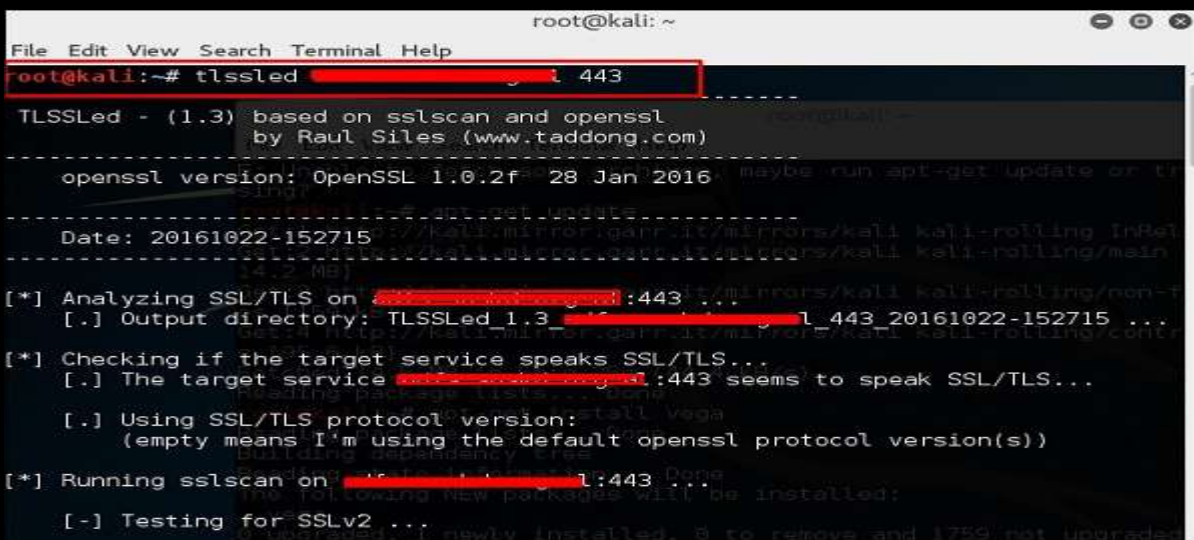


Website Penetration Testing-SSL Scanning Tools

TLSSLed is a Linux shell script used to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. It is based on **sslsan**, a thorough SSL/TLS scanner that is based on the **openssl** library, and on the “**openssl s_client**” command line tool.

The current tests include checking if the target supports the SSLv2 protocol, the NULL cipher, weak ciphers based on their key length (40 or 56 bits), the availability of strong ciphers (like AES), if the digital certificate is MD5 signed, and the current SSL/TLS renegotiation capabilities.

To start testing, open a terminal and type “**tlssled URL port**”. It will start to test the certificate to find data.

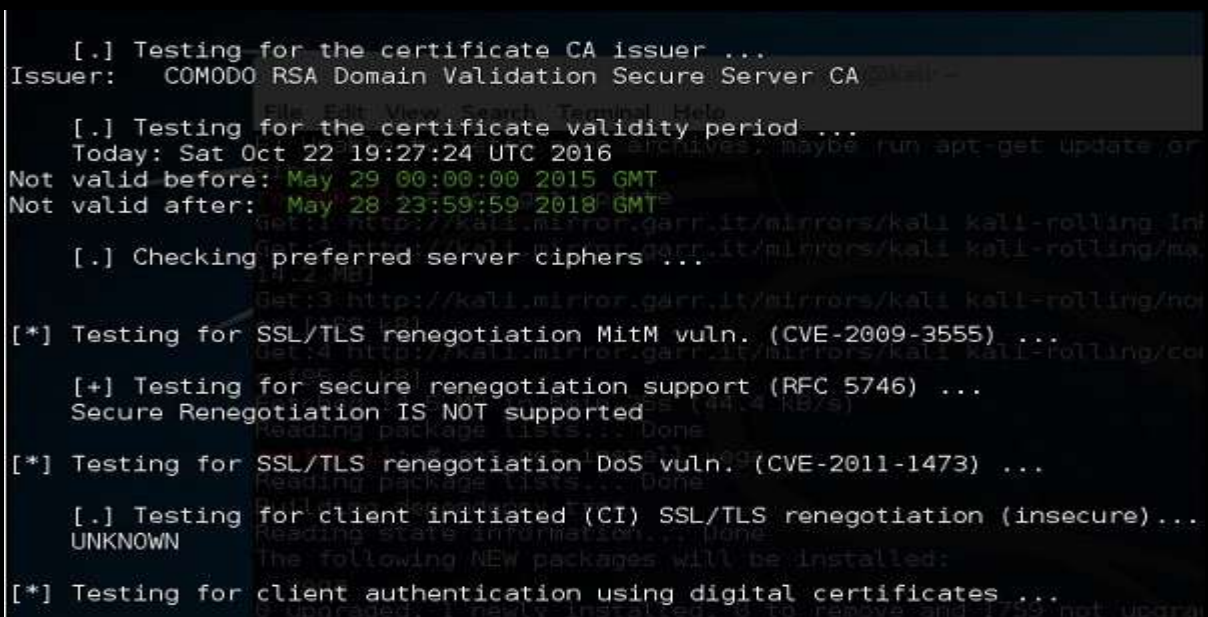


```
root@kali:~# tlssled http://kali.mirror.garr.it/ 443

TLSSLed - (1.3) based on sslscan and openssl
by Raul Siles (www.taddong.com)

-----
openssl version: OpenSSL 1.0.2f 28 Jan 2016. maybe run apt-get update or tr
-----
Date: 20161022-152715
-----
[*] Analyzing SSL/TLS on http://kali.mirror.garr.it/443...
[.] Output directory: TLSSLed 1.3 http://kali.mirror.garr.it/443 20161022-152715 ...
[*] Checking if the target service speaks SSL/TLS...
[.] The target service http://kali.mirror.garr.it/443 seems to speak SSL/TLS...
[.] Using SSL/TLS protocol version:
(empty means I'm using the default openssl protocol version(s))
[*] Running sslscan on http://kali.mirror.garr.it/443 ...
[.] Testing for SSLv2 ...
```

You can see from the finding that the certificate is valid until 2018 as shown in green in the following screenshot.



```
[.] Testing for the certificate CA issuer ...
Issuer: COMODO RSA Domain Validation Secure Server CA

[.] Testing for the certificate validity period ...
Today: Sat Oct 22 19:27:24 UTC 2016
Not valid before: May 29 00:00:00 2015 GMT
Not valid after: May 28 23:59:59 2018 GMT

[.] Checking preferred server ciphers ...

[*] Testing for SSL/TLS renegotiation MitM vuln. (CVE-2009-3555) ...
[+] Testing for secure renegotiation support (RFC 5746) ...
Secure Renegotiation IS NOT supported

[*] Testing for SSL/TLS renegotiation DoS vuln. (CVE-2011-1473) ...

[.] Testing for client initiated (CI) SSL/TLS renegotiation (insecure)...
UNKNOWN

[*] Testing for client authentication using digital certificates ...
```

w3af

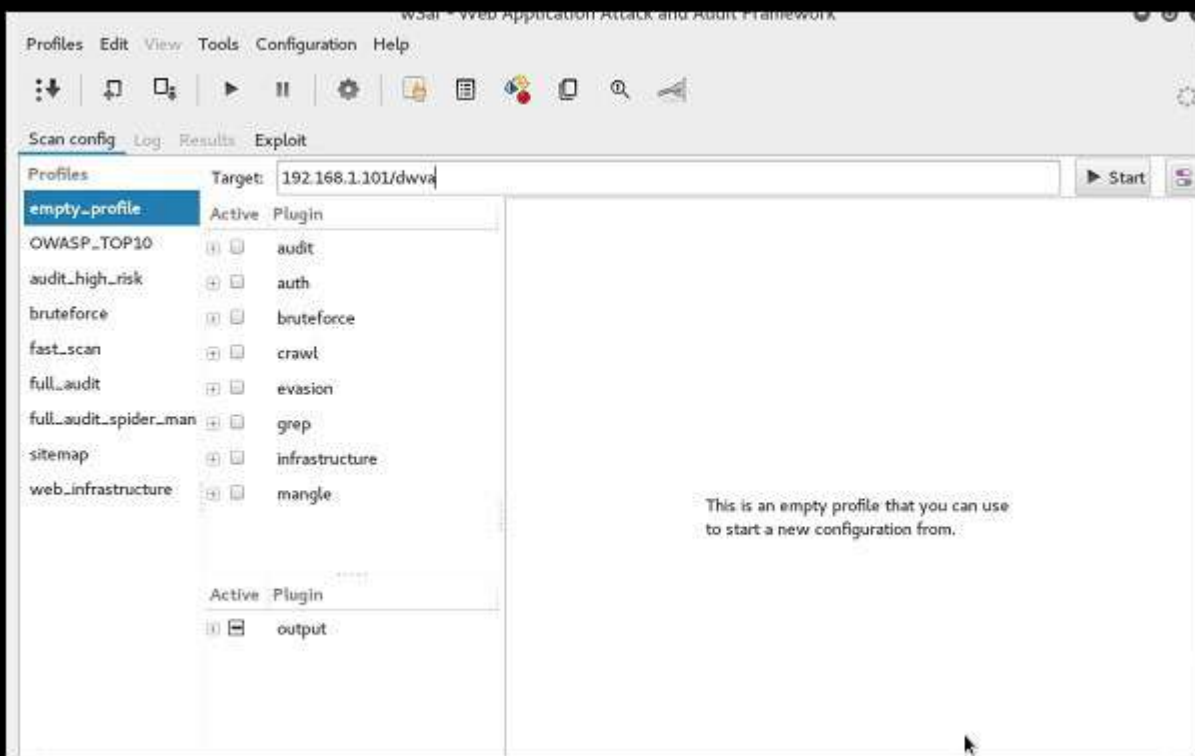
w3af is a Web Application Attack and Audit Framework which aims to identify and exploit all web application vulnerabilities. This package provides a Graphical User Interface (GUI) for the framework. If you want a command-line application only, install w3af-console.

The framework has been called the “metasploit for the web”, but it’s actually much more as it also discovers the web application vulnerabilities using black-box scanning techniques. The w3af core and its plugins are fully written in Python. The project has more than 130 plugins, which identify and exploit SQL injection, cross-site scripting (XSS), remote file inclusion and more.

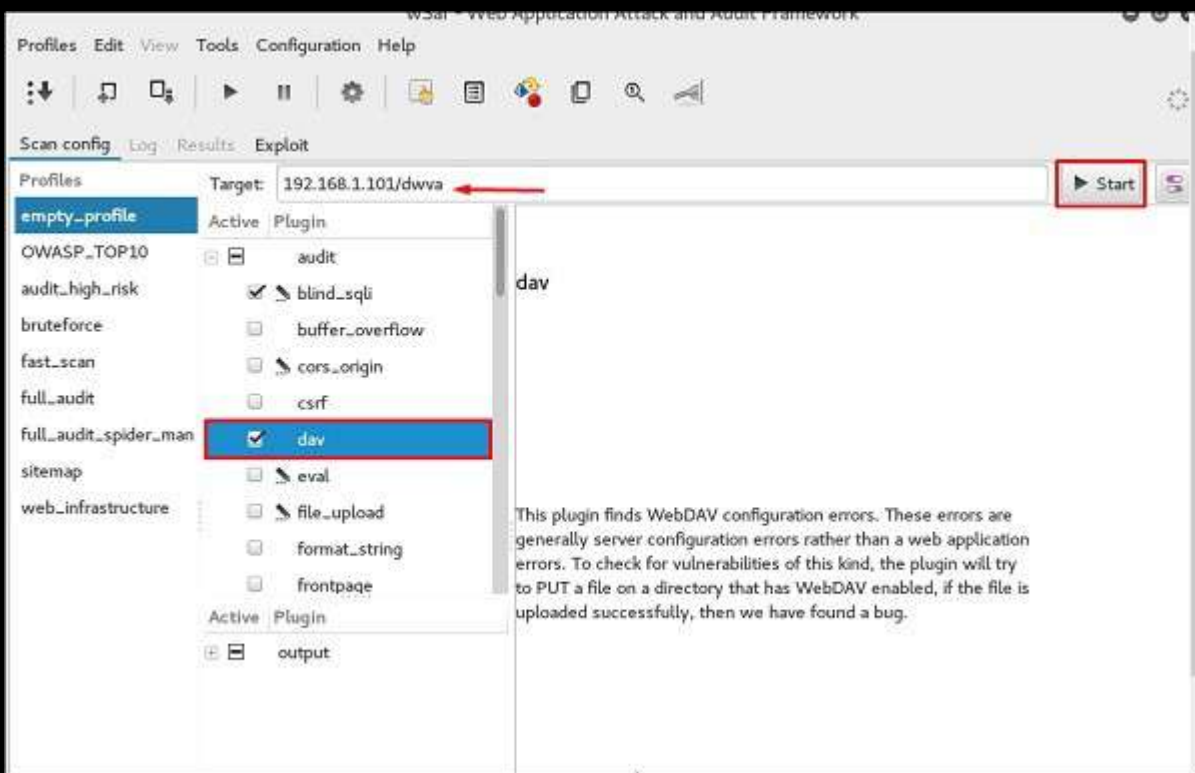
Step 1 – To open it, go to Applications → 03-Web Application Analysis → Click w3af.



Step 2 – On the “Target” enter the URL of victim which in this case will be metasploitable web address.



Step 3 – Select the profile → Click “Start”.



Step 4 – Go to “Results” and you can see the finding with the details.

w3af - [redacted]

Scan config Log Results Exploit

KB Browser URLs Request/Response navigator

☒ Vuln ☒ Info ☐ Misc

Knowledge Base

- ▼ XSS (1)
- ▼ XSS (29)
- ▼ sql (1)
- ▼ sql (2)
- ▼ SQL Injection
- ▼ SQL Injection

SQL Injection in a Unknown database was found at: "http://[redacted]/w3af/audit/sql_injection/select/sql_injection_string.php", using HTTP method GET. The sent data was: "name=d%27z%220". This vulnerability was found in the request with id 1725.

Request Response

Raw Headers

HTTP/1.1 200 OK
content-length: 368
content-encoding: gzip
x-powered-by: PHP/5.3.10-1ubuntu3.4
vary: Accept-Encoding
server: Apache/2.2.22 (Ubuntu)
date: Sat, 19 Jan 2013 20:17:18 GMT
content-type: text/html

Fatal error: Uncaught exception 'Exception' with message 'Error performing query: [redacted]users where name='d'z'0':
1064: 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 'z'0'' at line 1' in /var/www/[redacted]/w3af/audit/sql_injection/select/sql_injection_string.php:15
Stack trace:
#0 {main}
thrown in /var/www/[redacted]/w3af/audit/sql_injection/select/sql_injection_string.php on line 15

41 41 0