

* Cryptography related issues (Testing for weak cryptography)

1. weak ssl/tls protocols, ciphers, keys and insufficient transport layer protection

- Common issues:

1. ssl/tls protocol, ciphers, keys and renegotiation must be properly configured.

2. certificate validity must be ensured

3. software exposed must be updated due to possibility of known vulnerabilities.

4. usage of secure flag for session cookie.

5. HSTS

6. presence of both http and https.

7. presence of mixed https and http content in the same page, which can be used to leak information.

8. sensitive data transmitted in clear text.

1. ssl/tls protocol, ciphers, keys and renegotiation must be properly configured.

① weak protocols must be disabled.

(ssl v2 is enabled then there is a vulnerability)

② if renegotiation is possible then there is a vulnerability.

(it should be disabled)

③ if rsa or dsa is used the key must be at least 1024 bits encrypted

(if not then there is a vulnerability)

④ key must be generated with proper entropy.

⑤ md5/rdc should not be in used

⑥ server should be protected from beast as well as CRIME attack.

X with nmap you can recognition ssl service.

> nmap -sV --reason -PN -n --top-ports 100 target-ip

X Checking for certificate information, weak ciphers and sslv2 via nmap

> nmap --script ssl-enum-ciphers -p 443,465 target-ip

* checking for client-initiated renegotiation and secure renegotiation via openssl

```
> openssl s-client -connect target:443
```

Head / HTTP/1.1

8

Vulnerable results.

* Testing es6/tls vulnerabilities with sslyze script

> sslyze --regular target: 443
465

* Testing ssl/tls vulnerabilities with `testssl` script

> bash testssl.sh target

```
http://extension -D http://www.mozilla.org/ 2014-02-24  
[...]  
tbsat extension  
CCS (CVE-2014-0224)  
Ticketbleed (CVE-2016-9244), experiment.  
ion ticket extension  
ROBOT  
cipher suites that use RSA key transport  
Secure Renegotiation (CVE-2009-3555)  
Secure Client-Initiated Renegotiation  
timed out  
CRIME, TLS (CVE-2012-4929)  
BREACH (CVE-2013-3587)  
p HTTP compression. - only supplied "/" tested  
ges or if no secrets in the page  
POODLE, SSL (CVE-2014-3566)  
TLS_FALLBACK_SCSV (RFC 7507)  
tocol below TLS 1.2 offered (OK)  
SWEET32 (CVE-2016-2183, CVE-2016-6329)  
FREAK (CVE-2015-0204)  
DROWN (CVE-2016-0800, CVE-2016-0703)  
and port (OK)  
not vulnerable (OK)  
not vulnerable (OK), no sess  
Server does not support any  
not vulnerable (OK)  
likely not vulnerable (OK),  
not vulnerable (OK)  
potentially NOT ok, uses gzi  
Can be ignored for static pa  
not vulnerable (OK)  
No fallback possible, no pro  
not vulnerable (OK)  
not vulnerable (OK)  
not vulnerable on this host
```

```
1 URL: /
2
3 Attack details
4 This alert was issued because the following conditions were
met:
5
6 The page content is served via HTTPS
7 The server is using HTTP-level compression
8 URL encoded GET input redirect was reflected into the HTTP
response body.
9 HTTP response body contains a secret named csrf
10 The impact of this vulnerability
11 An attacker can leverage information leaked by compression to
recover targeted parts of the plaintext.
12 How to fix this vulnerability
13 The mitigations are ordered by effectiveness (not by their
practicality - as this may differ from one application to
another).
14
15 Disabling HTTP compression
16 Separating secrets from user input
17 Randomizing secrets per request
18 Masking secrets (effectively randomizing by XORing with a
random secret per request)
19 Protecting vulnerable pages with CSRF
20 Length hiding (by adding random number of bytes to the
responses)
21 Rate-limiting the requests
```

X SSL cookie without secure flag.

- ① sign up in any application and app will generate a cookie
- ② look in request body for cookie section, and there should be a secure flag. (parameter)

* Poodle attack (SSL v3 attack)

an attacker may be able to exploit this problem to conduct MITM attack and decrypt communication between the affected services and client.

```
> nmap -sV --version-light -Pn --script ssl-poodle -p 443 -iL Subdomains.txt
```

* Enumerate cipher

```
> nmap --script ssl-enum-ciphers -p 443 target
```

```
Host is up (0.10s latency).

PORT      STATE SERVICE
443/tcp    open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
```

```
> curl -v3 -X Head target → to test )
```

```
Nmap done: 1 IP address (1 host up) scanned in 10.10 seconds
root@kali:~# curl -v3 -X HEAD https://home.tomtom.com
Warning: Setting custom HTTP method to HEAD with -X/-request may not work the way you want. Consider using -I/--head instead.
* Trying 185.5.121.54...
* TCP_NODELAY set
* Connected to home.tomtom.com (185.5.121.54) port 443 (#0)
* OpenSSL was built without SSLv3 support → it is vulnerable
* Closing connection 0
curl: (4) OpenSSL was built without SSLv3 support
root@kali:~#
```

PORT	STATE	SERVICE	VERSION
443/tcp	open	ssl/http-proxy Varnish http accelerator	
		ssl-poodle:	↳ Vulnerable results
			SSL POODLE Information leak
			→ State: UNKNOWN
			IDs: OSVDB-113251 CVE: CVE-2014-3566
			The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext via padding-oracle attack, aka the "POODLE" issue.
			Disclosure date: 2014-10-14
			Check results:
			TLS_RSA_WITH_AES_128_CBC_SHA
			References:
			https://sevdb.org/113251
			https://www.openssl.org/~bodo/ssl-poodle.pdf
			https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

or you can use

SSLabs.com

2. Oracle padding

3. Testing for sensitive informations sent via unencrypted channel.

