

Scan Rapport

Algemene Informatie

Klant: test

Bedrijf: test

Email: webapplicatietest@gmail.com

Scan Informatie

URL: http://cms.local

Server: Apache

Scan type: Full Scan

Start tijd: 2017-09-30 12:24:18

Eind tijd: 2017-09-30 12:24:54

Scan tijd: 36 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 voorkomen:

Regels

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

Advies: Security Headers

Security 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-Security-Policy
- Public-Key-Pins (SLL)
- HttpOnly

Details van gevonden kwetsbaarheden

ID: 20645

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('1f9e9xrayc')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 12:24:25

ID: 20646

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert("1f9e9xrayc")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-30 12:24:25

ID: 20647
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <script>String.fromCharCode(0,1f9e9xrayc,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:26
ID: 20648
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <script src=http://1f9e9xrayc/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:26
ID: 20649
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <script[TAB]src=http://1f9e9xrayc/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:26
ID: 20650
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>alert('1f9e9xrayc')</script>

Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:30
ID: 20651
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>alert("1f9e9xrayc")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:30
ID: 20652
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>String.fromCharCode(0,1f9e9xrayc,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:30
ID: 20653
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt src=http://1f9e9xrayc/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:31
ID: 20654
Module: xss

Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>alert('htwprofck4')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:39
ID: 20655
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>alert("htwprofck4")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:39
ID: 20656
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>String.fromCharCode(0,htwprofck4,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:40
ID: 20657
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script src=http://htwprofck4/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8

Methode: POST
Datum: 2017-09-30 12:24:40
ID: 20658
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script[TAB]src=http://htwprofck4/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:41
ID: 20659
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert('htwprofck4')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:44
ID: 20660
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert("htwprofck4")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:45
ID: 20661
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,htwprofck4,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:45
ID: 20662
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt src=http://htwprofck4/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-30 12:24:45
ID: 20663
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 12:24:46
ID: 20664
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 12:24:46

ID: 20665
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 12:24:46
ID: 20666
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 12:24:46
ID: 20667
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 12:24:46
ID: 20668
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 12:24:46
ID: 20669
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 12:24:47
ID: 20670
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 12:24:47
ID: 20671
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 12:24:47
ID: 20672
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 12:24:47
ID: 20673
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 12:24:47
ID: 20674
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 12:24:47
ID: 20675
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 12:24:47
ID: 20676
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 12:24:47
ID: 20677
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 12:24:47
ID: 20678
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 12:24:47
ID: 20679
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 12:24:47
ID: 20680
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 12:24:47
ID: 20681
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 12:24:47
ID: 20682
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 12:24:47

ID: 20683
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 12:24:47
ID: 20684
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 12:24:47
ID: 20685
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 12:24:47
ID: 20686
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 12:24:47
ID: 20687
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 12:24:47
ID: 20688
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 12:24:47
ID: 20689
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 12:24:47
ID: 20690
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 12:24:47
ID: 20691
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 12:24:47
ID: 20692
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 12:24:47
ID: 20693
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 12:24:47
ID: 20694
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 12:24:47
ID: 20695
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 12:24:47
ID: 20696
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 12:24:47
ID: 20697
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 12:24:47
ID: 20698
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 12:24:47
ID: 20699
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 12:24:47
ID: 20700
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 12:24:47

ID: 20701
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 12:24:47
ID: 20702
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 12:24:47
ID: 20703
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 12:24:47
ID: 20704
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 12:24:47
ID: 20705
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 12:24:47
ID: 20706
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 12:24:47
ID: 20707
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 12:24:47
ID: 20708
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 12:24:47
ID: 20709
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 12:24:47
ID: 20710
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 12:24:47
ID: 20711
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 12:24:47
ID: 20712
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 12:24:47
ID: 20713
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 12:24:47
ID: 20714
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 12:24:47
ID: 20715
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 12:24:47