← → ♂ ☆ 🔹 https://www.huursector.nl/woning-verhuren/details			🚖 📬 🖌 🖾 🔹 🖄 🐜 🕾 🖄 Q 🔝 🕁 🕹 🖂 😣
III Apps @ Debian.org @ Latest News @ Help 📓 slither.lo 🛷 <			
	Aleen JPG, JPG, en PNG bestander, Maximale bestandsgroote is	57 1048.	
	Oppervlakte	Aantal Kamers	
	6 Huurprijs per maand 567 inclusief gas, water en licht	Aantal slaapkamers 1 V	
	Copleverstaat Geneubleerd Gestoffeerd Kaal	Beschikbaar vanaf 2018-08-02	
	Beschrijving		b.
		Ga vezdez	•

Als u nu op "Ga veder" drukt moet u daarna terug naar de webpagina <u>https://www.huursector.nl/account/verhuurder-advertenties</u>. 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.

	Huursector.ni - Chromium	
🖸 Account H. x 🗓 Mijn verhuu: x 🗄 Huursector.: X 🚺 view-source: X 🚺 Huursector.: X 🚺 Woonhuis te: X 🚺 b Huurwoni: X 🚺 v	kppartemen x 📳 Mijn verhuur x 🔛 Woonhuis to x 🔛 Mijn verhuur x 🔛 Mijn verhuur x 📲 Log into Fac-	x 🗅 https://imag. x 🔤 W3Schools 🗆 x 🔤 Tryit Editor 🛛 x 🔡 ISFuck - Writ x 🕇 🕂
← → C △ ® https://www.huursector.nl/account/verhuurder-advertenties/110809		x 🗞 🖉 🖉 🔹 🕆 🐴 🛏 🕾 🖄 Q 📴 😾 😝 😌
🛗 Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 <		
	Upload foto's	•
	Het uploaden van foto's kan eventueel ook op een later tijdstip	
	•	
	Alleen JPG, JPEG, en PNG bestanden. Maximale bestandsgroote is 10MB.	
	Oppervlakte Aantal Kamers	
	1	
	Austral alarmian and	
	Annai siaapkamers	
	567.00 1	
	Inclusier gas, water en licht	
	Opleverstaat Opleverstaat	
	Gemeubileerd 2019-09-02	
	Gestoffeerd	
	Kaal	
	Desetativies	
	beschrijving	
	<script>alert(document.domain)</script>	
	Opalaan	
		 Image: A start of the start of
		•

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)

	Attention Required! Clo	udflare - Chromium 📀 🔿 🗴
🚺 Account H. x 🚺 Mijn verhuu: x 🚺 Attention R: x 🚺 view-source: x 🚺 Huursecter.: x 🚺 Wo	onhuis te 🗴 🚺 þ-Huunwonii x 🚺 Appartemen x 🚺 Mijn verhuu	🗴 🔋 🚺 Woonhuis te: X 🛄 Mijn verhue:: X 🚺 Mijn verhue:: X 📓 Log into Fac:: X 🕐 https://imag:: X 💆 W3Schools 🗄 X 💆 Tryit Editor :: X 🕌 ISFluck - Weil:: X +
← → C △ (# https://www.huursector.nl/account/verhuurder-advertenties/110809		🔅 🗢 🚽 🖬 🔹 🕲 🗮 🖬 🖾 🔍 🖬 😓 😓
III Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 <		
	One means stan	
	One more step	
	Please complete the security check	to access huursector n
	ricuse complete the secondy encert	
	I'm not a robot	
	The fame	
	SUDINE	
	Why do I have to complete a	What can I do to prevent this in
	CADTCHA2	the future?
	CAPICHA?	the future?
	Completing the CAPTCHA proves you are a human and gives you	If you are on a personal connection, like at home, you can run an
	temporary access to the web property.	amevinus scan on your device to make sure it is not intected with malware.
		If you see at so affice or desced naturals you due with the national
		Ir you are at an omice or shared network, you can ask me network administrator for un a scan across the network looking for
		misconfigured or infected devices.
	CloudTare Ray ID: 50%bae71f2d9c3f • Your IP: 185.65.134.178	Performance & security by Cloudflare English
https://www.google.com/inti/en/policies/privacy/		

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.

Account H × Min verhui × M Huursector × M verwissurce × Huursector ← → C △ ▲ https://www.huursector.nl/account/verhuurder-advertenties/110809 Haps Ø Debianorg Ø Latest News Ø Help ▲ sitheric ♥ <	r 🗙 🚺 Woonhuis te >	t 🚺 🏷 Huurwonii: X 📗 App	antanes: x [] Mijo verhus: x [] Mijo verhus: x [] Mijo verhus: x [] Lag into fis: x] Intractional y x [2] VersSchool : x [2] Type Entre : x
	M HUURSEC	TOP _{ML}	Huurwoningen Huursectorni 🗸 Woning verhuren 🧁 🗸
	🔊 Home	🔊 Mijn account	Mjin advertentice
			test test2
			Turug
	Min accourt		Jouw huurwoning
	Mijn advert	enties	Type woning
	? Veelgesteld	le vragen	000
			Woothuis Appartement Kamer Studio
			Upload foto's Het utbodden win foto's kan eventueet ook oo een later Tiirdtin
			Alleen JPG, JPEG, en PNG bestanden. Maximale bestandsgroote is 10MB.
			Oppervlakte

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.

•	Mijn verhuur advertenties Huursector.nl - Chromium				
🚺 Account H.: x 🚺 Mijn verhuu: x 🚺 Mijn verhuu: x 🚺 view-source: x 🚺 Huursector.: x 🚺 Woonhuis te: x 🚺 b-Huurwoni: x 🚺 A	uppartemen: x 🚺 Mijn verhuur: x 🚺 Woonhuis to x 🚺 Mijn ve	erhuur 🛪 🚺 Mijn verhuur 🛪 🛃 Log into Face 🛪 🗅 http	sullimagi 🗙 🗱 W3Schools (🗙 🧱 Tryit Editor (🗙	III JSPuck - Writ × +	
← → C △ 🔺 https://www.huursector.nl/account/verhuurder-advertenties			x) 😋 🖌 🖸 🔹 🖄 🚱 🛏 🖽 🗷	۹ 🖬 🖻 😸 🔴	0 0
III Apps 🔞 Deblan.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 <					
	<u>°</u>	Harrer Fad			
		E123 AMSTEEDAM (f) I ammer Kat			
	Aangeboden wo	oningen *			
b		CS67 AMSTERDAM (B) Tamer Tamer Kal			
Populaire steden Hure in Andreden Hure in On Maa	Huren Huurs Registreren Contact Veelastielde vragen Woning	sector.nl			

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.

C Arcount Lie x C Min verbuis x C Weenbuis tr x C view-seurce x C	Huursertor : x 🕅 Woonbuis tr. x 🕅 tvi	woonnuis te nuur in Amsterdam, voor 567.	x Whenhuis to x	Chromium Mile verbus: x Mile verbus: x Mile into Fac. x D http://	sulfman x 2 WiSchools (x 2 Thill Editor (x 2 B) (Shirk - Writ x 2 +
		and a left when a left when a	a l G House a	C administration a C administration a C administration and C	
C					
11 Abba 6 promitorià 6 pressimenta 6 unite 2 augusto no si		www.huursector.nl says			
		www.huursector.nl		nl 🗸 Woning verhuren 🦲 🗸	
	🜖 Home 🚺 Ar	nsterdam			
	C Terug naar het overzicht				
	Woonbuig in to Ame	tordam			
	Te huar Beachikbaarheid geee	ntroleerd: 4 minuten geleden		Bewaar als favoriet	
	Angelosten und: 4 minuten Beschrijving	picter.		ES67 Tearring for reason To the set To the set Contact met de verhunder Plan een beschligtig Reageer op deze woning To nop Jeast	
	Kenmerken Foto's	Kaart			
	1	Status	Beschikbaar (te huur)	roon op kean	
	2	Aangeboden sinds	02-09-2019		
	3	Beschikbaarheid gecontroleerd	4 minuten geleden	Delen	
	4	Laatste prijs	€567 p/m	Is deze woning al verhuurd of is de vermelding	
	5	Type aanbod	Woonhuis	incorrect? Vertel het ons	
	6	Straatnaam	Postbus	-voningeenmenic iliuurur	
	Aantal kamers	1			
Huursector.nl	Annal descioners				Toevoegen aan beginscherm Annuleren
Processing request	Alerral changements				

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 <u>https://www.huursector.nl</u>.

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.

	Huurwoningen & Kamers Huursector.nl - Chromium 🗢 🔿 🗴
🔝 Mijn verhuur advertenties 🛛 🗶 Huurwoningen & Kamers 🗴 🕂	
← → C △ 🕯 https://www.huursector.nl	x) 🔍 🖻 🐘 😘 😘 🖕 🖬 🖕 👘 👘
🛗 Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 < 🚺 da	
	×
	Inloggen bij Huursector n
	mogger bij natisetor.m
	4 Lords and Shahada
	G Login met Gmail
	Inloggen met je e-mailadres
	E-mailadres
	Washhwoord
	Wachtwoord vergeten?
	Heb je nog geen account? Registreren
AURSECTAL	

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

Burp Sulle Professional v2.0.11beta - Temporary Project - Incensed to martin	* x
Burp Project Intruder Repeater Window Help	-
Dashbaurd Target: Jimose Intruder Repeater Sequencer Decoder Comparer Extender Project options User options USEP SOX Beautifier SAAR, Raider Certificates Upload Scamer Desenialization Scamer Java Smallad Paylobadk psycholatin Logger++ AutoRepeater Autorise	
Intervent HTTP history WebSockets History Options	
/ 🙆 Request to https://www.huorsector.nl/43 (104.20.59.169)	
Forward Drop intercept is on Action	•?
Raw Parary Headers Headers	
۲۲ //۱۰۵۵pps//hebs/stread/#197/.1 Some-Space (Lanz) And Some Stread (Lanz) And Some St	
hter:	
)
0 < + > 1%/b1 0r	natches

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.

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to martin	
Burp Project Intruder Repeater Window Help	
Dashbaard Target Jimme Intruder Repeater Sequence: Decoder Compare Extender Project options User options CSBF CO2 JSON Beauchier SAME Raider Certificates Upload Science: Java Senalized Payloads psychopATH Logger++ AutoRepeater Autorize	
Internet http://websoluti.http://we	
/ 🙆 Request to https://www.huurnettor.ri/443 [104.20.59.169]	
Forward Drop Intercept is on Action	ant this item 🔷 🕐
Raw Param Heades Hex	
OUT /inlogen/facebook_extendedsteat=dframe=HTP/1.3	2
Hell (Marcheles) Hell (Marche	#23/279420949630;
b	
	2
	0 matches

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to martin			*) (X)
Burp Project Intruder Repeater Window Help			
Dashbard Target Teme Sequence Decoder Compare Extender Project options User options CSPF C02 [SON Beaching SAME, Raider Centificates] Upland Science] Java Serialized Psyloads [psychaPATH] Logger++] AutoReparter Autorize			
Internet Int			
A Request to https://www.huursector.nl+43 [164.20.59.169]			
Forward Drop Intercept is on Action	Comment this item		0
Raw Parans Headers Hex			
GT /inlogen/gools_stands@tstands@tstands/ftsta			1
Connections close			- 1
Unge down intervent Frequencis A Under Agnetic NovalliAys,50 (21): Linux X00,64) AppleWebRity537.36 (100ML, like Gecko) Chromy72.0.3080.75 Safari/537.36			- 1
accept: text/min.upplcetcom/min.em_pulcetcom/milgen/wep_image/appg_/*jequive Beferer: https://ww.harsetcom/milgen/wep_image/appg_/*jequive Beferer: https://ww.harsetcom/milgen/wep_image/appg_/*jequive			- 1
Accept-Enrosoms; spire, derikate Accept-Language: en-US-Ansigne0.0,012(ept.)			- 1
	ZiNiZiPerzzkzTPezQPi	dMSJ9;	
_secial: 2.57562080.15001021; gitcal: 2.6023807.150001021; high=sitcae-1306-407b-427b-427b-66080(cb7%; hrstr regen; h user tree 3109-23bc5c004f0caubaaranteexpectations/and/superior scheduli is used interpret animyter is interpret animyter interpret animyter is			
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx			
b			
			- 1
			- 1
		0 ma	tches

Je krijgt dan een redirect naar de hoofdpagina.

Burp Project Intrudyir Apparter Window Help
Databased Target
Intervent HTTP httery websctwh httery Sptem
sepante from https://www.huursettor.nl+43/reloggenfacebook_extended [104.20.59.169]
Forward Drop Intercept is on Action Comment this item 🌳
Rine Jeaders Hee Inth, Rander
TP/1.1 302 Found
tak Mon, do sep 2010 11:4:1:3: defi montrilypei textfield, character/DF 8
ennectan: close dueControl: no-cache, private
- /ailgu: driet (starting new WW connection) action: https://doi.org/logi.com/action/acti
et-cookie: SMP-Tobew-yobitstkuthudolheterkileKinsklusceststandhwltjait#EbbitstkuthudolheterkileKinsklusceststandhwltjait#Ebbitstaitzistait/jtait#Ebbitstaitzistait/jtait#Ebbitstaitzistait/jtait#Ebbitstaitzistait/jtait#Ebitstaitzistait/jtait#Ebitstaitzistait/jtait#Ebitstaitzistait/jtait#Ebitstaitzistait/jtait#Ebitstaitzistait/jtait#Ebitstaitzistaitzistaitzistaitzistait/jtait#Ebitstaitzist
et. coasis in humsestant) sessionmybit (EndelsmuthusPathy)vedendaset(BSP3151abber(1)s12Fe125eh2200)/(aph/0mequ/Lesmber(1)s
n; men empranzio, partici menta in unenta in unenta per et el man in unenta in unent
rver : Court can F. Aris S138-06-07.01/17335-AMS
Lantont-Length: 376
00CTPP indu- table
- Onido wata dariater/UF-67 />
<pre>seta http-equiverefresh* content=*curl=https://www.huursector.nl?togin=1* /></pre>
<pre>stiluomdirecting to https://www.bwursector.al/logimi</pre> //iil/> //www.bwursector.al/logimi
dody Bedierelina ta us brefehttes //our humantes all/lasimel*altada/our humantes all/asimele/on

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.

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to martin	
Burp Project Intruder Papeleter Window Help	
Dashbard Target Termet Termet Neonater Sequence Decoder Compare Extender Project options User options (SRF CO2 JSON Beautifier SAML Raider Cetrificates Upload Scanner Deserialization Scanner Java Serialized Phyloads (psychopATH Logger++ AutoRepeater Autorize)	
Recordent HTTP history WebSockets history Options	
Besponse from https://www.huursector.nl/443/htopin=1 (104.20.59.169)	
Forward Drop Intercept is on Action	• ?
Raw Headers Hex HITM, Rander	
<pre>«option values*100* x41.560*/option></pre>	2
<pre>explice value=1700 val.98/option= explice value=2000 val.98/option=</pre>	
<pre>weption value="1500" >42.500" /0.500" /or ion></pre>	
<pre>aption value=3000 H3.0000/ptitlm aption value=3000 H3.0000/ptitlm </pre>	
<pre>«option values*4000* >d4.000*/option></pre>	
<pre>soption value*'.'* selected-Geen maximum-/option></pre>	
dabel classes floating-labels for standardis tota/labels	
div class for groups	
-button class="btm btm-primary btm-block">	
zek ess flasstion extra selli v Monthto / Association	
spath ds 1923.7, 20.7.19, 16.1-0.2-0.2-0.5-0.3-0.8-0.3h-0.821.3-1.7, 2.1-3.	
94.4,9.7,9.7,9.70,2.3,0,4.3=0.8,6-2.140.800.0.3,0.1,0.6,0.4,7.4,720.4,0.4,1.2,0.4,1.4,0(1.3).1.3	
Care 1, 21, 39, 24, 1, 21, 24, 24, 7, 20, 75, 76, -3, 30, -6, 27, -6, 06, -3, 3, 27, -0, 0, -05, 3, 30, 0, 27, 7, 0, 0, 15, 7, 15, 75, 79, 71, 15, 75, 79, 70, 75, 75, 75, 70, 75, 75, 75, 75, 75, 75, 75, 75, 75, 75	
«/div»	
	1
africidaes	
<pre>«/outo //hadet></pre>	
<pre>div class=latt alert-damper' folg="alert"> div class=latt-damper' folg="alert" div class=latt-damper' div</pre>	
dution type=buttor class=close_alert aria-label=close>	
0K	
facebook_extended&testmciframer_wordt niet ondersteund.	
N	
<pre> <pre>cutic(science**</pre> 6</pre>	
with Classification (1-5)'s	
do: class=text-primary text-centert=me werkt Huursector.nlt	
<pre>«div class="row mt-5"></pre>	
<pre>div class=coind.3 offset.se Coind offset.3 text-center'> control = 0.0156 offset.</pre>	
db5 class="nt-5">Maak een gratis profiel aan	
eportul je unommensen en je maximale budget in«/p>	
<pre>4/01/> div_class="col.md-3 offset-3 text-center"></pre>	
<pre>sing class="ing-fluid" data-src="https://www.hoursector.ml/images/zoom-watch.svg" src="data:image/png:baseda.ivDDexDCQpAAAADEAAADECXTAAAAE/DQBAAADEAAADECXTAAAAE/DQBCSXTBAAADECXECVTAAAE/DQSTwataABDCQEVyQtmP4+u37fwtlqAPiazuiCAAAAEDAUSErk/gggm=" alt="vind je droombuis"></pre>	
chi classified SYMD ye dreambase/https://doi.org/initiation/chi.classified/classified	
4/div	
<pre>cdiv class=col-ad.3 offset-im-0 col.6 offset.3 text-center'></pre>	
class training - tr	
eng qemakkelijk contact met de aanbieder van het buurhwis	
<pre>cluster classes cal.mb.3 difeat.sn.0 cal.s. difeat.s Text.conterts</pre>	
<pre>cimp class="imp-fluid" dita-src="https://www.hourisector.nl/images/zoom-relax.weg" src="data:imap/pog:baseda.iVDPwCKGppAAAMMUAAMAUAAAAAACXAAAAFCSDAAAAADCXAAAAFCSDAAAADDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaCDAEDQUIseDeut37FaaAaADCAEDQUIseDeut37FaaAaACDAEDQUIseDeut37FaaAaACDAEDQUIseDeut37FaaAaADCAEDQUIseDeut37FaaAaACDAEDQUIseDeut37FaaAaADCAEDQUIseDeut37FaaAaADCAEDQUIseDeut37FaaAaACDAEDQUIseDeut37FaaAaADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaaAAADCAEDQUIseDeut37FaAAAADCAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
4th class="nt.5"-MeLaxt+/https	
c/patienes de koriste keren met je voeten omnog in je nieuwe muirmits	
div classifree at-5 recent-restals/>	
0 < + > Type a search term	0 matches

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 <u>https://www.huursector.nl/account</u> gaan.

		Account Huursector.nl - Chromium				(*) (*) (*)
Acco x II Mijn x II Woor x II Acco x II view x II Huur x II Acco x	Do Hu X Moor X Appa X Appa	n x 🚺 Mijn x 🚺 Woor x 🚺 Mijn x 🚺 Mijr	🗙 👔 Log i x 🗅 http: x 🔤	W3S: X 🛛 🌉 Tryit X 🛛 🏭 JSPuc	× 🚺 Woor × 🚺 Huur × 🚺 Woor ×	Mijn x Mijn x +
G G Debianorg Australia News Help Sither.io S					ж 4 м 19 е с 44 е	
	b (UUUDCECTOD			A		
	HI HOURSELTUR	Huurwoningen Huurs	ector.ni 🗸 Woning vernuren	🥌 ×		
	🜖 Home 🚺 Mijn account					
		pizza kwaak				
	~	Persoonlijke gegevens		Bewerk		
	Profielfoto wijzigen	Naam	pizza kwaak			
		Geslacht	Man			
	Mijn account	E-mail adres	dummy6@zeelandnet.nl			
	~	Telefoonnummer	0612345678			
	Mijn huurdersprofiel	Geboortedatum	2000-01-01	Þ		
	Mijn zoekopdracht	A days	2000 01 01			
		Adias	1000AA			
	Mijn favorieten		Amsterdam			
	Mijn accounttype					
	U					
	Veelgestelde vragen	E-mail notificaties		Bewerk		
		Ik wil graag dagelijks een update van recent aa	nbod op basis van mijn zoekopdracht.			
	Nog vr. Lees de Fi	agen over Huursector AQ waar de meestgestelde vra	nl? gen beantwoord wor Ga naar de FAQ F	den.	Pers	portijke gegovens zijn Izgal

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

•	Account Huursector.nl - Chromium	* * x
1 Acco x 1 Mijn x 1 Woor x 1 Acco x 1 Huer x 1 Acco x 1 Huer x 1 Acco x 1 b Hu x 1 Woor x 1 Acco	x 🚺 Appalix 🚺 Mijni x 🛄 Woor x 🛄 Mijni x 🛄 Mijni x 📳 Mijni x 📳 Logi x 🗅 http: x 🗮 W3S: x 💭 Tryiti x 🔡 TsPu: x	Woor x 🚺 Huur x 🚺 Woor x 🚺 Mijn x 🚺 Mijn x +
← → C ☆ @ https://www.huursector.nl/account		* 🖏 🖌 🖸 🔹 🕸 🙀 🛏 🕾 🖪 🤤 😾 😝 😝 😖
III Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 🧾 slither.io 🛷 <		
	pizza kwaak	·
	Persoonlijke gegevens	
Prodelikate wijzigen	Naam	
	pizza kwaak	
	Geboortedatum Geslacht	
Mijn huurdersprohel	1 🗸 jame 2000 V 🧭 Man 💽 Vrouw	
Mijn zoekopdracht	Adres	
Mijn favorieten	1000AA 1 test	
Mijn accounttype	E-mail adres	
Veelgestelde vragen	dummy8@zeelandnet.nl	
	Telefoonnummer	
	0612345678	
	Anzaileren Opalisan	
	E moil potification	
C A Deserver Average Andre Sourcer Material Bedressana Manage Analisia Secular MTTDI Exception Self-Information	E-IIIdii HOUIICdiles Bewerk	
Al U. Service and a service a serv		Styles Computed Event Literess DOM Besigners Properties IP Fare cleans.style () body (and Literess, tables)
 Australian Sull'Australian Sull'A		service the service of the serv

•	Account Huursector.nl - Chromium				v A 8
L Acco x L Min x L Woor x L Acco x L View x L Huur x L Acco x L DHu x L Moor x L Appl x L Appl x L A	pa x 🚺 Nijn x 🚺 Woor x 🚺 Nijn x 🚺 Nijn	× 🛛 🛃 Log i × 🗎 🗅 https :	K 🛛 🗱 W3S: X 🗍 🧱 Tryit 🛛 🔡 JSPU	× 🛛 Woor × 🖾 Huur × 🖾 Woor × 🖾 Nijn	× Mijn × +
← → C △ ê https://www.huursector.nl/account				🖈) 🖏 🥖 📴 🔹 🖄 🚱 📼 🗷	Q 🖸 🛱 🥘 \varTheta 😌
🛗 Apps 🝳 Debian.org 🝳 Latest News 🝳 Help 📓 slither.lo 🛷 <					
	pizza kwaak				
	Devree en lijke gegeveng				
	Persooninjke gegevens				
Proheiloto wijzgen	div.form-group 350×54				
0	pizza	kwaak			
Mijn account	Geboortedatum	Geslacht			
Mijn huurdersprofiel		C Mag	O Marine		
A	1 Jame 2000 V				
Mijn zoekoparacht	Adres				
Vijn favorieten	1000AA 1		test		
Mijn accounttype	E-mail adres				
P Veelgestelde vragen	dummy6@zeelandnet.nl				
	Telefoonnunmer				
	0612345678				
		Annale	Ominan		
	E-mail notificaties		Bewerk		
G D Benerits Conside Audits Sources Network Performance Memory Application Security HTTPS Everywhere EditThisCostie					01 X
<pre>v=div=class='inline-box' data-type='basics'> v=div=class='inline-box' </pre>				* Styles Computed Event Listeners DC	OM Breakpoints Properties IN
 od class "wite" un/do od class "wite" un/do 				Filer element.style {	:boy .cls +
 odiv class="row at-3">/div odiv class="row") form white form - form-control (anal (ration, rss. dr54ee42650-3
* div class-"col-12 col-ad-6"> * div class-"col-12 col-12 c				font-family: Bockwell Std.serif; beckground.color: #75374;	BOLISSION STATESCONDER/
*-div id+'first name.container' class='input.container'>				padding: + .937Sree;	
 support class, removatives, type, text, water class, call? 10-TLSE_MME: Value: pLD21 required pLACEMER*TWOMAAM (FAMALY on 10				.form-control[readonly] { outline:+ 0; ber-shadow: none; berder.color:+ []transparent;	amplication.css.dc54ee42#b42:1
 -intr (tars-roll.2) edual-6- vint (tars-roll-party) -vint (tars-roll-party) -vin				} .form-control(disabled, .form- control(readon)y) { backgrouw color- opacity: 1: }	peolication.css_dc54me42#Bd2:3
cititius cititus tend body account div contact with account of resi-12 mi5 mis-5 div and div col resi-12 col-6-8 div tab. Term while form while form similar editable basic-efformation form initialized inline-edit. Bell	tet divinine-box dilbasics dd.edit div.rew div.col-12.col-md-6 div.lom-	roup divelinit name-container.input-conta	aner inputifirst_name.form-control	.form.control {	application.css.dc54ee42#942:3

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.

	Account Huursector.nl - Chromium			* * X
Accol X II Mijn X II Moor X II Accol X II View X II Huur X II Accol X II biHu X II Appl X II Appl X II Appl	N X Nijn X Woor X Mijn X Mi	in x 🔣 Logix 🗅 https x 🔤 W	/35: x 📰 Thyit x 🏭 JSFu: x 🚺 Woor x 🚺	Huur x 🚺 Woor x 🛄 Mijn x 🚺 Mijn x 🕂
← → C △ iii https://www.huursector.nl/account			÷ 📬	🖌 🖸 🔹 🦓 🛏 🖱 📓 Q 🖸 📅 🗉 😁 😌
III Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 <				
	pizza kwaak			
	Persoonlijke gegevens			
Produktore wijstgen	Naam			
Min account	pizza	kwaak		
	Geboortedatum	Geslacht		
	1 🗸 jann# 2000 🗸	Man 😲	Vrouw	
Mijn zoekopdracht	Adres			
Mijn favorieten	1000AA 1	test		
Mijn accounttype	E-mail adres			
Veelgestelde vragen	dummy6@zeelandnet.nl			
	Telefoonnummer			
	0612345678			
		Annuleren	Opsiaan	
	E-mail notificaties		Bewerk	
Dements Consile Audits Sources Network Performance Memory Application Security HTTPS Everywhere EditThisCookie				01 ; X
<pre>* dfu class='islow-box' data-type='basics'> * d0 id='basics'></pre>				* Styles Computed Event Listeners DOM Breakpoints Properties 34
<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	R			element.style {
> ofiv class="row nt-3"s="/dtvs + ofiv class="row">				*, safter, sbefare { <u>Boolication.css.dc54ee420942:3</u>
<pre>widiv class="col-12 col-ad-6"> widiv class="col-12 col-ad-6"> widiv class="col-12 col-ad-6"> </pre>				bex-sizing: border-bex; }
votiv instrust_name-container' classs'input-container's classs 'form-control' type:'text' name'first_name' ids'first_name' value'pizza' repliced placeholders'Wormaan's				div (display: block;
<pre>cspan class="message empty"> (/disp</pre>				bitested from body-account
 vertices vertices 				body (
*-01V Class**for=_prop>				font-family: Gotham Book, sams-serif; font-size: lree;
in Processing and consider consistent (part consistent in an inter-last name) as the "head," required placeholders'Adversam's const class'message empty://sistence.inter-last name' as the clast name inter-last name' as the clast name inter-last name inter-last name.				Test-weight: 400 ise-beight: 1.5: celor: M#22259: test-65gs: Left:
html body account div container div row section my-account.col-md-12 m5-mb-5 div row div col-md-12.col-ig-8 div/lab form.while-form inner editable basic-information.form initialized mine-edit febb	et div.inline-box dilibasios dd.edit div.rew div.col-12.col-md-6 div.lon	n-group divillant_name-container input-container		background-color: @#fff;

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".

	Account Huursector.nl - Chromium		· A 8
C Acco X C Min X Moor X Acco X Moor X Acco X	apa x 🚺 Mijn x 🚺 Woor x 🚺 Mijn x 🚺 Mijn	x 🚺 Log i x 🗅 http: x 🗮 W3S: x 📰 Tryit x 🔛	SFu: X 1 Woor X 1 Huur X 1 Woor X 1 Mijn X 1 Mijn X +
← → C () ■ nttps://www.nutrsector.ni/account # Anos @ Debian.org @ Latest News @ Help ■ Sitter in @ ≤			x 4 . U 4
10 bibs (armenik (armenican (cosh a second or)			•
	pizza kwaak		
	Persoonlijke gegevens		
Prode/flote wijstgen	Naam		
Min account	test	test2	
	Geboortedatum	Geslacht	
	1 🧹 jama/ 2000 🗸	Man 😯 Vrouw	
Mijn zoekopdracht	Adres		
Mijn favorieten	1000AA 1	test	
Mijn accounttype	E-mail adres		
Veelgestelde vragen	dummy6@zeelandnet.nl		
	Telefoonnummer		
	0612345678		
		Annuleren Opsiage	
	E-mail notificaties	Bewerk 🕥	
Benents Consite Audits Sources Network Performance Memory Application Security HTTPS Everywhere EditThisCookie HTTPS Everywhere EditThisCookie			94m Converted Event Literary DOM Residences In Security III
 And the first field of the first head of thead of the first head of thead of the first head of the first he			The second secon
	tiet div.mino-box diPlasics dit.edt div.row div.col-32.col.ed66 div.hom-	group diviliast_name-container.anput-container	fet-weight; 40) Lise-beight; 35 color: M22250 text-algo: Left: becomprod-color: Diff:

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

		Account Huursector.nl - Chromium			
C Acco: x C Mijn : x C Woor x C Acco: x V view x C Huur x C Acco	o x 🚺 b Hu x 🚺 Woor x 🚺 Appa x 🚺	Appa × 🚺 Mijn × 🚺 Woor × 🚺 Mijn ×	🚺 Mijn 🗙 🛃 Log i 🗙 🗅 http: 🗙 🧱	W3S: x 🇱 Tryit 🛛 x 🏭 JSI	Ruc x 🚺 Waar x 🚺 Huur x 🚺 Waar x 🚺 Mijn x 🚺 Mijn x 🕂
← → C △ @ https://www.huursector.nl/account					🖈 🗣 🖌 🖸 🔹 🖄 🚱 🔤 🕾 🤤 💆 😸
III Apps @ Debian.org @ Latest News @ Help 📓 slither.io 🥓 <					
	M HUURSECTOR			😩 ~	
	NL NL			•	
	🕥 Home 💿 Mijn account				
		test test2			
		h			
		Development 1991 and and a			
		Persooniijke gegeve	ens	Bewerk	
	Probelfoto wipzigen	Naam	test test2		
		Geslacht	Man		
	Miin account	E-mail adres	dummy6@zeelandnet.nl		
	U		0.0007.05.070		
	Mijn huurdersprofiel	leteroonnummer	0612345678		
		Geboortedatum	2000-01-01		
	Mijn zoekopdracht	Adres	Postbus 1 test		
	Miin favorieten		1000AA		
			Amsterdam		
	Mijn accounttype				
		E mail notification		1	
	Veelgestelde vragen	L-man nouncaties		Beweik	Persoonliike gegevens ziin
		Ik wil graag dagelijks een update van	i récent aanbod op basis van mijn zoekopdracht		gewijzigd
					ок
Image: Conside Audits Sources Network Performance Memory Application Security HI c1dectype htmls c dectype htmls	ITTPS Everywhere EditThisCookie				Styles Computed Event Listeners DOM Byvainvaints Evenueties in
-html Lang-inL's +-head itenscope itentype="http://schema.arg/WebSite">== <th></th> <th></th> <th></th> <th></th> <th>Fitter :boy .cls</th>					Fitter :boy .cls
<pre>www.booy.class-account_data.restricted- == s0 et Google Tag Manager (noscrigt)> </pre>					elesent.style (
<pre>store End Google Tag Banager (rescript) -> > toeder class' imall'></pre>					body (<u>Boolication.css.dc54ee42d5</u> Bis-beight: 200vh;
+ ofiv class="alert alert-success" role="alert">~//dix> + ofiv class="breadcrunk d-nese d-sm-block">~//dix>					position: relative:
+-div class-'header-lessee-profile canvas dark-gray'>=-/div +-div class-'container'>=-/div-					body (application.css.dc54ee42db margin: + 0;
<pre>> div class='canves'>=> <fcoters=< footers<="" pre=""></fcoters=<></pre>					font-family: Gotham Book.sams-serif: font-size: iree:
 Norvise screet-re-tep tercer more sover w//div Script type://application/javascript/w/script Norvise/teps/mode/index/soverise/index/sove 	section laste adal label's cities				Line-height: 2.5; celor: ##212529;
• div class-model hide id- submittation-signup-model tabindes-if rove-wideled aris-labelledby-suffic- series twee-modelation/invaries succession.signup-model tabindes-if role-dialog aris-labelledby-suffic- series twee-modelation/invaries succession.signup-model tabindes-if role-dialog.	hentication-signup-model-label ">>>/div>				text-align: left; background-color: □#fff;
+ -script type-"application/jewscript"/script-					 * safter, :before {

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

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

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

<u>B</u> estand Be <u>w</u> erken Beeld <u>G</u> eschiedenis Bl <u>a</u> dwijzers E <u>s</u> tra <u>H</u> elp		000
🖸 Drago 🐠 👮 Slack 🐖 🛛 03RRjNG 🛛 🚱 acctivity 📄 DB Fiddle 🖉 WWASP Mod. 🔤 HTML in	ifn 📑 Thylt Edic 🕒 Peplace 🛛 🗮 MySQL B 📓 Online ja hackoolipse 📓 Woonhau 📓 Huurses: 📓 Account 1 📓 Woonhau 📲 Favorieta 🕝 reflectes 🛛 📳 DNSdam 🕝 intextiou 🖌 XSS Hum 👿 Klacht 🗙 📓 Account 1 🚳 Sikkom a	G blind xss +
(→) C () Nttps://www.huursector.nl/klacht		a 🔗 (S) 😑
	Rome Kischtenurgodure	
	Klachtenprocedure	
	Hoe dien ik een Vlacht in?	
	Bij het indivene van de klacht, dienen wij te weten waar de klacht over gaat zodat we je goed kunnen helpen.	
	Heb je een klacht over	
	contact met een aanbieder	
	een huurwoning of het huuraanbod	
	Ib Huursectorni account	
	Lees onderstaande informatie goed door, alvorens je klacht in te dienen.	
	Contact met een verhuurder	
	Huursector.ni verzameli het aanbod van alle beschikbare huurwoningen in Nederland Huursector.ni hungeert hierbij als een zoekmachingkektronisch prikbod en is dus hiel de verhuurder.	
	Wij kunnen geen garanties geven dat een verhuurder reegeert of aan u wilt verhuren. Wij bemiddelen niet.	
	Omdat momenteel er een enorme krapte op de huurwoningmarkt is komt het voor dat sommige verhuurders veel reacties krijgen en daarom	
	niet op alles reageren. Dit vinden wij verwelend maar het is aan de verhuurder om te bepalen wie en hoe hij natwoord op reacties. Wij zijn geen verhuurder en bemiddelen niet maar proberen verhuurder en huurders bij elikaar te brengen door het aanbod te verzamelen van	
	huurwoningen.	
	Het woningaanbod	
	Doorniddel van onze unieke zoektechnologie vergroten wij de kansen van woningzoekenden. Je bespaart veel tijd door niet zelf allerlei webvilste te hoveren doorzenken en onwande denersonaliseerente undetse met hetschikbere buiturenen innen Hierdoor	
	sneller en eerder dan andere geintereseerden reageren op het nieuwste woningaanbod.	
	Foute vermelding	
	We deen ons ulterste best om te zorgen dat alle informatie correct is en actueel, ondanks dit streven kunnen wij niet garandeten dat alle	
	micromaue auto comprese toutoons is, wiji upoatein de website meerdeek keren per dag om te zorgen voor een zo actueel mogenipe informatie, aasto nze eigen inspanningen om alle informatie correct te houden zijn wij och afhankelijk van hoed e aanbieder de informatie	
	doorgeeft.	
	Mocht je een foutje ontdekken? Dan kan je dit melden vanaf de website of ons contacteren via support@huursector.nl, hiermee help je ons de informatie accuraat te houden.	
	Geen woning gevonden	
	Huursector.nl bled dus de mogelijkheid om efficient een woning te zoeken en dat is wat onze dienst inhoudt. We kunnen dus niet	
	garanzeren dat u een nuurwoning zuit vinden. Dit is aimankeijk van uw specifieke woonwensen en de eisen die verhuurders stellen. Je bepald helmenal zelf weike isen je stelt aan een huis. Vind je geen huurvoning? Prober je zoekkorfofiel aan te passer want mischien is er	
	geen aanbod wat aan jouw vereisten voldoet beschikbaar.	
	We zullen ons best doen om zoveel mogelijk geschikte woningen te vinden die aan jouw zoekprofiel voldoen.	
	je account	

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)

Kachtenprocedure Huurnector.nl - Pirefex Developer Edition					* * X			
Bestand Begerken Begeld Geschiedenis Bigdelijzers Egtra Help Image:	🗃 HTML if:: 📑 Tryit Edi: 🔶 Replace : 🚞	MySQL II 🛛 🖬 Online Jo 🛛 hackoclipse 🔛 Wac	anhui 🔛 Huursect 🔛 Account i 🔛 Waanhui	📓 Favoriet: 🕲 reflected 🛛 🚺 DNSdum 🕲 inte	xthu 🖌 XSS Huni 🔢 Klachi 🗙 📗	Account		
Heb je en klacht die over lets ander gaat dan het bowardsandel? Neen des contact op met ons doreren ernal te sturen naar isotoret it hussender of valut onderstanden formulier in Mo tudien van letter kat zu is in bekendeling opene.								
	apportentational		South 2.2.11. In personality remain.					
		5 C						
	test		test					
	0612345678		bl4ckh4ck5greybox@mailinator.com					
	Contact met een verhuurde	r		~				
	kiacm-kiacm							
A								
				4				
			Verstuur					
	Huren in Amsterdam Huren in Den Haag	Registreren Veelgestelde vragen	Contact Woning verhuren					
	Huren in Rotterdam Huren in Utrecht	Hoe werkt het? Huurtips	Voor makeiaars Over Huursector.nl					
	Huren in Einanoven Huren in Groningen							
	© Copyright 2018 - 2019 Huursecto Voorwaarden en privacy Notice &	x.nl, dienst van PC Internet Ltd. Company no. LL15: i takedown Responsible Disclosure						

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.

N	Naam= gemeld via e-mail, één r aan: Support <support@huursec< th=""><th>ninuut geleden (ma., 2 sep. 2019 om 2:57 PM) :tor.nl></th><th>2 7</th></support@huursec<>	ninuut geleden (ma., 2 sep. 2019 om 2:57 PM) :tor.nl>	2 7
		Hallo	
	klacht=klacht		
	Naam	naam= naam	
	Telefoo nnumm er	0612345678	
	E-mail adres	bl4ckh4ck5greybox@mailinator.com	
	Туре		

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)

	Woonhuis te h	nuur in Amsterdam, voor 784.00 p/m Huursector.nl	I - Chromium	× • ×
Huursector.nl × 🔣 Woonhuis te huur in Amstri × 🔛 Huursector.nl	× D data:text/html base64,PHI × 🔜 W3Schools	Online Web Tu: × 🔤 Tryit Editor v3.6 ×		
← → C ☆ a https://www.huursector.nl/huren/112003				🖈 🐂 🕖 🗶 🤷 😡 🗵 🧶 Incognito 💮 🥥
🔎 Debian.org 🧧 Latest News 🔴 Help 📓 slither.io 🛷 < 🔢 da				
	🕖 Home 🕥 Amsterdam			
	Laat de aanbie	eder weten dat je geïntere dit huis in Amsterdam	esseerd bent in:	×
werkdagen een follow-up berichtje sturen. Tip: reageer zo uitgebreid mogelijk in correct Nede	rlands en beschrijf je persoonlijke situatie wat be			
institut(p)-strong(p)>				
Min huurdersprofiel meesturen				
				Verstuur
Uw reactie word direct naar de aanbieder gestuurd. Huursectorn	I bemiddeld niet in het onderlinge contact en heeft als zoekr	machine geen invloed op de reactiesnelheid van de aanbie	rder of de gunning van woningen.	
	Type aanbod	Woonhuis		
	Straatnaam			
	Aantal kamers	4	Woningkenmerk 112003	

je krijgt nu een bevestiginging dat het bericht is verstuurt.



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

	Reactie op te huur st	aande woning Postbus - Inbox - dummy&@zeelandnet.nl - Mozilla Thunderbird		· · · · · · · · · · · · · · · · · · ·
🖄 Inbox - dummy6@zeelan: 🛛 Reactie op te huur stan 🗙				0 0
Get Messages V Vitte V Chat & Address Book O Tag V V Quick Filter		Q, Search <ctrl+k></ctrl+k>	=	Events < > ×
From Huursector.nl <noreply@huursector.nl>☆</noreply@huursector.nl>			Beply → Forward Archive & Junk Delete More More	4 Wed (o)
Subject Reactie op te huur staande woning Postbus			9.56 AM	5ep 2019 CW 36
my6@zeelandnet.nl>★				Co New Event
To protect your privacy, Thunderbird has blocked remote content in this message.			greferences ×	> Tomorrow
		그는 것이 없는 것이 같은 것이 같은 것이 없는 것이 같이 많은 것이 같이 많을 것이다.		Upcoming (5 days)
		Hallo		
	testtest			
	strong			
	₽			
		Woningdetails:		
	Lifes	Posthus aaaa		
	Partos	100046		
	Postole	Amatadam		
	Pilants	Anserdam		
	Buun	704.00		
	Prijs	784.00		
		Generate seturator		
		Orgenera darinager		
	E-mail adres	dummy60@zeelandnet.nl		
	Telefconnummer	0629907059		
	Veelges	stelde vragen Contact Over Huursector.nl		
	Huursector.nl	Like ons op Facebook		
	Huursector.m is een pro	duct van: PC Internet LTD Postadres: Boulevard Saint-Michel 47, 1040 Brussel, België		
Thunderbird now contains calendaring functionality by integrating the Lightning extension.			Learn more	Disable Keep X
M				(1) Today Pane v

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

Reactie op te huur st	taande woning Postbus - Inbox - dummy6⊜zeelandnet.nl - Mozilla Thunderbird		· · ·
Indox - ournimyogyzeetan: Wikacce op te nuur stall X Wikacce op te nuur stall X	0 court and an	Franks	
Construction of the Argentic Synamous above Orag & Broade when	C Station Activities	evens	
Subject Reactie op te huur staande woning Postbus	Propy Freeman Encode Program Board Program Boa Board Program Board Progr	4 Sep 20:	19 CW 36
Reply to Commy60@zeelandnet.nl> 1		2 New Event	
hy6@zeelandhet.nl>		# Today	
To protect your privacy. Thunderbird has blocked remote content in this message.	greferences ×	 Tomorrow Upcoming 	(5 days)
phishing mail link:			
\$			
Thunderbird now contains calendaring functionality by integrating the Lightning extension.	Learn more	Disable	Keep X Today Pane V

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 **september** er achter dat als u een bericht stuurt in het contactformulier op de webpagina <u>https://www.huursector.nl/contact-vragen</u> 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 <u>https://www.huursector.nl/contact-vragen</u>.

		Contact Huursector.nl - Chromium		* * *
Contact Huursector.nl x 💠 Huizenmarkt.nl x +				
← → C △ iii https://www.huursector.nl/contact-wagen				* 🖏 🖉 🖉 🔹 🤹 🗞 🖬 🖉 🖉 🖬 😁 😁
10 Apps (e bestanoid) (e catest news (e net) a situetto an e				2
	M HUURSECTOP _M			
	🔊 Home 🔕 Contact			
		Contact		
	Heb je een vraag over het gebruik va Vul onc	n Huursector.nl? Lees dan eerst onze Veelgestelde ' iets laten weten? We horen het graag! terstaand formulier in en we nemen zo snel mogelijk	/ragen. Staat je vraag er niet tussen of wil je ons contact met je op.	
			Huursector.nl	
	Þ		Huursector.nl PC Internet Ltd. Postadres: Boulevard Saint-Michel 47 1040 Brussel Beigle	
	Voornaam	Achternaam		
	Onderwerp	E-mailadres		
	Je bericht			
			Verstuur	
	Huursector.ni is een dienst van PC Inte Hoofdkantoor: LOR1029, 2018, Unit No	rnet Ltd. J Company no. LL15246 Labuan, Maleisië. L 5.09 (Office) Level 5, Labuan Times Square, Maleis	sch federaal territorium Labuan, 87000 Maleisië.	
	Huren in Amsterdam	Registreren	Contact	
Huursector.nl				Toevoegen aan beginschorm Annuleren

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

		Contact Huursector.nl -	Chromium		
🚺 Contact Huursector.nl x 🛷 Huizenmarkt.nl x 🕂					
← → C ☆ @ https://www.huursector.nl/contact-wagen					x 🗞 🖉 🖉 🔍 🛪 🖓 🛏 🕾 🖻 🤤 🖯 🖯 😌
III Apps 🔞 Debian.org 🔞 Latest News 🔞 Help 📓 slither.io 🛷 <					
	M HUURSECTOR				
	RL NL				
	Home S Contact				
		Conta	ct		
	Heb je een vraag over het gebruik van Huursect	tor.nl? Lees dan eerst onze iets laten weten? We hor	Veelgestelde Vragen. Staat je vraag ren het graag!	g er niet tussen of wil je ons	
	Vul onderstaand fo	formulier in en we nemen z	o snel mogelijk contact met je op.		
				Huursector.nl	
		-		Huursectorn	
				PC Internet Ltd.	
			3	Postadres: Boulevard Saint-Michel 47	
				1040 Brussel	
		~***		Beigie	
	voornaam= voornaam	ac	chternaam= achternaam		
	onderwerp= onderwerp	da	ummy6@zeelandnet.nl		
	bericht= bericht				4
			Verstuur		
		_			
	Huursector.ni is een dienst van PC Internet Ltd. C Hoofdkantoor: LOR1029, 2018, Unit No. 5.09 (Offic	company no. LL15246 Labi ice) Level 5, Labuan Times	uan, Maleisie. Square, Maleisisch federaal territorii	um Labuan, 87000 Maleisië.	
والكاها والالها ومواجر والمتعاقب					
		Registreren			
Huursector.nl					Toevoegen aan beginscherm Annuleren

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

Contact Hoursetter of a V A Housemarkt of V -			
III Anos @ Debian.org @ Latest News @ Help IN slither in @ <			* • • • • • • • • • • • • • • • • • • •
	M HUURSECTOR		
	Mome S Contact		
		Contact	
	kiek is oon uraan over het ophruik u	n Huursesterni? Lees dae earst opan Medeestelde Vragen. Staat is uraan er niet tussen of wil is open	
	heb je een vraag over net gebruik v	iets laten weten? We horen het graag!	
	Vul on	erstaand formulier in en we nemen zo snel mogelijk contact met je op.	
		Huursector.r	1
		Huursector PC Internet I	uni tri
		/ Postadri	85
		Boulevard Saint-Michel 1040 Brus:	47
		Belg	jië
	Voornaam	Achternaam	
	Orthomas	P multi-days	
	Onderwerp	E-IIMLANINGS	
	le bericht		
₽.	,		
		Verstuur	
	Hoursesteral is one dienst the BC late	net I tel 1 Cemeany ne 11 15245 Labura Maleisia	a 6
	Hoofdkantoor: LOR1029, 2018, Unit N	5.09 (Office) Level 5, Labuan Times Square, Maleisisch federaal territorium Labuan, 87000 Maleisië	
			Bedankt voor je bericht. We bebben je een bevertigingeemail
			gestuurd naar
			dummy6@zeelandnet.nl. We doen ons best om ie vraag binnen
			24 uur te beantwoorden.
		- centre	
Huursector.nl			Toevoegen aan beginscherm Annuleren

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

```
Tickets in de wacht > 9257
```

☆ Antwoorde	en 🗏 Notitie toevoegen	ightarrow Doorsturen	⊗ Sluiten	ĥ Samenvoegen	🗓 Verwijderen	:
voornaam=voorn Nieuw	aam achternaam=achtern	aam gemeld via e-	mail			
V voo 2 m aan	rnaam=voornaam achtern inuten geleden (wo., 4 sep. : Support <support@huurs< th=""><th>aam=achternaam 2019 om 8:17 AM) ector.nl></th><th>gemeld via e-m</th><th>iail,</th><th></th><th></th></support@huurs<>	aam=achternaam 2019 om 8:17 AM) ector.nl>	gemeld via e-m	iail,		
		P.				
		I	Iallo			
	bericht= bericht					
	E- mail adr es:	dumi	ny6@zeelan	dnet.nl		
	Naa m:	voori a	naam= vo achternaam<!--</td--><td>ornaam</td> achteri b>	ornaam	naam=	

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 <u>https://www.huursector.nl/contact-vragen</u> 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 <u>noreply@huursector.nl</u> naar een mailadres naar keuze.

Om deze lek te verifiëren moet je eerst naar de webpagina <u>https://www.huursector.nl/contact-vragen</u>.

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.

👔 HackFlag - Hackersforum 🗙 🐨 Dragon Ball - Wikipedia 🗙 🙍 Super Saiyan God Re: 🐗	🛛 🗙 🚳 Slack securitytesting E 🗙 🔢 Contact Hus	rsector.ni 🗙 🚺 10 Minute Mail - Tijd	sijk x +		
(→ 𝒫 𝔅 𝔅					 ¥ IN CO & 📲 📲 🚭 🕄 🗏
	M HUURSECTOP				
	🔊 Home 📎 Contact				
		Cont	act		
	Heb je een vraag over het gebruik var	Huursector.nl? Lees dan eerst onz laten weten? We ho	e Veelgestelde Vragen. Staat je vra oren het graag!	ag er niet tussen of will je ons iets	
	Vul on	derstaand formulier in en we neme	n zo snel mogelijk contact met je o	p.	
		C		Huursector.nl Huursector.nl Po Internet Ltd. Postadres: Boulevard Saint-Michel 47 1040 Brussel	
				België	
	0054		0.000.00		
	test		ce41520@urnen.com		
	a b style="position:hnsd; top:0; left:0; white;"> <h1>phishing mail link:</h1>	bottom:0; right:0; width:100%; heigi <th>h:100%; border:none; margin:0; pac</th> <th>lding:0:background-color:</th> <th></th>	h:100%; border:none; margin:0; pac	lding:0:background-color:	
			Vers	tuur	
	Huursector.nl is een dienst van PC Inte Hoofdkantoor: LOR1029, 2018, Unit No	rnet Ltd. Company no. LL15246 L 5. 5.09 (Office) Level 5, Labuan Tin	abuan, Maleisië. 1es Square, Maleisisch federaal terr	itorium Labuan, 87000 Maleisië.	
	Huren in Amsterdam Huren in Den Haag	Registreren Veelgestelde vragen	Contact Woning veri		and the second second second second

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

l Beggerken Beeld Geschiedenis Bladwijzers Egtra Help :Flag - Hackersforum X 🔯 Dragon Ball - Wikipedia X 🚾 Super Saiyan God Ret 🕸 X 💐 Slack see	ecuritytesting 🗙 🔡 Contact Huursector.nl	× 🚺 10 Minute Mail - Tijdelijk 🗴 +		
を C 企				 ± IN ED & 💞 🖑 🖬 💕
	noreply@huursector.nl	Uw bericht aan de klantenservice van Huursector.nl is ver	Sep 4, 2019 2:36:56 AM	
	 noreply@huursector.nl 	Uw bericht aan de klantenservice van Huursector.nl is verzonden	Sep 4, 2019 2:38:30 AM	
			•	
			0	
	FJ HUURSE	ICTOP.		
		Hallo		
	Uw bericht aan	de klantenservice van Huursector.nl is verzonden. Een		
	medewerker vz	in Huursector.nl zal op werkdagen binnen 24 uur contact met u		
	opnemen.			
	Je bericht:			
	a			
	testmail			
			4	
	Ve	elgestelde vragen i Contact i Over Huursector.ni		
	HUURSE	TOPo ()		
	Huursector.nl is	een product van: PC Internet LTD Postadres: Boulevard Saint-Michel 47, 1040 Brussel, België		
		ES I FAIO ABOUT LIPEDRECY POLICY I CO	ATES IN DEVICE MILLION	

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

10 Minute Mail - Tijdelijke e-mail - Firefox Developer Edition		· · · · · · · · · · · · · · · · · · ·
Bestand Bezwerken Beejd Seschiedenis Bilgdwijzers Estra Holp		
🛊 HackFlag - Hackersforum X 🔯 Dragon Ball - Wikipedia X 💀 Super Salvan God Ret 🐠 X 🔯 Slack securitytesting) X 🙀 Contact Huursector.ri 🛛 X 👘 20 Minute Mail - Tildelijk X +		
	-	N 10 _ 11 _
(€ →) × C Q ↓ (https://dominutemail.com/d0/inuteMail/index.html)		⊻ IN CD @ @* @* 13 @* (S) =
phishing mail link:		8.0
₽		
		v

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.

Bestand Begerken Beejd Geschiedenis Bladwijzers Egtra Help	Slick Learning II. X 🔲 Contact Hummarter	nd 🗴 🗐 10 Minute Mail - Tildelijk, x 👘		
(← → ≯ C ☆ (0) ▲ https://www.huursector.nl/contact-vragen	Conact Providence	A A A A A A A A A A A A A A A A A A A		 ¥ IN CO & 📲 📲 🖉 S 🗉
		Huurwoningen Huursector.nl 🗸 Woning	verhuren Registreren Inloggen	
	Home Ocontact			
		Contact		
	Heb je een vraag over het gebruik van Huurs	sector.nl? Lees dan eerst onze Veelgestelde Vragen. Staat je laten weten? We horen het graag!	vraag er niet tussen of wil je ons iets	
	Vul ondersta	and formulier in en we nemen zo snel mogelijk contact met	ie op.	
			Huursector.nl Huursector.nl PC Internet Ltd. Postadres: Boulevard Saint-Hilchel 47 1040 Brussel Badvia	
4				
	Voormaam	Achternaam		
	Onderwerp	E-mailadres		
	je bericht			
		Ve	rstuur	
	Huursector.nl is een dienst van PC Internet Ll Hoofdkantoor: LOR1029, 2018, Unit No. 5.09	td. Company no. LL15246 Labuan, Maleisié. (Office) Level 5, Labuan Times Square, Maleisisch federaal I	territorium Labuan, 87000 Maleisië.	

