Scan Rapport

Algemene Informatie	
Klant: wp-example	
Bedrijf: console	
Email: webapplicatietest@gmail.com	

Scan Informatie	
URL: http://cms.local	
Server: Apache	
Scan type: Full Scan	
Start tijd: 2017-09-30 00:51:14	
Eind tijd: 2017-09-30 00:51:54	
Scan tijd: 40 secondes	

Scan Resultaten

Dreigingsniveau (Kleur code)	Niveau	Omschrijving
	4	Er zijn één of meer zeer zorgwekkende kwetsbaarheden op de website gevonden. De kans op exploitatie door hackers is zeer hoog. Hackers kunnen toegang krijgen tot het backend systeem en daarop de databases muteren.

Totale dreigementen gevonden
Hoog: 18
gemiddeld: 168
Laag: 168

Categorie dreigementen	Dreigingsniveau	Aantal	Omschrijving
XSS	hoog	18	Cross-site scripting is een type kwetsbaarheid dat vooral gevonden wordt in webapplicaties. XSS maakt het mogelijk voor hackers om client-side scripting talen te injecteren op webpagina's.
Security Headers Gemiddeld	gemiddeld	168	De http security headers van dit niveau voorzien een website met een extra laag van beveiliging om aanvallen af te weren en kwetsbaarheidlekken te dichten, kwetsbaarheden met betrekking tot XSS. Het missen van security headers maakt uw website kwetsbaar voor aanvallen.
Security Headers Laag	laag	168	De http security headers van dit niveau hebben vooral betrekking op misconfiguraties aan de server kant. Dit kan leiden tot het lekken van informatie.

Advies: XSS

Cross-site scripting is een veel voorkomende client-side kwetsbaarheid waarbij
de aanvaller client-site code injecteert op webpagina.
Er zijn twee basis regels waar een website aan moet
voldoen om dit probleem te verkomen:

Regels

- Voer nooit onvertrouwde data in, behalve op toegestaande locaties
- Voordat de data wordt ingevoerd moet de HTML Escaped worden

Advies: Security Headers

Secuirty Headers zorgen voor een veilig verkeer tussen de server en de client.
Wanneer hier niet gebruik van gemaakt wordt kan het zijn dat hackers het als een kans
zien om uw website te exploiteren. Om dit te voorkomen kunt u gebruik maken van de volgende headers:

- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- Content-Secuirty-Policy
- Public-Key-Pins (SLL)
- HttpOnly

Detials van gevonden kwetsbaarheden

ID: 20291

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params

Aanval: <script>alert('cypnxq539y')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:21

ID: 20292

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params

Aanval: <script>alert("cypnxq539y")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:21

ID: 20293	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php	
Parameter: form-params	
Aanval: <script>String.fromCharCode(0,cypnxq539y,1)</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:22	

ID: 20294	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php	
Parameter: form-params	
Aanval: <script src=http://cypnxq539y/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:22	

ID: 20295	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php	
Parameter: form-params	
Aanval: <script[TAB]src=http://cypnxq539y/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:22	

ID: 20296	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php	
Parameter: form-params	
Aanval: <scr<script>ipt>alert('cypnxq539y')</script>	

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:26

ID: 20297

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params

Aanval: <scr<script>ipt>alert("cypnxq539y")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:26

ID: 20298

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params

Aanval: <scr<script>ipt>String.fromCharCode(0,cypnxq539y,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:27

ID: 20299

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params

Aanval: <scr<script>ipt src=http://cypnxq539y/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 00:51:27

ID: 20300

Module: xss

Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword	
Parameter: form-params	
Aanval: <script>alert('590vfovct2')</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:37	

ID: 20301	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword	
Parameter: form-params	
Aanval: <script>alert("590vfovct2")</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:37	

ID: 20302	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword	
Parameter: form-params	
Aanval: <script>String.fromCharCode(0,590vfovct2,1)</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-30 00:51:37	

ID: 20303	
Module: xss	
Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword	
Parameter: form-params	
Aanval: <script src=http://590vfovct2/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	

Methode: POST	
Datum: 2017-09-30 00:51:38	

ID: 20304
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script[TAB]src=http://590vfovct2/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 00:51:38

ID: 20305
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert('590vfovct2')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 00:51:42

ID: 20306
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert("590vfovct2")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 00:51:42

ID: 20307
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter:	form-params
Aanval:	<scr<script>ipt>String.fromCharCode(0,590vfovct2,1)</script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST
Datum:	2017-09-30 00:51:43

ID:	20308
Module:	xss
Risico:	high
Target URL:	http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter:	form-params
Aanval:	<scr<script>ipt src=http://590vfovct2/x.js></script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST
Datum:	2017-09-30 00:51:43

ID:	20309
Module:	X-Content-Type-Options
Risico:	average
Target URL:	http://cms.local/?C=N;O=A
Parameter:	n/a
Aanval:	n/a
Error:	Header missing
WASC ID:	15
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20310
Module:	X-Frame-Options
Risico:	average
Target URL:	http://cms.local/?C=N;O=A
Parameter:	n/a
Aanval:	n/a
Error:	Header not set
WASC ID:	15
Methode:	GET
Datum:	2017-09-30 00:51:45

ID: 20311

Module: X-XSS-Protection

Risico: average

Target URL: http://cms.local/?C=N;O=A

Parameter: n/a

Aanval: n/a

Error: Not enabled

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20312

Module: Content-Secuirty-Policy

Risico: low

Target URL: http://cms.local/?C=N;O=A

Parameter: n/a

Aanval: n/a

Error: Header not set

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20313

Module: Public-Key-Pins

Risico: low

Target URL: http://cms.local/?C=N;O=A

Parameter: n/a

Aanval: n/a

Error: Public Key is missing (Only for SLL)

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20314

Module: HttpOnly

Risico: low

Target URL: http://cms.local/?C=N;O=A

Parameter: n/a

Aanval: n/a

Error: No HttpOnly flag

WASC ID: 13

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20315

Module: X-Content-Type-Options

Risico: average

Target URL: http://cms.local/?C=M;O=A

Parameter: n/a

Aanval: n/a

Error: Header missing

WASC ID: 15

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20316

Module: X-Frame-Options

Risico: average

Target URL: http://cms.local/?C=M;O=A

Parameter: n/a

Aanval: n/a

Error: Header not set

WASC ID: 15

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20317

Module: X-XSS-Protection

Risico: average

Target URL: http://cms.local/?C=M;O=A

Parameter: n/a

Aanval: n/a

Error: Not enabled

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20318

Module: Content-Secuirty-Policy

Risico: low	
Target URL: http://cms.local/?C=M;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20319	
Module: Public-Key-Pins	
Risico: low	
Target URL: http://cms.local/?C=M;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Public Key is missing (Only for SLL)	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20320	
Module: HttpOnly	
Risico: low	
Target URL: http://cms.local/?C=M;O=A	
Parameter: n/a	
Aanval: n/a	
Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20321	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/?C=S;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	

Methode: GET	
Datum: 2017-09-30 00:51:45	
ID: 20322	
Module: X-Frame-Options	
Risico: average	
Target URL: http://cms.local/?C=S;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	
ID: 20323	
Module: X-XSS-Protection	
Risico: average	
Target URL: http://cms.local/?C=S;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Not enabled	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	
ID: 20324	
Module: Content-Secuirty-Policy	
Risico: low	
Target URL: http://cms.local/?C=S;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	
ID: 20325	
Module: Public-Key-Pins	
Risico: low	
Target URL: http://cms.local/?C=S;O=A	

Parameter: n/a	
Aanval: n/a	
Error: Public Key is missing (Only for SLL)	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20326	
Module: HttpOnly	
Risico: low	
Target URL: http://cms.local/?C=S;O=A	
Parameter: n/a	
Aanval: n/a	
Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20327	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/?C=D;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20328	
Module: X-Frame-Options	
Risico: average	
Target URL: http://cms.local/?C=D;O=A	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID:	20329
Module:	X-XSS-Protection
Risico:	average
Target URL:	http://cms.local/?C=D;O=A
Parameter:	n/a
Aanval:	n/a
Error:	Not enabled
WASC ID:	14
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20330
Module:	Content-Secuirty-Policy
Risico:	low
Target URL:	http://cms.local/?C=D;O=A
Parameter:	n/a
Aanval:	n/a
Error:	Header not set
WASC ID:	14
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20331
Module:	Public-Key-Pins
Risico:	low
Target URL:	http://cms.local/?C=D;O=A
Parameter:	n/a
Aanval:	n/a
Error:	Public Key is missing (Only for SLL)
WASC ID:	14
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20332
Module:	HttpOnly
Risico:	low
Target URL:	http://cms.local/?C=D;O=A
Parameter:	n/a
Aanval:	n/a

Error:	No HttpOnly flag
WASC ID:	13
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20333
Module:	X-Content-Type-Options
Risico:	average
Target URL:	http://cms.local/wordpress/
Parameter:	n/a
Aanval:	n/a
Error:	Header missing
WASC ID:	15
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20334
Module:	X-Frame-Options
Risico:	average
Target URL:	http://cms.local/wordpress/
Parameter:	n/a
Aanval:	n/a
Error:	Header not set
WASC ID:	15
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20335
Module:	X-XSS-Protection
Risico:	average
Target URL:	http://cms.local/wordpress/
Parameter:	n/a
Aanval:	n/a
Error:	Not enabled
WASC ID:	14
Methode:	GET
Datum:	2017-09-30 00:51:45

ID:	20336
Module:	Content-Secuirty-Policy

Risico: low	
Target URL: http://cms.local/wordpress/	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20337	
Module: Public-Key-Pins	
Risico: low	
Target URL: http://cms.local/wordpress/	
Parameter: n/a	
Aanval: n/a	
Error: Public Key is missing (Only for SLL)	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20338	
Module: HttpOnly	
Risico: low	
Target URL: http://cms.local/wordpress/	
Parameter: n/a	
Aanval: n/a	
Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20339	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/icons/blank.gif	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20340

Module: X-Frame-Options

Risico: average

Target URL: http://cms.local/icons/blank.gif

Parameter: n/a

Aanval: n/a

Error: Header not set

WASC ID: 15

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20341

Module: X-XSS-Protection

Risico: average

Target URL: http://cms.local/icons/blank.gif

Parameter: n/a

Aanval: n/a

Error: Not enabled

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20342

Module: Content-Secuirty-Policy

Risico: low

Target URL: http://cms.local/icons/blank.gif

Parameter: n/a

Aanval: n/a

Error: Header not set

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20343

Module: Public-Key-Pins

Risico: low

Target URL: http://cms.local/icons/blank.gif

Parameter: n/a	
Aanval: n/a	
Error: Public Key is missing (Only for SLL)	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20344	
Module: HttpOnly	
Risico: low	
Target URL: http://cms.local/icons/blank.gif	
Parameter: n/a	
Aanval: n/a	
Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20345	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/icons/folder.gif	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20346	
Module: X-Frame-Options	
Risico: average	
Target URL: http://cms.local/icons/folder.gif	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20347

Module: X-XSS-Protection

Risico: average

Target URL: http://cms.local/icons/folder.gif

Parameter: n/a

Aanval: n/a

Error: Not enabled

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20348

Module: Content-Secuirty-Policy

Risico: low

Target URL: http://cms.local/icons/folder.gif

Parameter: n/a

Aanval: n/a

Error: Header not set

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20349

Module: Public-Key-Pins

Risico: low

Target URL: http://cms.local/icons/folder.gif

Parameter: n/a

Aanval: n/a

Error: Public Key is missing (Only for SLL)

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:51:45

ID: 20350

Module: HttpOnly

Risico: low

Target URL: http://cms.local/icons/folder.gif

Parameter: n/a

Aanval: n/a

Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20351	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20352	
Module: X-Frame-Options	
Risico: average	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20353	
Module: X-XSS-Protection	
Risico: average	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Not enabled	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20354	
Module: Content-Secuirty-Policy	

Risico: low	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20355	
Module: Public-Key-Pins	
Risico: low	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Public Key is missing (Only for SLL)	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20356	
Module: HttpOnly	
Risico: low	
Target URL: http://cms.local/?C=M;O=D	
Parameter: n/a	
Aanval: n/a	
Error: No HttpOnly flag	
WASC ID: 13	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20357	
Module: X-Content-Type-Options	
Risico: average	
Target URL: http://cms.local/?C=S;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header missing	
WASC ID: 15	

Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20358	
Module: X-Frame-Options	
Risico: average	
Target URL: http://cms.local/?C=S;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 15	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20359	
Module: X-XSS-Protection	
Risico: average	
Target URL: http://cms.local/?C=S;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Not enabled	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20360	
Module: Content-Secuirty-Policy	
Risico: low	
Target URL: http://cms.local/?C=S;O=D	
Parameter: n/a	
Aanval: n/a	
Error: Header not set	
WASC ID: 14	
Methode: GET	
Datum: 2017-09-30 00:51:45	

ID: 20361	
Module: Public-Key-Pins	
Risico: low	
Target URL: http://cms.local/?C=S;O=D	

| **Parameter:** n/a |
| **Aanval:** n/a |
| **Error:** Public Key is missing (Only for SLL) |
| **WASC ID:** 14 |
| **Methode:** GET |
| **Datum:** 2017-09-30 00:51:45 |