# 95.179.196.14

## Scan time

**Scan started**
2019-03-12 21:21

**Scan finished**
2019-03-12 21:25

## Finding summary

| | | |
|---|---|---|
| 🔴 | SQL Injection | 4 |
| 🔴 | Login Cross Site Request Forgery (CSRF/XSRF) | 1 |
| 🟡 | Cross Site Request Forgery (CSRF/XSRF) | 1 |
| 🟡 | Unencrypted Login Sessions | 1 |
| 🟡 | Login over HTTP-GET | 1 |
| 🔵 | Apache Icon Leakage | 1 |
| 🔵 | Referrer-Policy / Missing Header | 1 |
| 🔵 | Host Header Injection / Potential Open Redirect | 1 |
| 🟢 | Content-Security-Policy / Missing Header | 1 |
| 🟢 | Crawled URL's | 1 |
| 🟢 | Discovered IP | 1 |
| 🟢 | Email Enumeration | 1 |
| 🟢 | HTML Comments | 1 |

## Scan settings

| | |
|---|---|
| Crawl subdomains | No |
| Scan as device | Detectify |

# ● SQL Injection

## What does this mean?

our article about SQL Injection
(http://support.detectify.com/customer/portal/articles/1711514-sql-injection).

## What can happen?

An attacker may be able to execute SQL-code, which includes reading/writing to the database and possible write directly to the file system.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/sqlinjection/example4/ | 10 |
| 2 | http://95.179.196.14/sqlinjection/example5/ | 10 |
| 3 | http://95.179.196.14/sqlinjection/example6/ | 10 |
| 4 | http://95.179.196.14/sqlinjection/example7/ | 10 |

# 1. SQL Injection

## Summary

**Found At**
http://95.179.196.14/sqlinjection/example4/

**Request URL**
http://95.179.196.14/sqlinjection/example4/?req=username%3d%27hacker%27%27%22%60%F0%9D%8C%86

**CVSS**
10 of 10.0

**Command**

```
python sqlmap.py --technique=EUS --url=http://95.179.196.14/sqlinjection/example4/?req=username%3d%27hacker%27
```

## Request Headers

```
GET
/sqlinjection/example4/?req=username%3d%27hacker%27%27%22%60%F0%9D%8C%86
HTTP/1.1
```

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |

| | |
|---|---|
| Content-Encoding | gzip |
| Content-Length | 800 |
| Content-Type | text/html;charset=utf-8 |
| Date | Tue, 12 Mar 2019 21:24:09 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

```
 40px;
      }
    </style>
    <link href="/css/bootstrap-responsive.css" rel="stylesheet">

  </head>

  <body>

    <div class="navbar navbar-inverse navbar-fixed-top">
      <div class="navbar-inner">
        <div class="container">
          <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </a>
          <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
          <div class="nav-collapse collapse">
            <ul class="nav">
              <li class="active"><a href="/">Home</a></li>
            </ul>
          </div><!--/.nav-collapse -->
        </div>
      </div>
    </div>

    <div class="container">


Mysql2::Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near
&#x27;&#x27;hacker&#x27;&#x27;&quot;`??&#x27; at line 1: SELECT * FROM users WHERE
username=&#x27;hacker&#x27;&#x27;&quot;`??;
<table class="table table-striped">
  <tr><th>id</th><th>name</th></tr>

</table>

      <footer>
        <p>&copy; PentesterLab 2013</p>
      </footer>

    </div> <!-- /container -->


  </body>
</html>
```

## Resources

DETECTIFY - Detectify Support Center - SQL Injection
OWASP - SQL Injection
WIKIPEDIA - SQL Injection

# 1. SQL Injection

## Summary

**Found At**
http://95.179.196.14/sqlinjection/example5/

**Request URL**
http://95.179.196.14/sqlinjection/example5/?limit=3E999%27%22%60%00

**CVSS**
10 of 10.0

**Command**

```
python sqlmap.py --technique=EUS
--url=http://95.179.196.14/sqlinjection/example5/?limit=3
```

## Request Headers

GET /sqlinjection/example5/?limit=3E999%27%22%60%00 HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify)<br>+https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |
| Content-Encoding | gzip |

| | |
|---|---|
| Content-Length | 787 |
| Content-Type | text/html;charset=utf-8 |
| Date | Tue, 12 Mar 2019 21:24:09 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

```
 padding-bottom: 40px;
     }
   </style>
   <link href="/css/bootstrap-responsive.css" rel="stylesheet">

 </head>

 <body>

   <div class="navbar navbar-inverse navbar-fixed-top">
     <div class="navbar-inner">
       <div class="container">
         <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
           <span class="icon-bar"></span>
           <span class="icon-bar"></span>
           <span class="icon-bar"></span>
         </a>
         <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
         <div class="nav-collapse collapse">
           <ul class="nav">
             <li class="active"><a href="/">Home</a></li>
           </ul>
         </div><!--/.nav-collapse -->
       </div>
     </div>
   </div>

   <div class="container">


Mysql2::Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near &#x27;3E999&#x27;&quot;`&#x27; at line
1: SELECT * FROM users LIMIT 3E999&#x27;&quot;`;
<table class="table table-striped">
  <tr><th>id</th><th>name</th></tr>

</table>

     <footer>
       <p>&copy; PentesterLab 2013</p>
     </footer>

   </div> <!-- /container -->


  </body>
</html>
```

## Resources

DETECTIFY - Detectify Support Center - SQL Injection
OWASP - SQL Injection
WIKIPEDIA - SQL Injection

# 1. SQL Injection

## Summary

**Found At**
http://95.179.196.14/sqlinjection/example6/

**Request URL**
http://95.179.196.14/sqlinjection/example6/?group=username%27%22%60%
F0%9D%8C%86

**CVSS**
10 of 10.0

**Command**

```
python sqlmap.py --technique=EUS
--url=http://95.179.196.14/sqlinjection/example6/?group=username
```

## Request Headers

GET /sqlinjection/example6/?group=username%27%22%60%F0%9D%8C%86 HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |

|  |  |
|---|---|
| Content-Encoding | gzip |
| Content-Length | 795 |
| Content-Type | text/html;charset=utf-8 |
| Date | Tue, 12 Mar 2019 21:24:09 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

```
   padding-bottom: 40px;
      }
    </style>
    <link href="/css/bootstrap-responsive.css" rel="stylesheet">

  </head>

  <body>

    <div class="navbar navbar-inverse navbar-fixed-top">
      <div class="navbar-inner">
        <div class="container">
          <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </a>
          <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
          <div class="nav-collapse collapse">
            <ul class="nav">
              <li class="active"><a href="/">Home</a></li>
            </ul>
          </div><!--/.nav-collapse -->
        </div>
      </div>
    </div>

    <div class="container">


Mysql2::Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near &#x27;&#x27;&quot;`??&#x27; at line 1:
SELECT * FROM users GROUP BY username&#x27;&quot;`??;
<table class="table table-striped">
  <tr><th>id</th><th>name</th></tr>

</table>

      <footer>
        <p>&copy; PentesterLab 2013</p>
      </footer>

    </div> <!-- /container -->


  </body>
</html>
```

# Resources

DETECTIFY - Detectify Support Center - SQL Injection
OWASP - SQL Injection
WIKIPEDIA - SQL Injection

# 1. SQL Injection

## Summary

**Found At**
http://95.179.196.14/sqlinjection/example7/

**Request URL**
http://95.179.196.14/sqlinjection/example7/?id=1E999%27%22%60%00

**CVSS**
10 of 10.0

**Command**

```
python sqlmap.py --technique=EUS
--url=http://95.179.196.14/sqlinjection/example7/?id=1
```

## Request Headers

GET /sqlinjection/example7/?id=1E999%27%22%60%00 HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |
| Content-Encoding | gzip |

| | |
|---|---|
| Content-Length | 727 |
| Content-Type | text/html;charset=utf-8 |
| Date | Tue, 12 Mar 2019 21:24:09 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

```
    <link href="/css/bootstrap.css" rel="stylesheet">

    <style type="text/css">
      body {
        padding-top: 60px;
        padding-bottom: 40px;
      }
    </style>
    <link href="/css/bootstrap-responsive.css" rel="stylesheet">

  </head>

  <body>

    <div class="navbar navbar-inverse navbar-fixed-top">
      <div class="navbar-inner">
        <div class="container">
          <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </a>
          <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
          <div class="nav-collapse collapse">
            <ul class="nav">
              <li class="active"><a href="/">Home</a></li>
            </ul>
          </div><!--/.nav-collapse -->
        </div>
      </div>
    </div>

    <div class="container">


Mysql2::Error: Illegal double &#x27;1E999&#x27; value found during parsing: SELECT * FROM
users WHERE id=1E999&#x27;&quot;`
<table class="table table-striped">
  <tr><th>id</th><th>name</th></tr>

</table>

      <footer>
        <p>&copy; PentesterLab 2013</p>
      </footer>

    </div> <!-- /container -->


  </body>
</html>
```

# Resources

DETECTIFY - Detectify Support Center - SQL Injection
OWASP - SQL Injection
WIKIPEDIA - SQL Injection

# ● Login Cross Site Request Forgery (CSRF/XSRF)

## What does this mean?

The web site seems to be lacking CSRF token on a login form.

our knowledge base (http://support.detectify.com/customer/portal/articles/1969819-login-csrf).

## What can happen?

An attacker can force an unsuspecting user to sign in to the attacker's account. What can be done from there depends on the application. Example: An attacker can force an unsuspecting user to login to the attacker's account and when the user buys something, the credit card is added to the attacker's account.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/mongodb/example1/ | 6.2 |

# 1. Login Cross Site Request Forgery (CSRF/XSRF)

## Summary

**Found At**
http://95.179.196.14/mongodb/example1/

**Request URL**
http://95.179.196.14/mongodb/example1/?username=&submit=Submit+Query
&password=

**CVSS**
6.2 of 10.0

## Request Headers

GET /mongodb/example1/?username=&submit=Submit+Query&password= HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify)<br>+https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=46 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:23 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |

| | |
|---|---|
| Content-Length | 660 |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

```
<form action="" action="get">

  Username: <input type="text" name="username">
  Password: <input type="password" name="password">
  <input type="submit" name="submit">
</form>
```

## Resources

DETECTIFY - Detectify Support Center - Login CSRF
STACKOVERFLOW - How to protect against login CSRF?

# ● Cross Site Request Forgery (CSRF/XSRF)

## What does this mean?

The site doesn't check for tokens or make sure that the request really is from the user in any other way.

here (http://support.detectify.com/customer/portal/articles/2792245-csrf).

## What can happen?

An attacker can force a victim to perform unwanted actions at the site.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/captcha/example2/ | 5.8 |

# 1. Cross Site Request Forgery (CSRF/XSRF)

## Summary

**Found At**
http://95.179.196.14/captcha/example2/

**Request URL**
http://95.179.196.14/captcha/example2/

**CVSS**
5.8 of 10.0

## Request Headers

GET /captcha/example2/ HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=94 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:21 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |
| Content-Length | 716 |

| | |
|---|---|
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

```
<form action="submit" action="get">

  <img src="captcha.png?t=1552425801.903983">
  Answer: <input type="text" name="captcha">
  <input type="hidden" name="answer" value="^fnYZA^RuS">
  <input type="submit" name="submit">
</form>
```

## Resources

DETECTIFY - CAPTCHA does not prevent CSRF

# ● Unencrypted Login Sessions

## What does this mean?

The login form isn't using HTTPS.

here (http://support.detectify.com/customer/portal/articles/2792104-unencrypted-login-sessions).

## What can happen?

An attacker can, if intercepting the traffic, read login credentials in plain text.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/mongodb/example1/ | 5.5 |

# 1. Unencrypted Login Sessions

## Summary

**Found At**
http://95.179.196.14/mongodb/example1/

**Request URL**
http://95.179.196.14/mongodb/example1/?username=&submit=Submit+Query
&password=

**CVSS**
5.5 of 10.0

## Request Headers

GET /mongodb/example1/?username=&submit=Submit+Query&password= HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify)<br>+https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=46 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:23 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |

| | |
|---|---|
| Content-Length | 660 |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

```
<form action="" action="get">

  Username: <input type="text" name="username">
  Password: <input type="password" name="password">
  <input type="submit" name="submit">
</form>
```

## Resources

OWASP - Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

# ● Login over HTTP-GET

## What does this mean?

The login form is sending data using HTTP GET-request.

## What can happen?

Passwords may appear visible in the URL and stored in the browser's history. It may also be cached by immediate proxies and getting stored in remote server logs.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/mongodb/example1/ | 5 |

# 1. Login over HTTP-GET

## Summary

**Found At**
http://95.179.196.14/mongodb/example1/

**Request URL**
http://95.179.196.14/mongodb/example1/?username=&submit=Submit+Query&password=

**CVSS**
5 of 10.0

## Request Headers

GET /mongodb/example1/?username=&submit=Submit+Query&password= HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=46 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:23 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |

| | |
|---|---|
| Content-Length | 660 |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

```
<form action="" action="get">

  Username: <input type="text" name="username">
  Password: <input type="password" name="password">
  <input type="submit" name="submit">
</form>
```

# ● Apache Icon Leakage

## What does this mean?

The HTTP server discloses what type of technology that is currently used on the HTTP-server.

here (http://support.detectify.com/customer/portal/articles/2792281-technology-disclosure).

## What can happen?

An attacker can use that information to look up known vulnerabilities in the specific technology and then use them against the website.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/ | 2.9 |

# 1. Apache Icon Leakage

## Summary

**Found At**
http://95.179.196.14/

**Request URL**
http://95.179.196.14/

**CVSS**
2.9 of 10.0

## Request Headers

GET / HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=96 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:18 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |
| Content-Length | 1541 |

| | |
|---|---|
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

By observing the checksums of the files accessible from /icons/ it's possible to work out what versions of Apache that is used. You can reconfigure your Apache setup to disable access to /icons/.

## Resources

MISC - Removal of the /var/www/icons alias from Apache config
MISC - Hardening an Apache Server
MISC - Apache hardening cheat sheet

# ● Referrer-Policy / Missing Header

## What does this mean?

No referrer policy was found in the response and browsers will therefore use their default referrer policy.

## What can happen?

Browsers may send sensitive information if it is stored in the URL to external websites.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/ | 1.8 |

# 1. Referrer-Policy / Missing Header

## Summary

**Found At**
http://95.179.196.14/

**Request URL**
http://95.179.196.14/

**CVSS**
1.8 of 10.0

## Request Headers

GET / HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |
| Content-Encoding | gzip |
| Content-Length | 1541 |
| Content-Type | text/html;charset=utf-8 |

| | |
|---|---|
| Date | Tue, 12 Mar 2019 21:24:06 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

## Resources

OWASP - Referrer-Policy
MOZILLA - Referrer-Policy
MOZILLA - Tighter Control Over Your Referrers
MISC - A new security header: Referrer Policy
MISC - Using CORS policies to implement CSRF protection
W3 - Referrer Policy

# ● Host Header Injection / Potential Open Redirect

## What does this mean?

It's possible to cause the web application to redirect the victim to a site of the attacker's choice.

## What can happen?

An attacker may, by redirecting the user to the attacker's site, launch an online phishing scam and steal user credentials or other sensitive information.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/captcha/example2/submit | 1.2 |

# 1. Host Header Injection / Potential Open Redirect

## Summary

**Found At**
http://95.179.196.14/captcha/example2/submit

**Request URL**
http://pentest.detectify.com/captcha/example2/submit?submit=Submit+Query&captcha=&answer=%5EfnYZA%5ERuS

**CVSS**
1.2 of 10.0

## Request Headers

GET
/captcha/example2/submit?submit=Submit+Query&captcha=&answer=%5EfnYZA%5ERuS
HTTP/1.1

| | |
|---|---|
| Host | pentest.detectify.com |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Connection | close |

## Response Headers

HTTP/ 1.1 302 Found

| | |
|---|---|
| Date | Tue, 12 Mar 2019 21:24:08 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Location | http://pentest.detectify.com/captcha/example2/ |
| Content-Length | 0 |
| Status | 302 |
| Vary | Accept-Encoding |
| Connection | close |

| | |
|---|---|
| Content-Type | text/html;charset=utf-8 |

This can potentially be abused in Safari.

## Resources

DETECTIFY - Scratching the surface of host headers in Safari
OWASP - Cache Poisoning
MISC - Practical HTTP Host header attacks

# ● Content-Security-Policy / Missing Header

## What does this mean?

The header contain an undefined policy.

## What can happen?

Browsers may interpret this in different ways, and may open up for undefined behaviors.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/ | 0 |

# 1. Content-Security-Policy / Missing Header

## Summary

**Found At**
http://95.179.196.14/

**Request URL**
http://95.179.196.14/

**CVSS**
0 of 10.0

## Request Headers

GET / HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |
| Host | 95.179.196.14 |
| Cache-Control | no-store, no-cache |
| Pragma | no-cache |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| X-XSS-Protection | 1; mode=block |
| X-Content-Type-Options | nosniff |
| X-Frame-Options | SAMEORIGIN |
| Status | 200 |
| Vary | Accept-Encoding |
| Content-Encoding | gzip |
| Content-Length | 1541 |
| Content-Type | text/html;charset=utf-8 |

| | |
|---|---|
| Date | Tue, 12 Mar 2019 21:24:06 GMT |
| Server | Apache/2.2.16 (Debian) |
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security.

## Resources

MISC - Content Security Policy Reference
OWASP - Content Security Policy
OWASP - Content Security Policy Cheat Sheet
GOOGLE - Content Security Policy
MOZILLA - Content Security Policy
WIKIPEDIA - Content Security Policy

# ● Crawled URL's

## What does this mean?

This finding is generated for debugging purposes. A link is associated with this finding containing a CSV file with all crawled URL's.

## What can happen?

A scan might take too long due to representative content on the application. Vulnerabilities may also be missed if Detectify lack coverage in some area of the application. If you suspect Detectify can perform better, then take a look at the associated CSV.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | 95.179.196.14 | 0 |

# 1. Crawled URL's

## Summary

**Found At**
95.179.196.14

**CVSS**
0 of 10.0

Detectify tried to access 416 URL's, 16 of these were identified as unique during crawling and went through further testing.

## Resources

DETECTIFY - Download Crawled URL's CSV

# ● Discovered IP

## What does this mean?

Detectify has found the following hosts. This is in no way a vulnerability, but should be considered an indicator for what has been covered.

here (http://support.detectify.com/customer/portal/articles/2792024-discovered-endpoint).

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | 95.179.196.14 | 0 |

# 1. Discovered IP

## Summary

**Found At**
95.179.196.14

**CVSS**
0 of 10.0

```
95.179.196.14:
80/http http open
81/unknown closed
443/unknown closed
444/unknown closed
1443/unknown closed
2082/unknown closed
2083/unknown closed
3000/unknown closed
3001/unknown closed
3128/unknown closed
3790/unknown closed
4443/unknown closed
4444/unknown closed
4502/unknown closed
4505/unknown closed
4567/unknown closed
5050/unknown closed
5051/unknown closed
5984/unknown closed
5985/unknown closed
5986/unknown closed
6443/unknown closed
7001/unknown closed
7077/unknown closed
8000/unknown closed
8001/unknown closed
8047/unknown closed
8080/unknown closed
8081/unknown closed
8083/unknown closed
8088/unknown closed
8089/unknown closed
8090/unknown closed
8100/unknown closed
8111/unknown closed
8161/unknown closed
8181/unknown closed
8443/unknown closed
8444/unknown closed
8500/unknown closed
8880/unknown closed
8888/unknown closed
8983/unknown closed
9000/unknown closed
9001/unknown closed
9002/unknown closed
9003/unknown closed
9080/unknown closed
9090/unknown closed
9093/unknown closed
9100/unknown closed
9200/unknown closed
9300/unknown closed
9443/unknown closed
11211/unknown closed
16686/unknown closed
17000/unknown closed
28017/unknown closed
50000/unknown closed
50013/unknown closed
50014/unknown closed
50070/unknown closed
50470/unknown closed
61680/unknown closed
61681/unknown closed
```

# ● Email Enumeration

## What does this mean?

The web site reveals one or more email addresses in plain text.

here (http://support.detectify.com/customer/portal/articles/2792087-email-enumeration).

## What can happen?

Spammers can easily gather these email addresess and use them in spam campaigns. An attacker may also use those email adressess for spear phishing and other attacks.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/sqlinjection/example5/ | 0 |

# 1. Email Enumeration

## Summary

**Found At**
http://95.179.196.14/sqlinjection/example5/

**Request URL**
http://95.179.196.14/sqlinjection/example5/?limit=3

**CVSS**
0 of 10.0

## Request Headers

GET /sqlinjection/example5/?limit=3 HTTP/1.1

| | |
|---|---|
| Accept | text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8 |
| Upgrade-Insecure-Requests | 1 |
| User-Agent | Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/701e6f4763d16abda616d359d41752bc3d76f3b6 |
| Accept-Encoding | gzip, deflate |
| Accept-Language | en-US |

## Response Headers

HTTP/ 1.1 200 OK

| | |
|---|---|
| Status | 200 |
| Keep-Alive | timeout=15, max=76 |
| Server | Apache/2.2.16 (Debian) |
| X-Content-Type-Options | nosniff |
| Connection | Keep-Alive |
| Date | Tue, 12 Mar 2019 21:23:22 GMT |
| X-Frame-Options | SAMEORIGIN |
| Content-Encoding | gzip |
| Vary | Accept-Encoding |
| X-XSS-Protection | 1; mode=block |
| Content-Length | 670 |

| | |
|---|---|
| X-Powered-By | Phusion Passenger (mod_rails/mod_rack) 3.0.12 |
| Content-Type | text/html;charset=utf-8 |

## Email

```
louis@pentesterlab.com
```

# ● HTML Comments

## What does this mean?

knowledge base (http://support.detectify.com/customer/en/portal/articles/2243487-html-comments).

## What can happen?

The snippets of code within comments will remain inactive until you remove the comment brackets.
The comments might also contain sensitive information not meant for the public.

## Summary

| Entry | Found at | CVSS |
|---|---|---|
| 1 | http://95.179.196.14/captcha/example2/ | 0 |

# 1. HTML Comments

## Summary

**Found At**
http://95.179.196.14/captcha/example2/

**Request URL**
http://95.179.196.14/captcha/example2/

**CVSS**
0 of 10.0

```
<!-- Le styles -->
```

```
<!--/.nav-collapse -->
```

```
<!-- /container -->
```