

# What is Web Application Penetration testing?

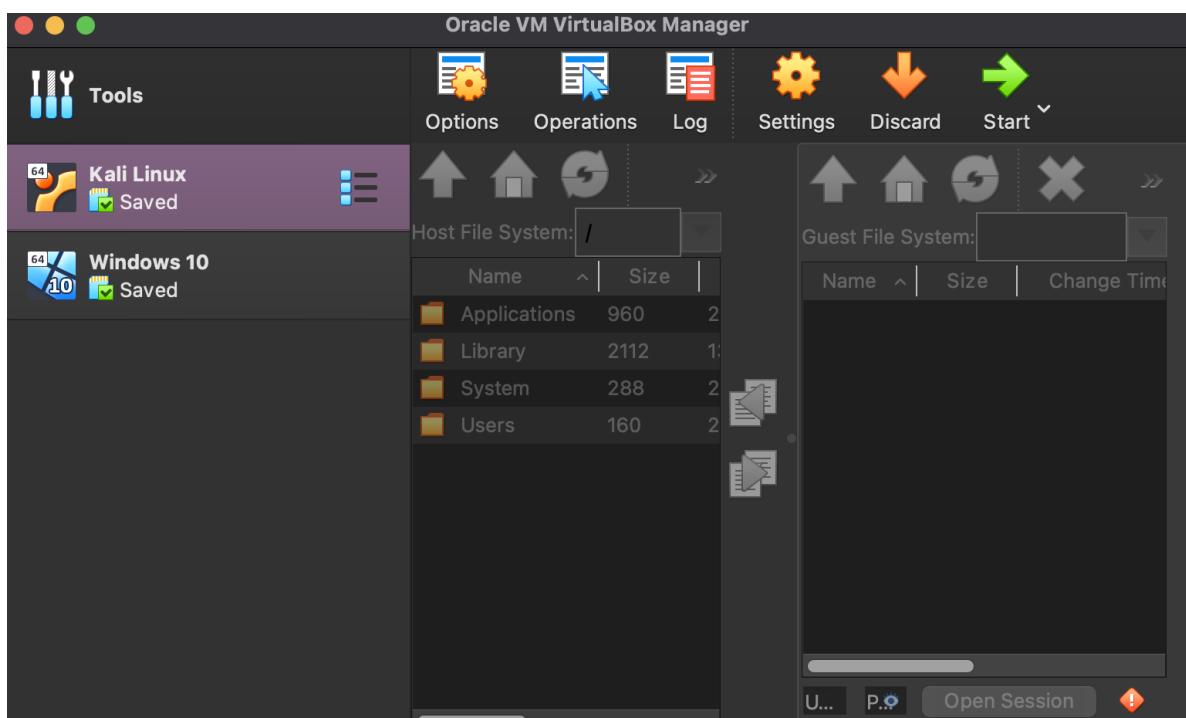
Web application penetration testing is a process of simulating an attack on a web application in order to identify and mitigate vulnerabilities. Kali Linux is a popular operating system that provides a range of tools for web application penetration testing.

## Installation Processes and my experience:

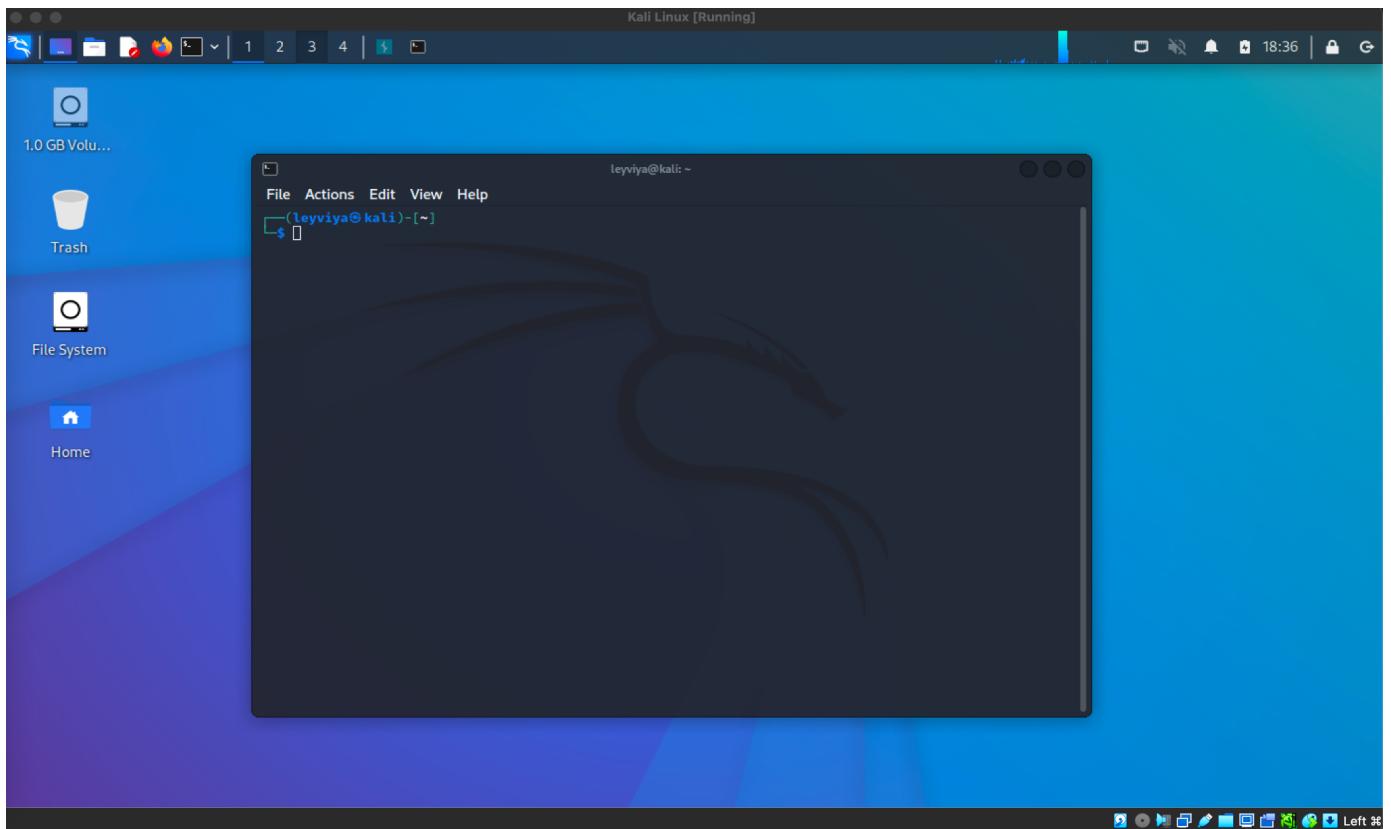
Mac computers do not natively support the Linux operating system, but you can install and run a Linux distribution such as Kali Linux on a Mac using virtualization software like VirtualBox. VirtualBox allows you to create a virtual machine on your Mac, which is a software simulation of a computer that runs within your existing Mac operating system. You can then install and run Kali Linux on the virtual machine, giving you the ability to use and test Kali Linux on your Mac without having to dual boot or replace your current operating system.

To install Kali Linux on a Mac using VirtualBox, you will need to first download and install VirtualBox on your Mac. Then, you can create a new virtual machine and follow the prompts to install Kali Linux on the virtual machine. Keep in mind that running Kali Linux on a virtual machine may not provide the same level of performance as running it on a dedicated physical machine, but it can be a useful way to experiment with and test Kali Linux on a Mac. Once VirtualBox is installed, open the application and click on the "New" button to create a new virtual machine. Give the virtual machine a name and select "Linux" as the type and "Debian (64-bit)" as the version. Click "Next" and specify the amount of memory you want to allocate to the virtual machine. Next, select "Create a virtual hard disk now" and click "Create." Choose "VDI (VirtualBox Disk Image)" as the hard disk file type and click "Next." Select "Dynamically allocated" as the storage on the physical hard disk option and click "Next." Finally, specify the size of the virtual hard disk and click "Create."

Once the virtual machine has been created, click on the "Start" button to begin the installation process. Follow the prompts to install Kali Linux on the virtual machine. Once the installation is complete, you will be able to boot into Kali Linux on your Mac using VirtualBox.



Homescreen and terminal installed “Kali Linux” on my local machine via VirtualBox.



## Web Application Analysis processes that I've done in this project:

1. Burp Suite

2. Nikto

3. SQLMap

4. Whatweb

5. Maltego

6. Skipfish

7. Whois

8. Wpscan

9. Commix

## Burp Suite processes and analysis

Burp Suite is a comprehensive tool for web application analysis that includes a number of features such as a web proxy, a web application scanner, and a manual testing interface.

The screenshot shows the Burp Suite Free Edition v1.6 interface. At the top, there's a toolbar with various tabs: Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, and Alerts. The 'Intruder' tab is currently selected. Below the toolbar, there's a status bar with 'Burm 9.0; Windows NT 6.1; Win64; x64; Trident/5.0'. The main area has two panes: a left pane showing a tree view of targets (including 'owaspbwa OWASP Broken Web Applications', 'Metasploitable2 - Linux', 'Burp Suite Free Edition', 'OWASP Mutillidae II: Web Pwn I', 'Magical Code Injection F...', 'Broken WordPress', and 'Metasploitable2'), and a right pane showing the 'Burp Suite Free Edition v1.6' window. In the right pane, a context menu is open over the 'mutillidae' target in the tree view. The menu options include 'Remove from scope', 'Spider from here' (highlighted with a red arrow), 'Do an active scan', 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Comparer', 'Request in browser', 'Engagement tools [Pro version only]', 'Compare site maps', 'Delete item', 'Copy URL', and 'Coov as curl command'. A red arrow points to the 'Spider from here' option, with the text 'Select Spider From Here Option' overlaid.

**Target** **Proxy** **Spider** **Scanner** **Intruder** **Repeater** **Sequencer** **Decoder** **Comparer** **Extender** **Options** **Alerts**

**Site map** **Scope**

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title
http://192.168.0.160	GET	/mutillidae/index.php		200	39045	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	37673	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	39534	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	39349	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	37299	script	
http://192.168.0.160	GET	/mutillidae/index.php...		302	626	HTML	
http://192.168.0.160	GET	/mutillidae/index.php...		302	610	HTML	
http://192.168.0.160	GET	/mutillidae/index.php...		302	634	HTML	
http://192.168.0.160	GET	/mutillidae/index.php...		302	608	HTML	
http://192.168.0.160	GET	/mutillidae/index.php...		302	630	HTML	
http://192.168.0.160	GET	/mutillidae/index.php...		302	615	HTML	

**Response from the Target**

HTTP/1.1 200 OK  
Date: Wed, 12 Aug 2015 06:07:26 GMT  
Server: Apache/2.2.14 (Ubuntu) mod\_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch  
proxy\_html/3.0.1 mod\_python/3.3.1 Python/2.6.5 mod\_ssl/2.2.14 OpenSSL/0.9.8k  
Phusion Passenger/3.0.17 mod\_perl/2.0.4 Perl/v5.10.1  
X-Powered-By: PHP/5.3.2-1ubuntu4.5  
Server Headers  
Logged-In-User:  
Vary: Accept-Encoding

**Site map** **Scope**

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title
http://192.168.0.160	GET	/mutillidae/index.php		200	39045	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	37673	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	39534	script	
http://192.168.0.160	GET	/mutillidae/index.php...		200	39349	script	

**Page Source**

```
<link rel="stylesheet" type="text/css" href=".//styles/global-styles.css" />
<link rel="stylesheet" type="text/css" href=".//styles/ddsmoothmenu/ddsmoothmenu.css" />
<link rel="stylesheet" type="text/css" href=".//styles/ddsmoothmenu/ddsmoothmenu-v.css" />

<script type="text/javascript" src=".//javascript/bookmark-site.js"></script>
<script type="text/javascript" src=".//javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
<script type="text/javascript" src=".//javascript/ddsmoothmenu/jquery.min.js">
*****
 * Smooth Navigational Menu - (c) Dynamic Drive DHTML code library
 (www.dynamicdrive.com)
 * This notice MUST stay intact for legal use
 * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code
 ****
</script>
```

**Target** **Proxy** **Spider** **Scanner** **Intruder** **Repeater** **Sequencer** **Decoder** **Comparer** **Extender** **Options** **Alerts**

**Control** **Options**

**Spider Status**

Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".

**Spider is running** **Clear queues**

Requests made: 369  
Bytes transferred: 3,548,131  
Requests queued: 0  
Forms queued: 0

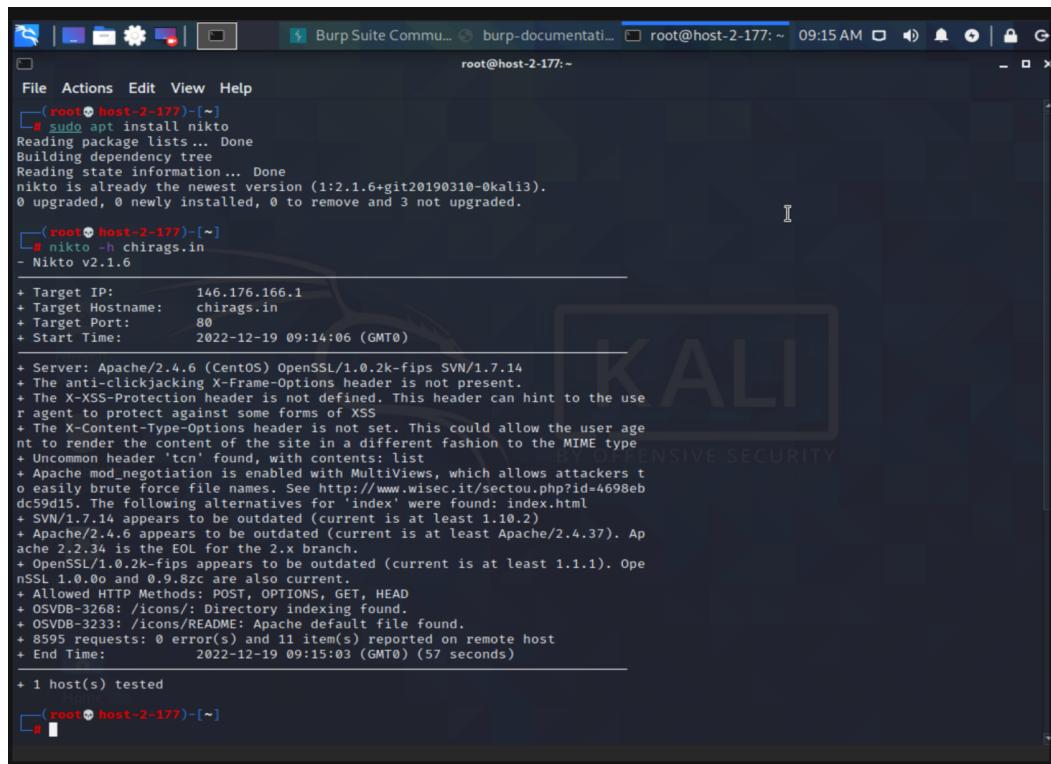
**Spider Scope**

Use suite scope [defined in Target tab]  
 Use custom scope

## Nikto processes and analysis

Nikto is a tool for identifying vulnerabilities in web servers and web applications. It can be used to scan a web application and identify any known vulnerabilities or misconfigurations that may be present. Here is a simple example of how you can use Nikto in Kali Linux:

Screenshots from application:



```
(root@host-2-177) [~]
# sudo apt install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
nikto is already the newest version (1:2.1.6+git20190310-0kali3).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.

(root@host-2-177) [~]
# nikto -h chirags.in
- Nikto V2.1.6

+ Target IP:          146.176.166.1
+ Target Hostname:    chirags.in
+ Target Port:        80
+ Start Time:         2022-12-19 09:14:06 (GMT0)

+ Target: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with Multiviews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ SVN/1.7.14 appears to be outdated (current is at least 1.10.2)
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOF for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8595 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2022-12-19 09:15:03 (GMT0) (57 seconds)

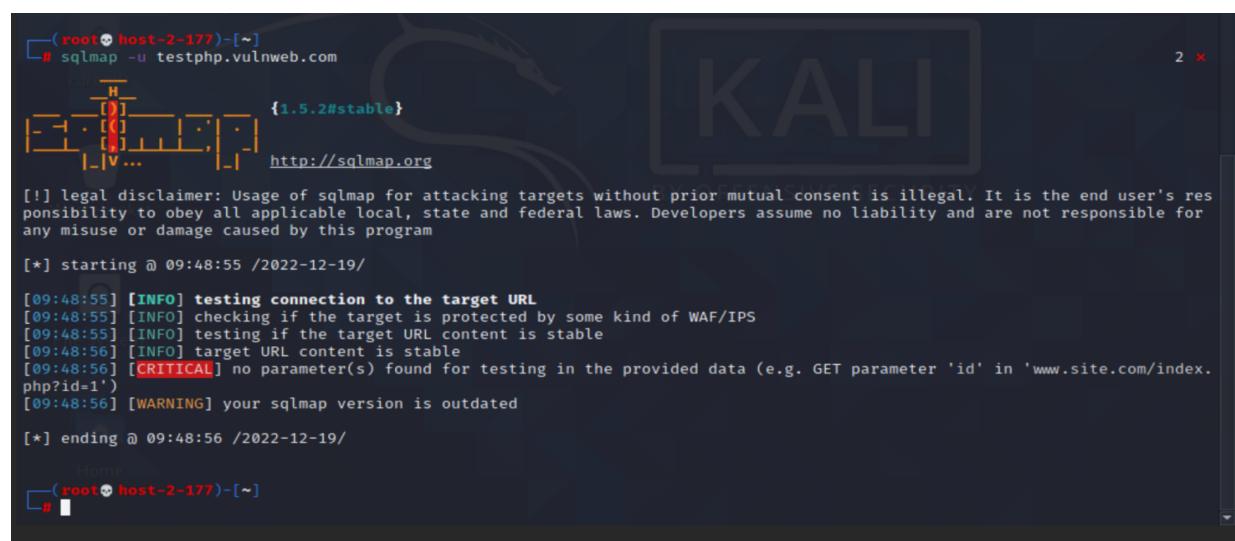
+ 1 host(s) tested

(root@host-2-177) [~]
```

## SQLMap Processes and Analysis

SQLMap is a tool for detecting and exploiting SQL injection vulnerabilities in web applications. It can be used to identify and exploit vulnerabilities in a web application by injecting malicious SQL commands into the database. Here is a brief and simple summary of how you can use SQLMap in Kali Linux to analyze a web application for SQL injection vulnerabilities:

Screenshots from Kali Linux:



```
(root@host-2-177) [~]
# sqlmap -u testphp.vulnweb.com
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 09:48:55 /2022-12-19/
[09:48:55] [INFO] testing connection to the target URL
[09:48:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:48:55] [INFO] testing if the target URL content is stable
[09:48:56] [INFO] target URL content is stable
[09:48:56] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[09:48:56] [WARNING] your sqlmap version is outdated
[*] ending @ 09:48:56 /2022-12-19/
Home
(root@host-2-177) [~]
#
```

## Whatweb Processes and Analysis

WhatWeb is a tool that is included in Kali Linux and is used for identifying the technologies that are used by websites. It can be used to gather information about a website's server-side software, client-side software, and other technical details. This information can be useful for a variety of purposes, such as website security testing, web development, and competitive analysis.

```
File Actions Edit View Help
* Scan reddit.com slashdot.org with verbose plugin descriptions.
./whatweb -v reddit.com slashdot.org

* An aggressive scan of wired.com detects the exact version of WordPress.
./whatweb -a 3 www.wired.com

* Scan the local network quickly and suppress errors.
whatweb --no-errors 192.168.0.0/24

* Scan the local network for https websites.
whatweb --no-errors --url-prefix https:// 192.168.0.0/24

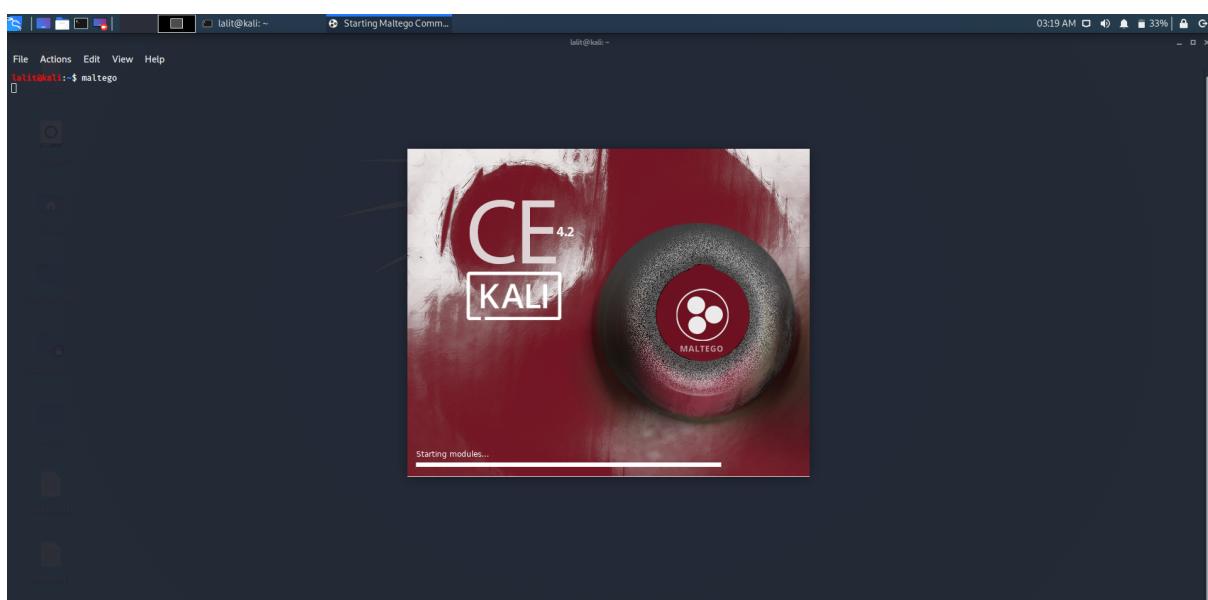
* Scan for crossdomain policies in the Alexa Top 1000.
./whatweb -i plugin-development/alexa-top-100.txt \
--url-suffix /crossdomain.xml -p crossdomain_xml

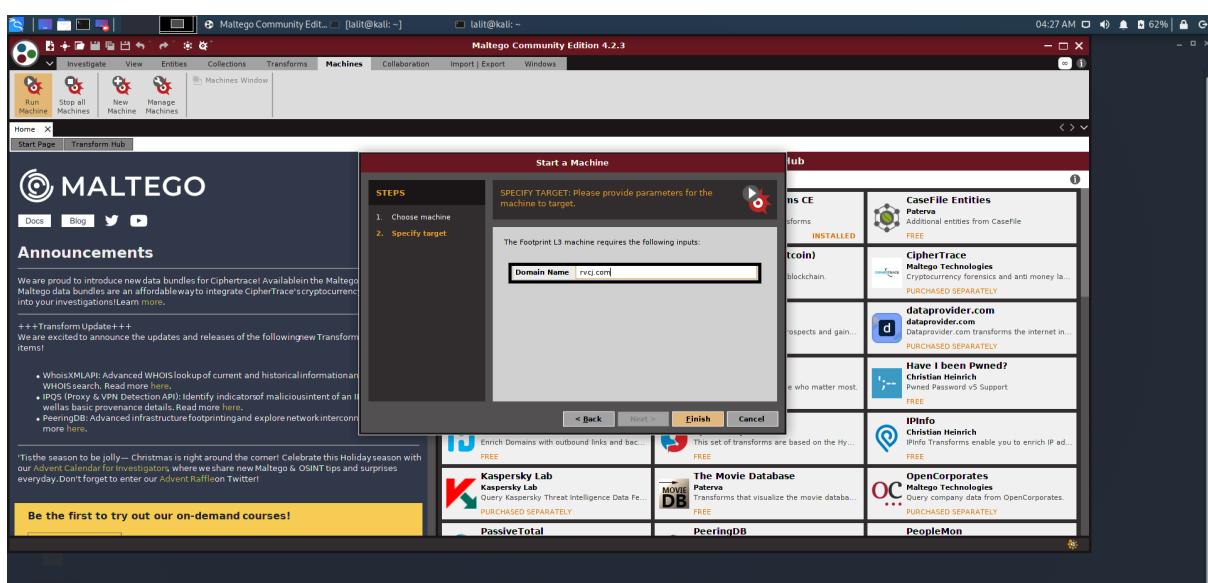
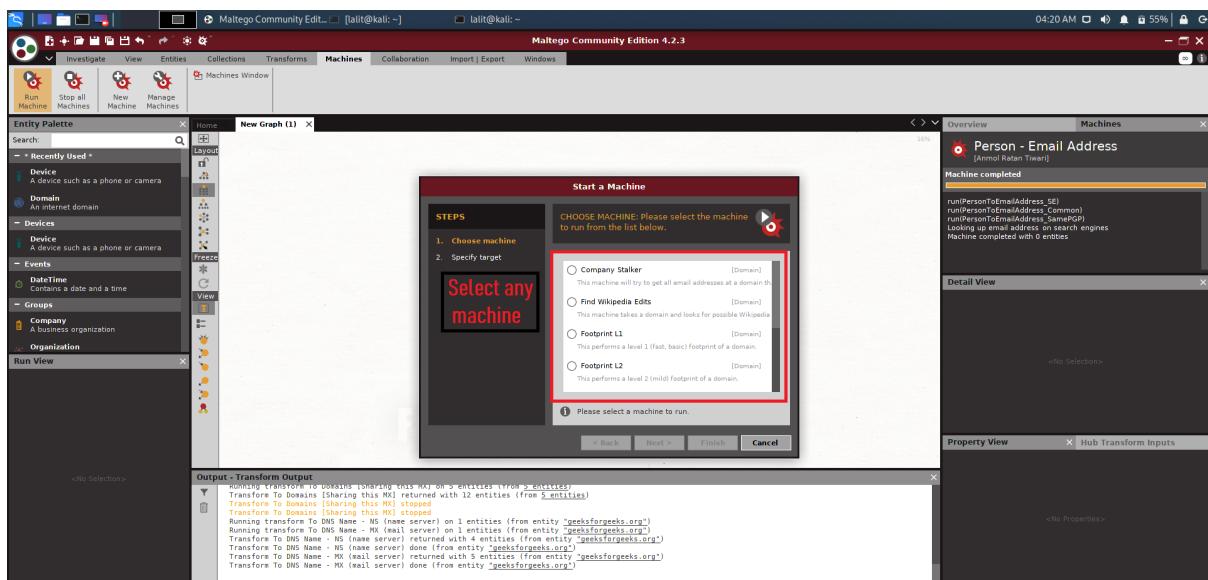
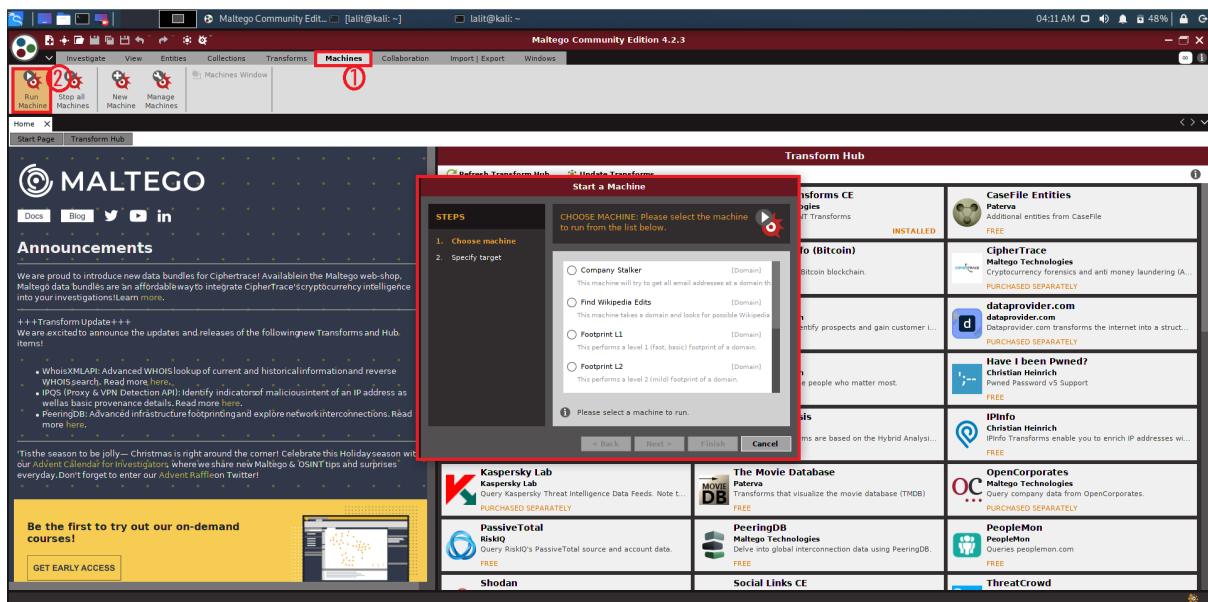
(leyviya㉿kali)-[~]
$ whatweb leyviya.github.io
http://leyviya.github.io [301 Moved Permanently] HTTPServer[GitHub.com], IP[185.199.110.153], RedirectLocation[UncommonHeaders[permissions-policy,x-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastrly-request-id], V https://leyviya.github.io/ [200 OK] Bootstrap, Email[leyla.violetta05@gmail.com], HTML5, HTTPServer[GitHub.com] FirstName], Script, Strict-Transport-Security[max-age=31556952], Title[Leyla Abdullayeva], UncommonHeaders[per-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastrly-request-id], Via-Proxy[1.1 varnish], X-UA-Compatible[chrome]

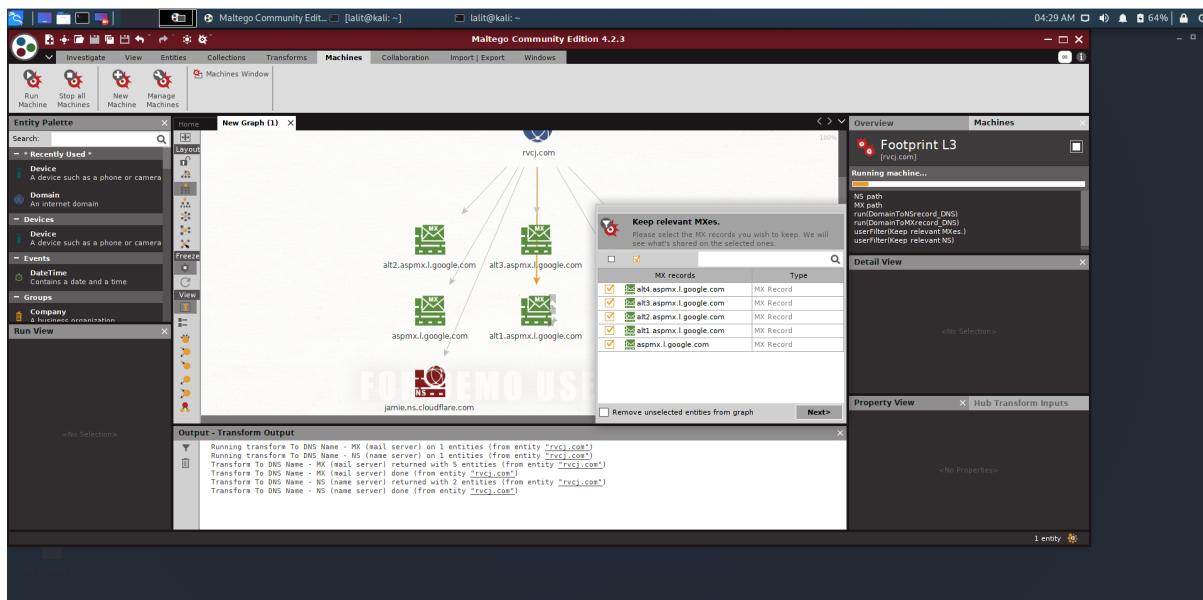
(leyviya㉿kali)-[~]
$ 
```

## Maltego

Maltego is a tool for performing open-source intelligence (OSINT) analysis and visualizing the relationships between different entities. It can be used to analyze a web application and identify any potential vulnerabilities or security risks. Here is a simple example of how you can use Maltego in Kali Linux:







## Skipfish

Skipfish is a web application security scanner that can be used to identify vulnerabilities in web applications. It is a tool that is included in the Kali Linux distribution, which is a Linux distribution specifically designed for penetration testing and digital forensics.

```

elp
leyviya@kali: ~

File Actions Edit View Help
[~]: Temporary failure in name resolution
skipfish version 2.10b by lcamtuf@google.com

- 192.168.1.202 -
[~]: Temporary failure in name resolution

Scan statistics:

  Scan time : 0:00:37.047
  HTTP requests : 2 (0.1/s), 0 kB in, 0 kB out (0.0 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 2 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 2 total (1.0 req/conn)
  TCP faults : 0 failures, 2 timeouts, 0 purged
  External links : 0 skipped
  Reqs pending : 0

Database statistics:

  Pivots : 3 total, 3 done (100.00%)
  In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 0 spotted
  Node types : 1 serv, 1 dir, 0 file, 0 pinfo, 1 unkn, 0 par, 0 val
  Issues found : 0 info, 2 warn, 0 low, 0 medium, 0 high impact
  Dict size : 5 words (5 new), 0 extensions, 0 candidates
  Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 3
[+] Looking for duplicate entries: 3
[+] Counting unique nodes: 3
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 3
[+] Generating summary views...
[+] Report saved to '202/index.html' [0x3bd7d896].
[+] This was a great day for science!

(leyviya@kali)-[~]
$
```

## Whois

WHOIS is a network protocol used to query databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The WHOIS service is provided by various organizations and is typically used to identify the owner of a domain name, or to look up technical and administrative information about a domain, IP address, or network.

```
%C  
(base) layyi@layla-MacBook-Pro ~ % whois google.com  
% IANA WHOIS server  
% For more information on IANA, visit http://www.iana.org  
% This query returned 1 object  
  
refer: whois.verisign-grs.com  
  
domain: COM  
  
organisation: VeriSign Global Registry Services  
address: 12061 Blumenthal Way  
address: Reston VA 20198  
address: United States of America (the)  
  
contact: administrative  
name: Registry Customer Service  
organisation: VeriSign Global Registry Services  
address: 12061 Blumenthal Way  
address: Reston VA 20198  
address: United States of America (the)  
phone: +1 703 925-4999  
fax-no: +1 703 948 3978  
e-mail: info@verisign-grs.com  
  
contact: technical  
name: Registry Customer Service  
organisation: VeriSign Global Registry Services  
address: 12061 Blumenthal Way  
address: Reston VA 20198  
address: United States of America (the)  
phone: +1 703 925-4999  
fax-no: +1 703 948 3978  
e-mail: info@verisign-grs.com  
  
nserver: A.GTLD-SERVERS.NET 192.5.6.30 2001:503:ab3e:0:0:0:2:30  
nserver: B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30  
nserver: C.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30  
nserver: D.GTLD-SERVERS.NET 192.31.88.30 2001:503:356a:10:0:0:0:30  
nserver: E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30  
nserver: F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30  
nserver: G.GTLD-SERVERS.NET 192.42.93.30 2001:503:ee3d:0:0:0:0:30  
nserver: H.GTLD-SERVERS.NET 192.54.112.38 2001:502:8cc0:0:0:0:0:30  
nserver: I.GTLD-SERVERS.NET 192.54.112.38 2001:502:8cc0:0:0:0:0:30  
nserver: J.GTLD-SERVERS.NET 192.48.79.30 2001:503:7994:0:0:0:0:30  
nserver: K.GTLD-SERVERS.NET 192.52.176.38 2001:503:d201:0:0:0:0:30  
nserver: L.GTLD-SERVERS.NET 192.41.162.38 2001:500:d937:0:0:0:0:30  
nserver: M.GTLD-SERVERS.NET 192.55.83.38 2001:501:b1f9:0:0:0:0:30  
ds-data: 30909 8 2 ed3dc916fdeecac73294e826fb5885044a833fc5459588f4a9184fc41a5766  
  
whois: whois.verisign-grs.com  
  
status: ACTIVE  
remarks: Registration information: http://www.verisigninc.com  
  
created: 1986-01-01  
changed: 2019-08-14  
source: IANA  
  
# whois.verisign-grs.com  
  
Domain Name: GOOGLE.COM  
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
```

```
Registry Domain ID: 2138514_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z  
Creation Date: 1997-09-15T04:00:00Z  
Registrar Expiry Date: 2028-09-14T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2086851750  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM  
Name Server: NS4.GOOGLE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-12-29T10:35:38Z <<  
  
# whois.markmonitor.com  
  
Domain Name: google.com  
Registry Domain ID: 2138514_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z  
Creation Date: 1997-09-15T07:00:00Z  
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000  
Registrar: MarkMonitor, Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2086850779  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Registrant Organization: Google LLC  
Registrant State/Province: CA  
Registrant Country: US  
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com  
Admin Organization: Google LLC  
Admin State/Province: CA  
Admin Country: US  
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com  
Tech Organization: Google LLC  
Tech State/Province: CA  
Tech Country: US  
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com  
Name Server: ns1.google.com  
Name Server: ns2.google.com  
Name Server: ns4.google.com  
Name Server: ns1.google.com  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2022-12-29T10:35:58+0000 <<
```

## Wpscan

WPSCAN is a command-line tool used to scan WordPress websites and identify any security vulnerabilities. It is included in the Kali Linux distribution, a collection of open-source tools used for ethical hacking and penetration testing.

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:07 ←

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - kwheel / cutiepie1
Trying kwheel / dallas1 Time: 00:05:05 <----- Red box highlights this line

[!] Valid Combinations Found:
| Username: kwheel, Password: cutiepie1 ←

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Aug 19 14:03:57 2022
[+] Requests Done: 3007
[+] Cached Requests: 30
[+] Data Sent: 1.488 MB
[+] Data Received: 1.749 MB
[+] Memory used: 251.238 MB
[+] Elapsed time: 00:05:59
```

## Commix

Commix (short for [Command Injection exploiter]) is a tool that can be used to test web applications for command injection vulnerabilities. It is included in the Kali Linux distribution, a collection of open-source tools used for ethical hacking and penetration testing.

```
root@kali:~# commix -h
Usage: commix [option(s)]

Options:
-h, --help           Show help and exit.

General:
These options relate to general matters.

-v VERBOSE          Verbosity level (0-4, Default: 0).
--version           Show version number and exit.
--output-dir=OUT.. Set custom output directory path.
-s SESSION_FILE     Load session from a stored (.sqlite) file.
--flush-session    Flush session files for current target.
--ignore-session   Ignore results stored in session file.
-t TRAFFIC_FILE    Log all HTTP traffic into a textual file.
--batch             Never ask for user input, use the default behaviour.
--encoding=ENCOD..  Force character encoding used for data retrieval (e.g.
                   GBK).
--charset=CHARSET   Time-related injection charset (e.g.
                   "0123456789abcdef")
--check-internet   Check internet connection before assessing the target.

Target:
This options has to be provided, to define the target URL.

-u URL, --url=URL  Target URL.
--url-reload       Reload target URL after command execution.
-l LOGFILE         Parse target from HTTP proxy log file.
```