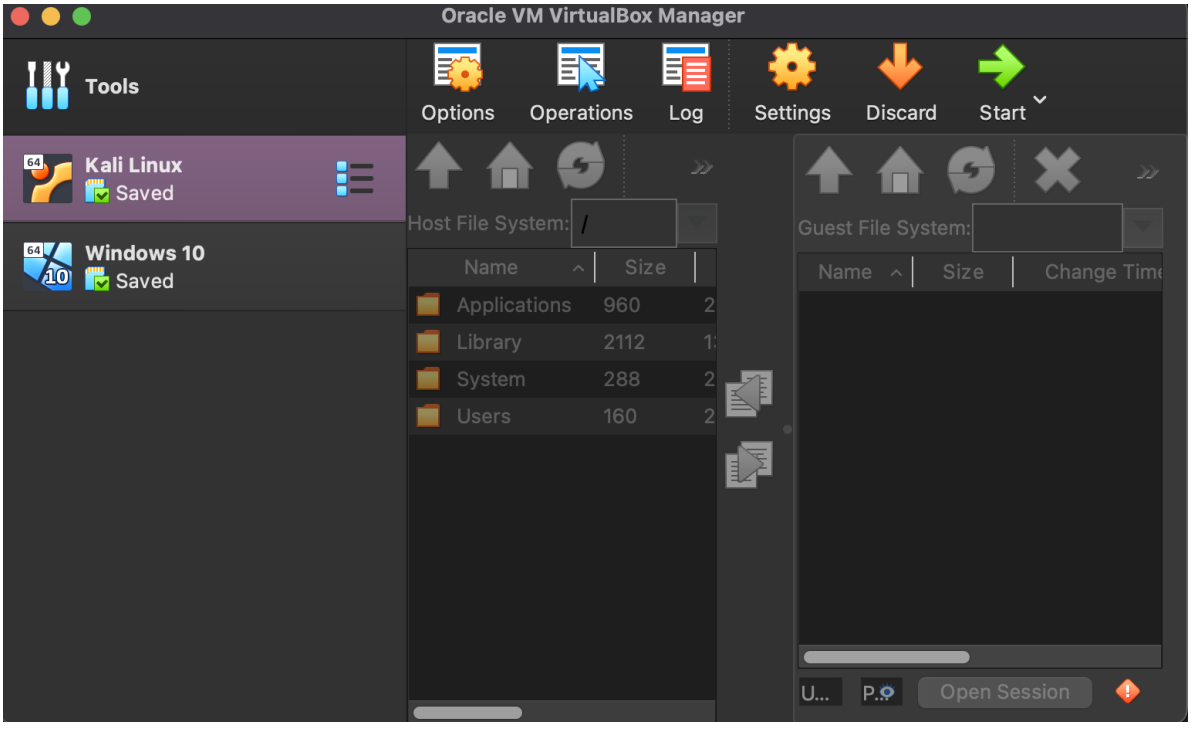
What is Web Application Penetration testing?

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.

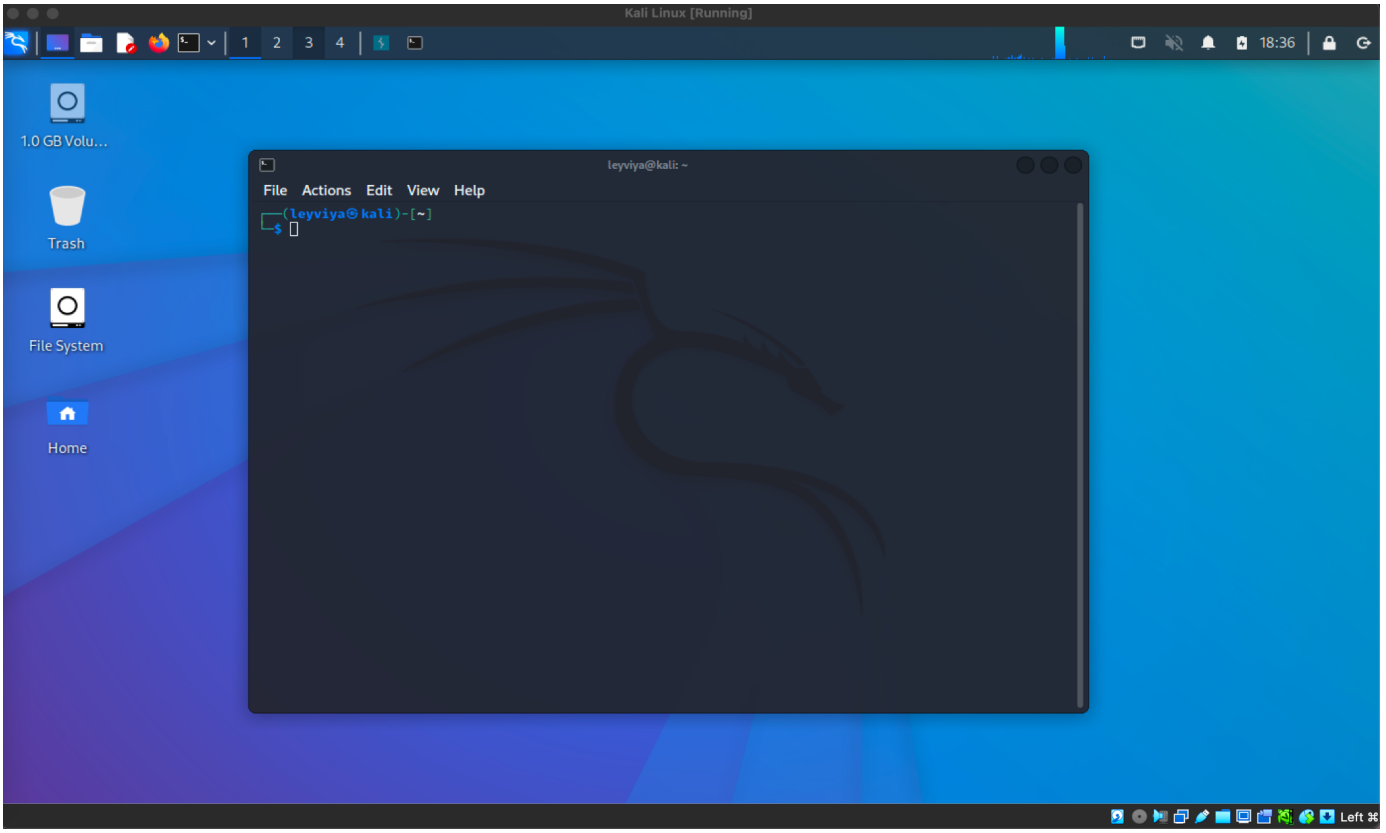
Installation Processes and my experience:

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.

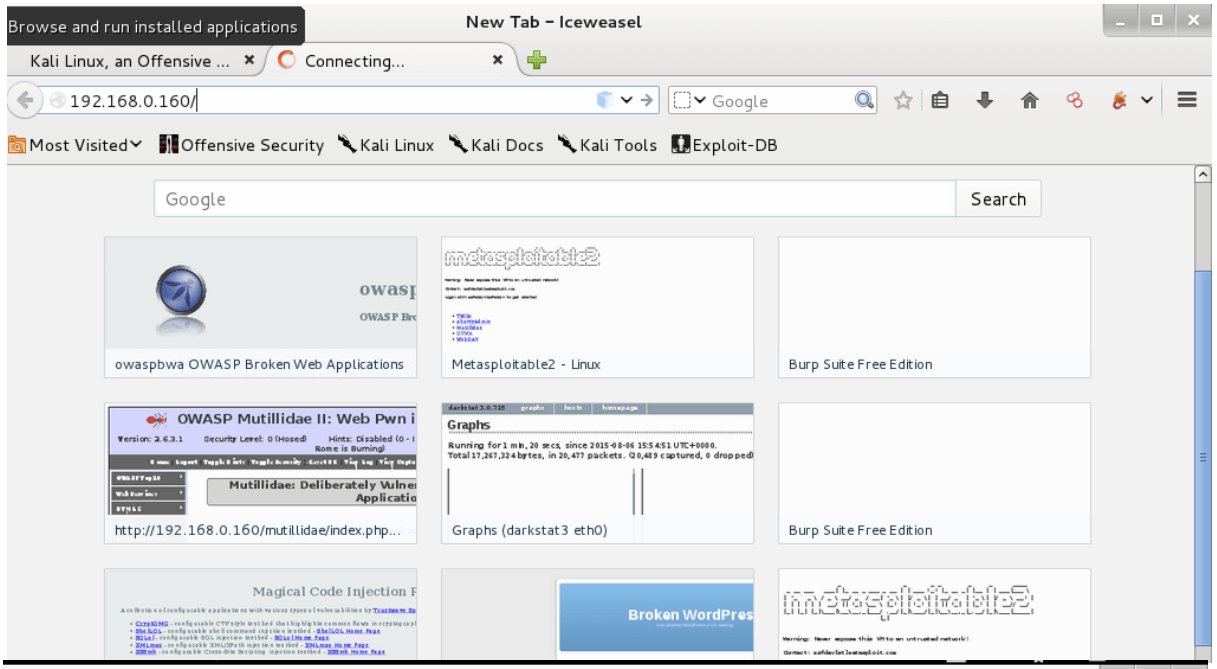


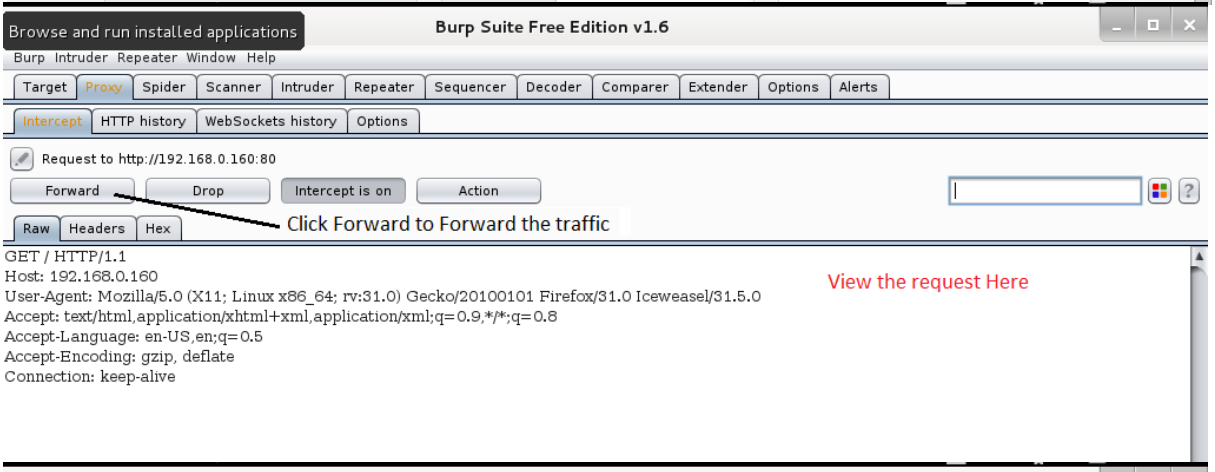
Web Application Analysis processes that I’ve done in this project:

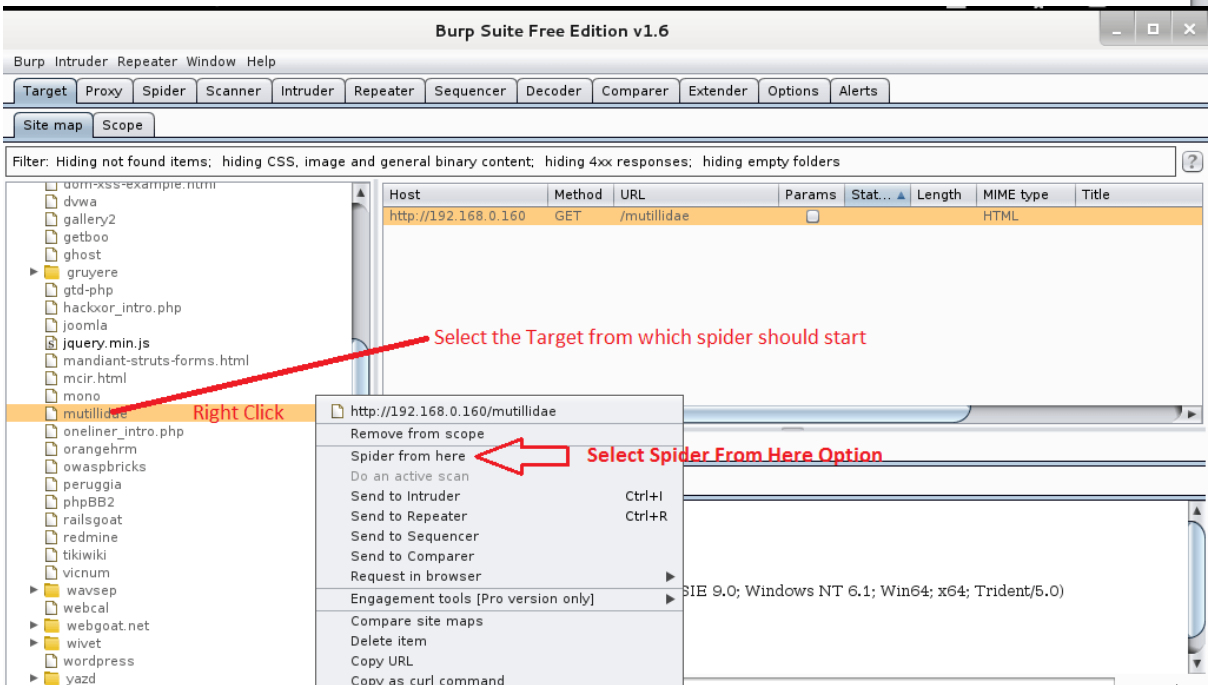
1. **Burp Suite**
2. **Nikto**
3. **SQLMap**
4. **Whatweb**
5. **Maltego**
6. **Skipfish**
7. **Whois**
8. **Wpscan**
9. **Commix**

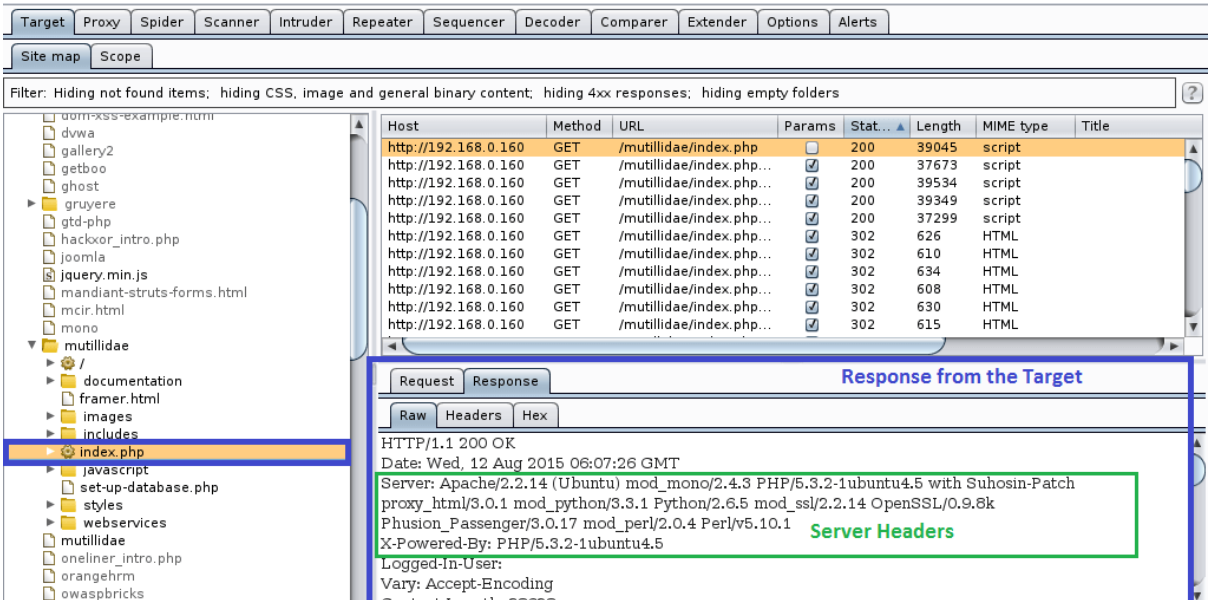
Burp Suite processes and analysis

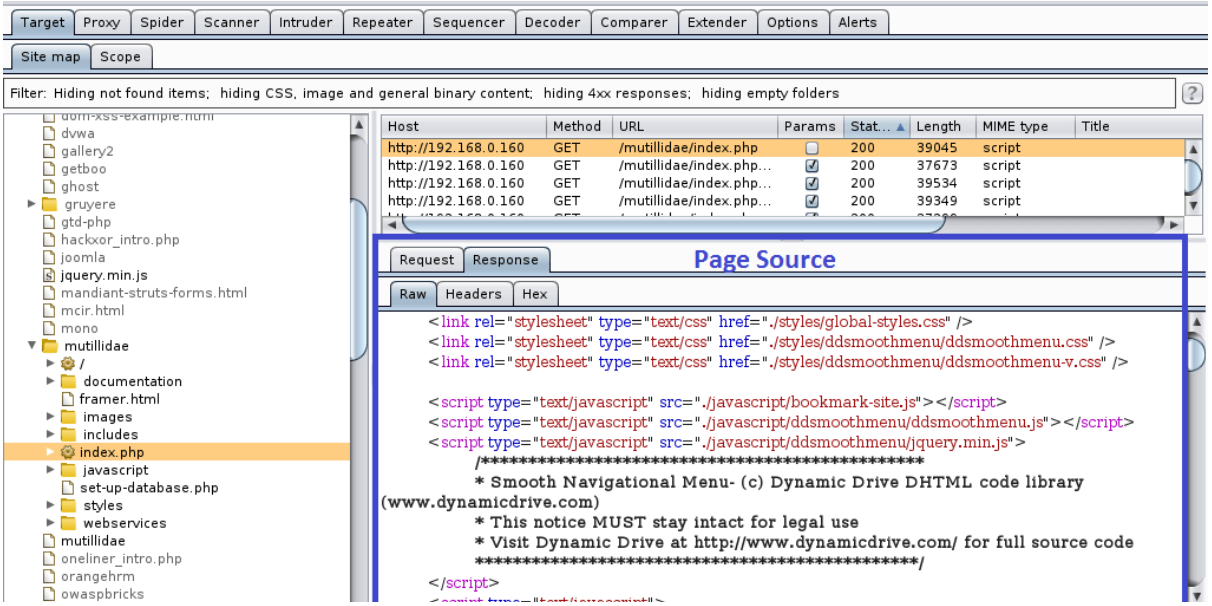
Burp Suite is a comprehensive tool for web application analysis that includes a number of features such as a web proxy, a web application scanner, and a manual testing interface.

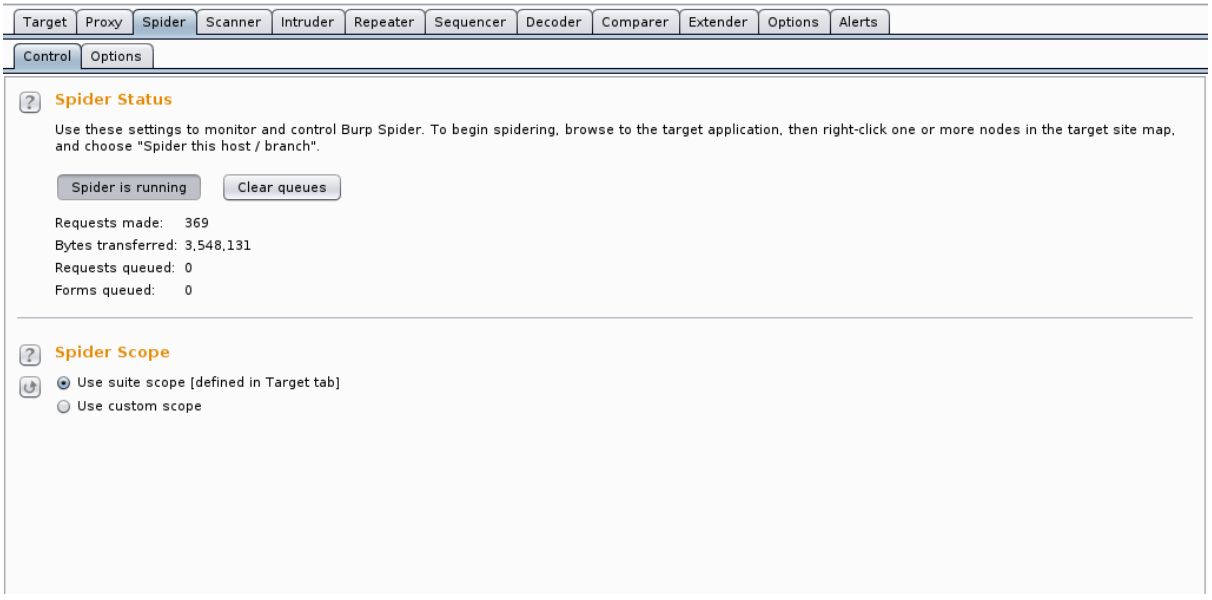







Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Stat... Length MIME type Title
http://192.168.0.160 GET /mutillidae/index.php 200 39045 script
Request Response
Response from the Target
Raw Headers Hex
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

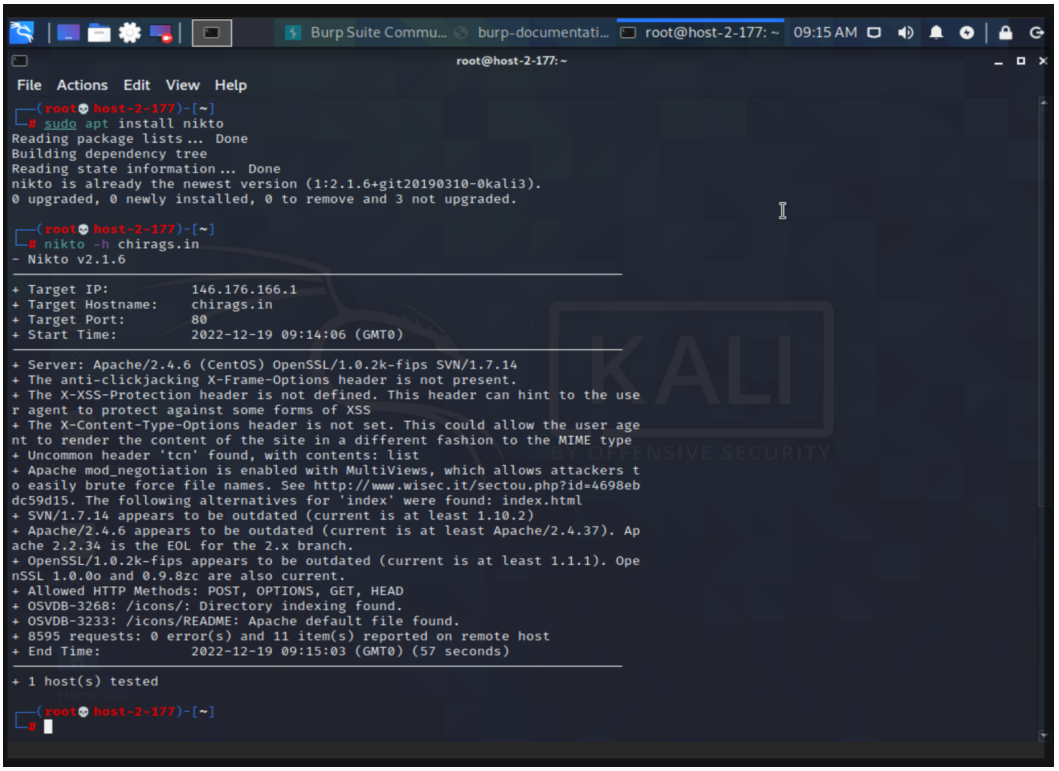

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Request Response
Page Source
Raw Headers Hex
<link rel="stylesheet" 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

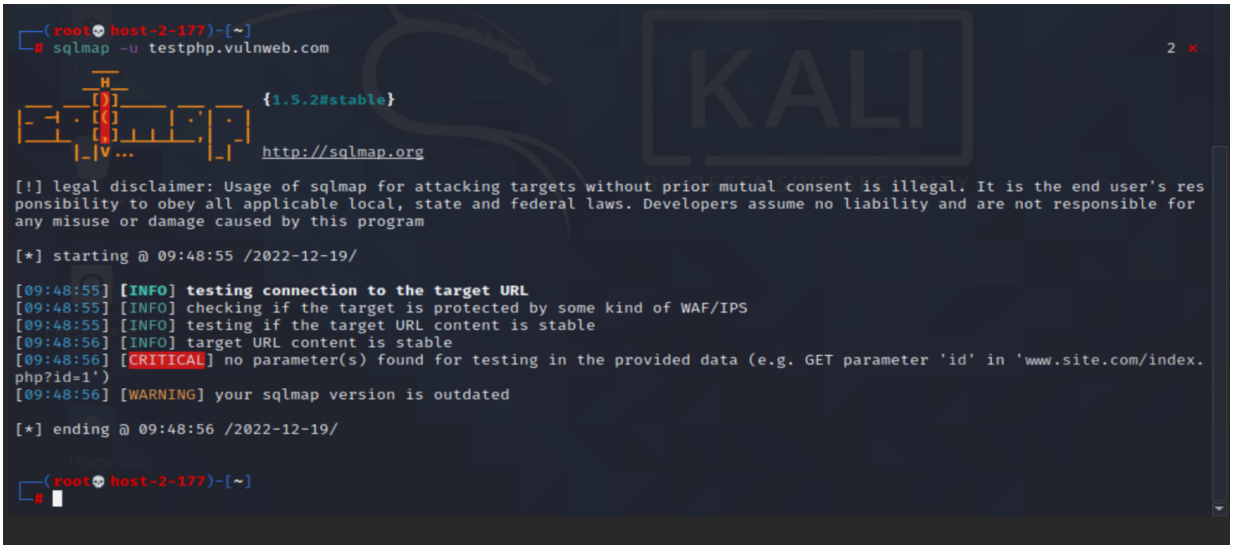
Nikto is a tool for identifying vulnerabilities in web servers and web applications. It can be used to scan a web application and identify any known vulnerabilities or misconfigurations that may be present. Here is a simple example of how you can use Nikto in Kali Linux:

Screenshots from application:



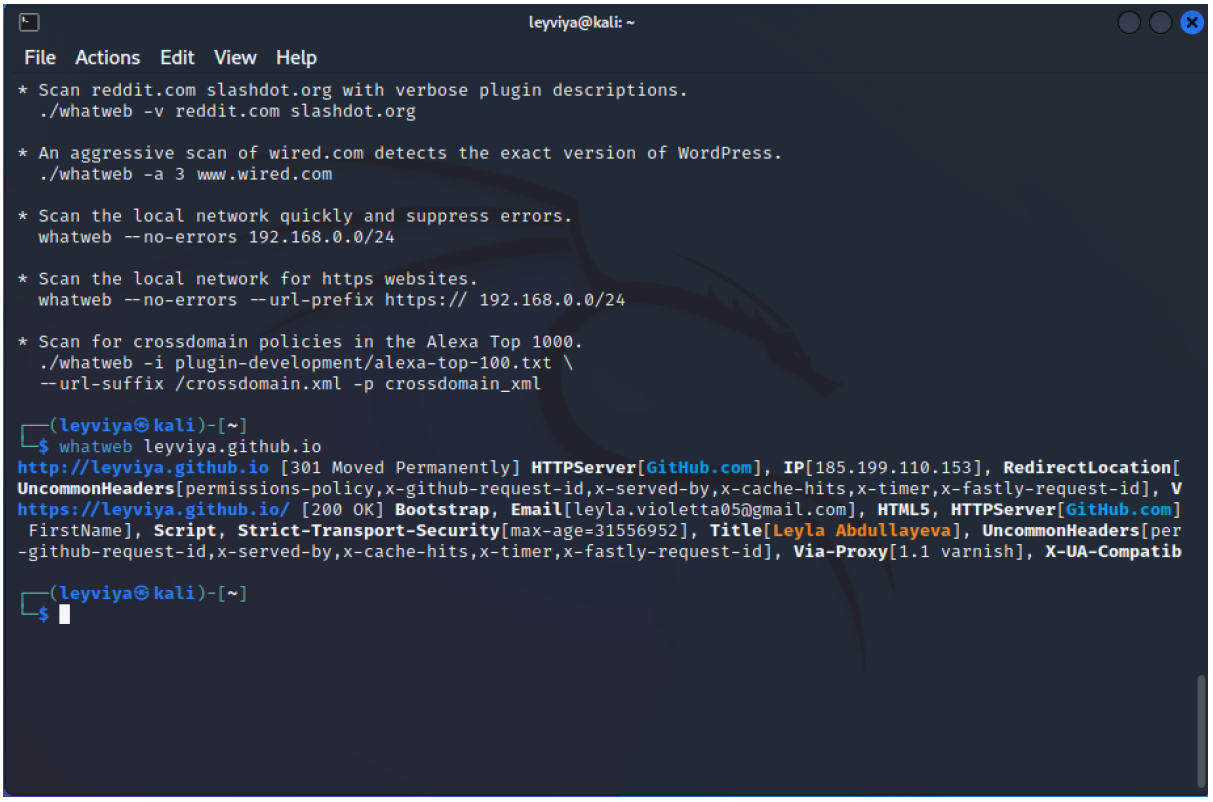
SQLMap Processes and Analysis

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:



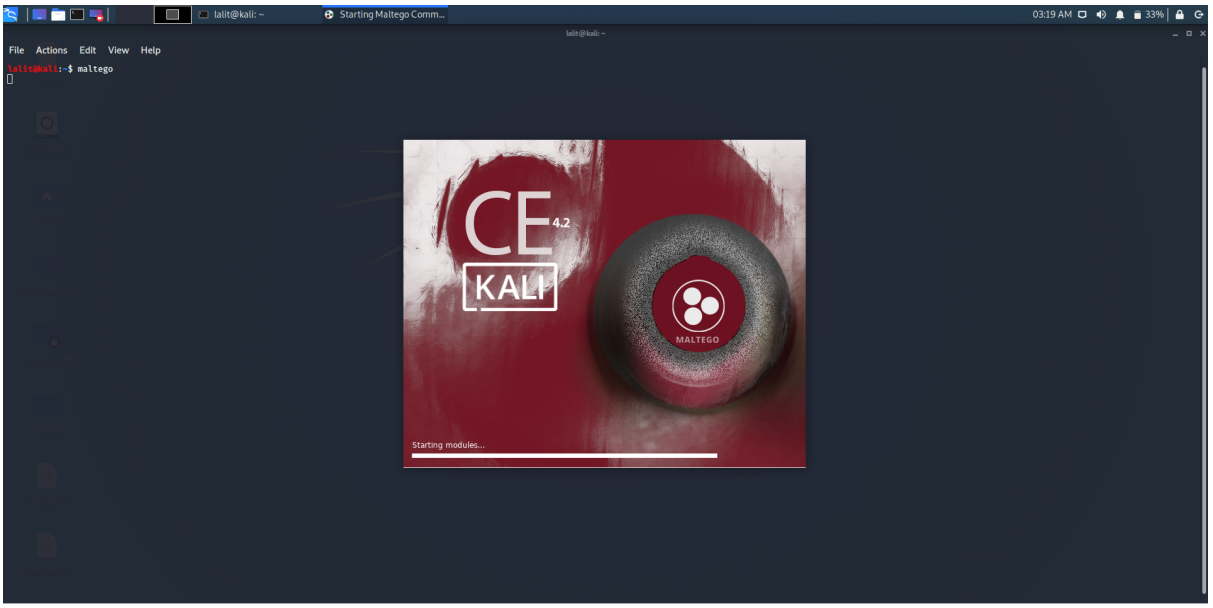
Whatweb Processes and Analysis

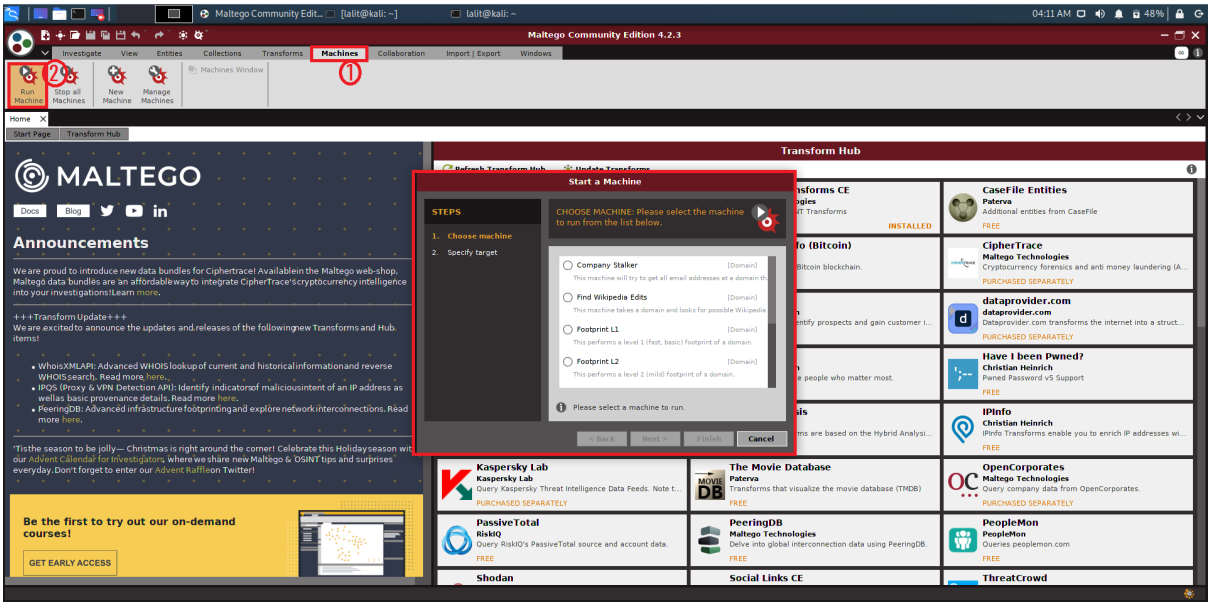
WhatWeb is a tool that is included in Kali Linux and is used for identifying the technologies that are used by websites. It can be used to gather information about a website's server-side software, client-side software, and other technical details. This information can be useful for a variety of purposes,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

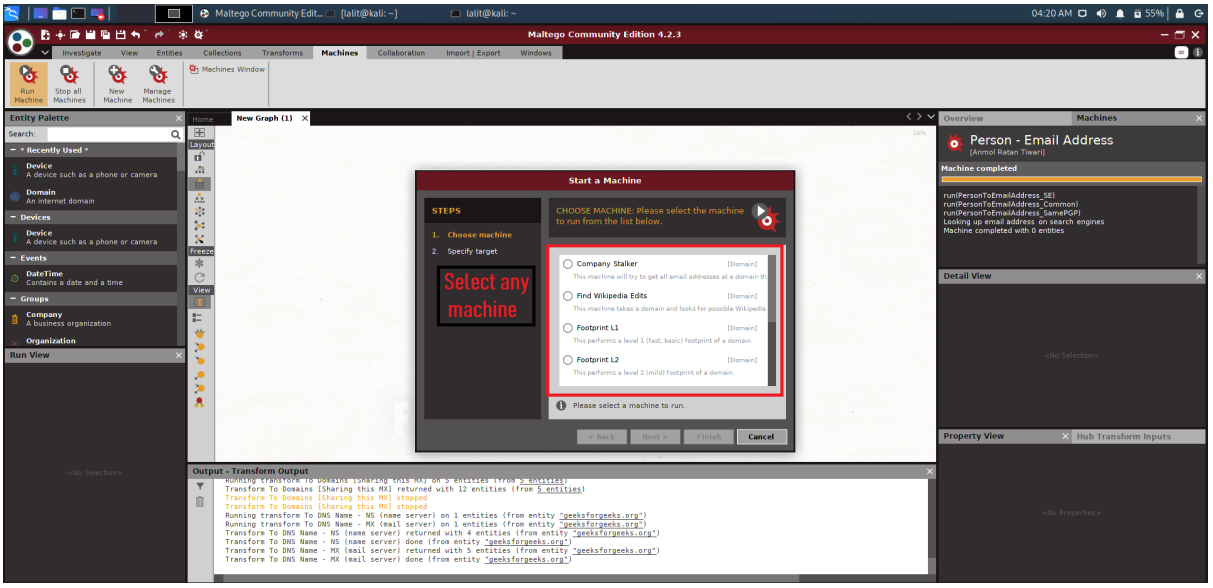


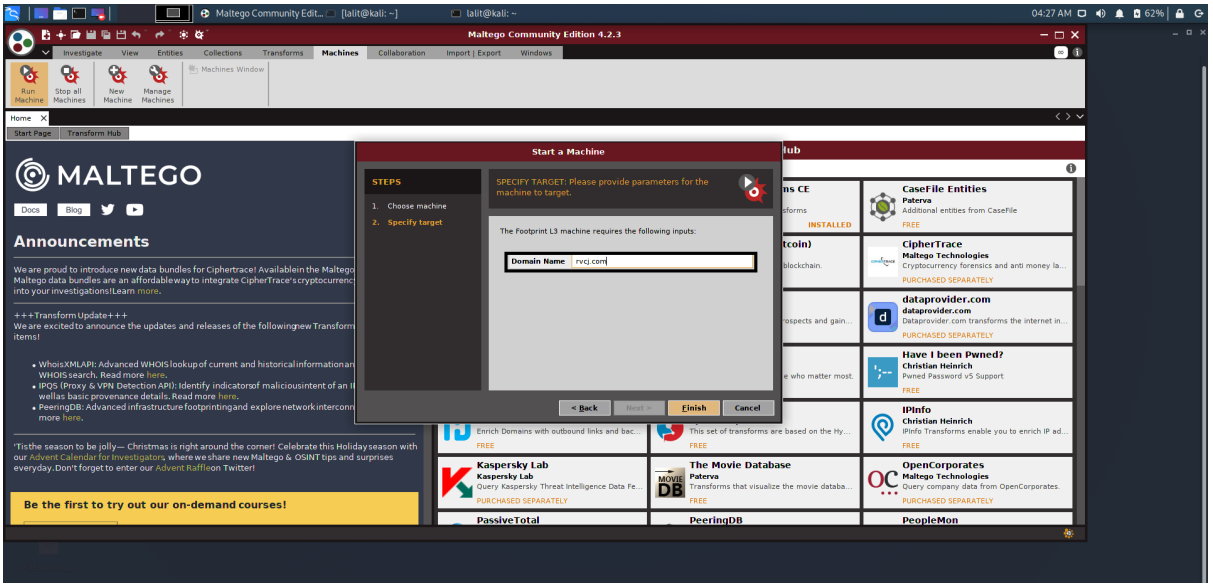
Maltego

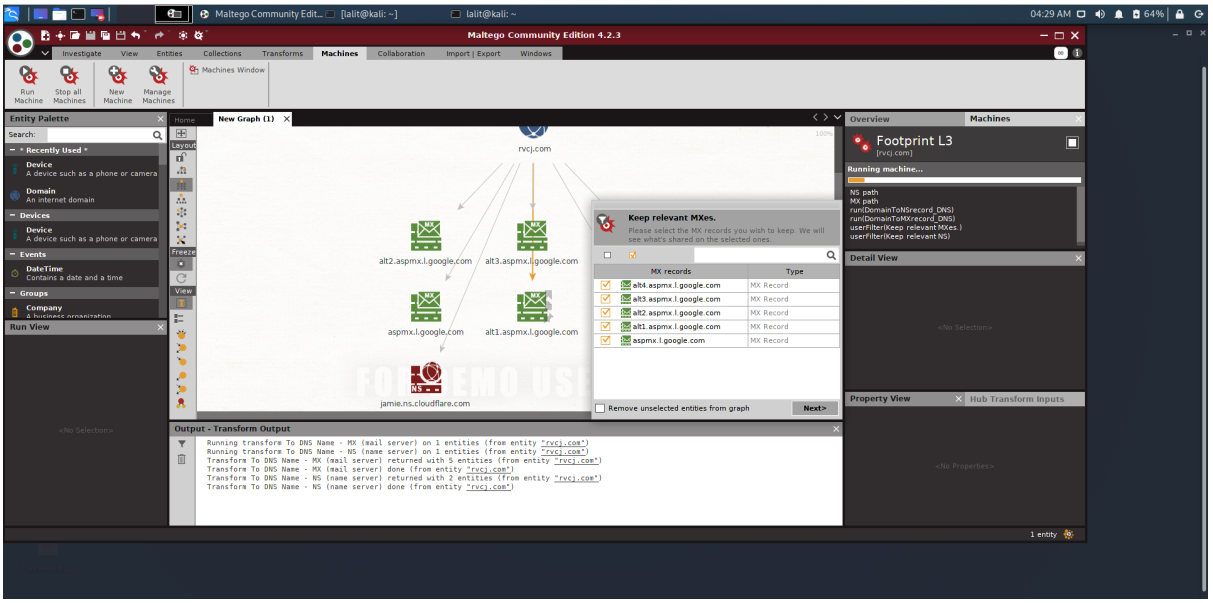
Maltego is a tool for performing open-source intelligence (OSINT) analysis and visualizing the relationships between different entities. It can be used to analyze a web application and identify any potential vulnerabilities or security risks. Here is a simple example of how you can use Maltego in Kali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




Maltego Community Edition 4.2.3
Machines
Run Machine
Stop all Machines
New Machine
Manage Machines
Transform Hub
MALTEGO
Announcements
Start a Machine
STEPS
1. Choose machine
2. Specify target
CHOOSE MACHINE: Please select the machine to run from the list below.
Company Stalker
Find Wikipedia Edits
Footprint L1
Footprint L2
Please select a machine to run.
Cancel
Be the first to try out our on-demand courses!
GET EARLY ACCESS

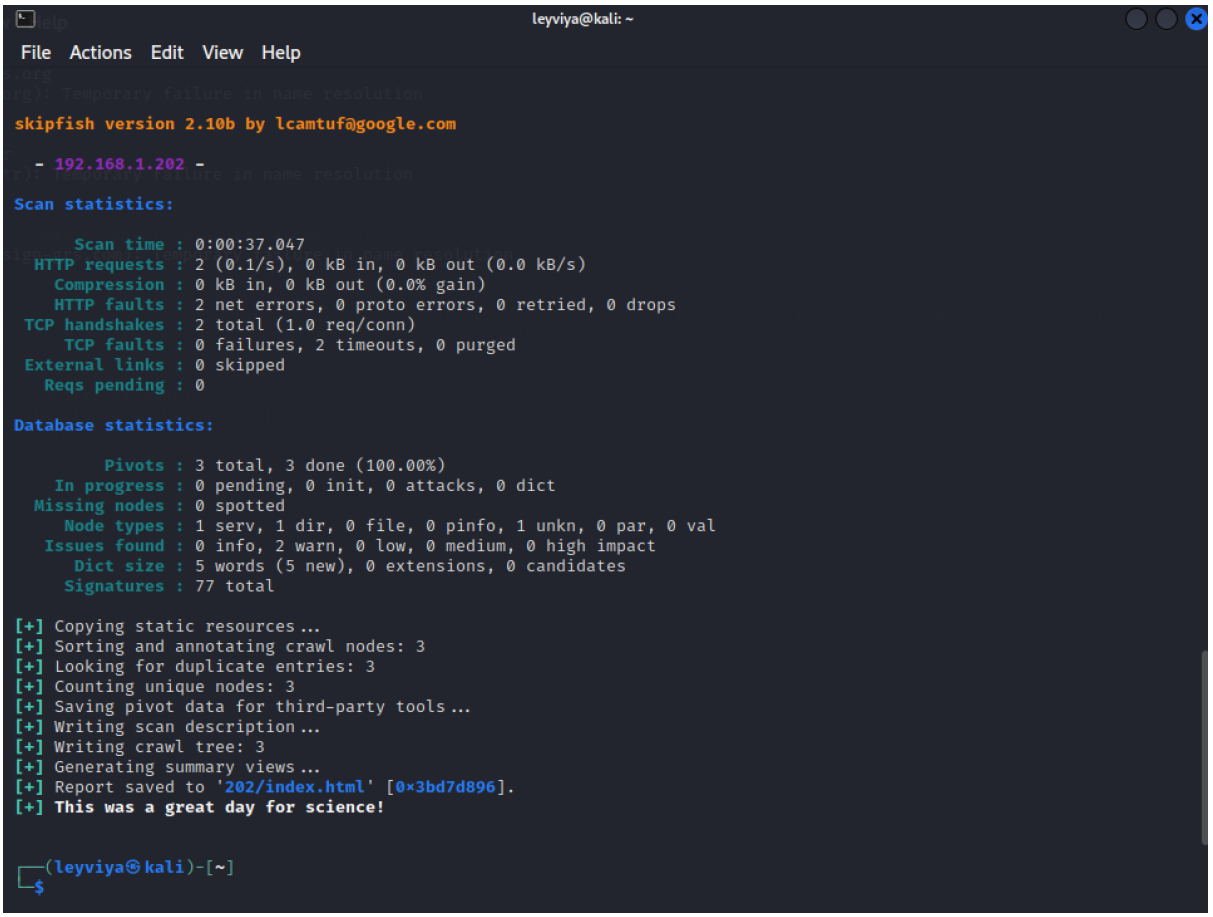

Maltego Community Edition 4.2.3
Entity Palette
New Graph (1)
Start a Machine
STEPS
1. Choose machine
2. Specify target
CHOOSE MACHINE: Please select the machine to run from the list below.
Select any machine
Company Stalker
Find Wikipedia Edits
Footprint L1
Footprint L2
Please select a machine to run.
Cancel
Person - Email Address
Machine completed
Output - Transform Output
Property View


Maltego Community Edition 4.2.3
MALTEGO
Announcements
Start a Machine
STEPS
1. Choose machine
2. Specify target
SPECIFY TARGET: Please provide parameters for the machine to target.
The Footprint L3 machine requires the following inputs:
Domain Name
rvcj.com
< Back
Next >
Finish
Cancel
Be the first to try out our on-demand courses!



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.



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) leyviya@Leyla-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 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
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 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e: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 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
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:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     30909 8 2 e2d3c916f6deeac73294e8268fb5885044a833fc5459588f4a9184cfc41a5766

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2019-08-14
source:       IANA

# whois.verisign-grs.com

   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
```

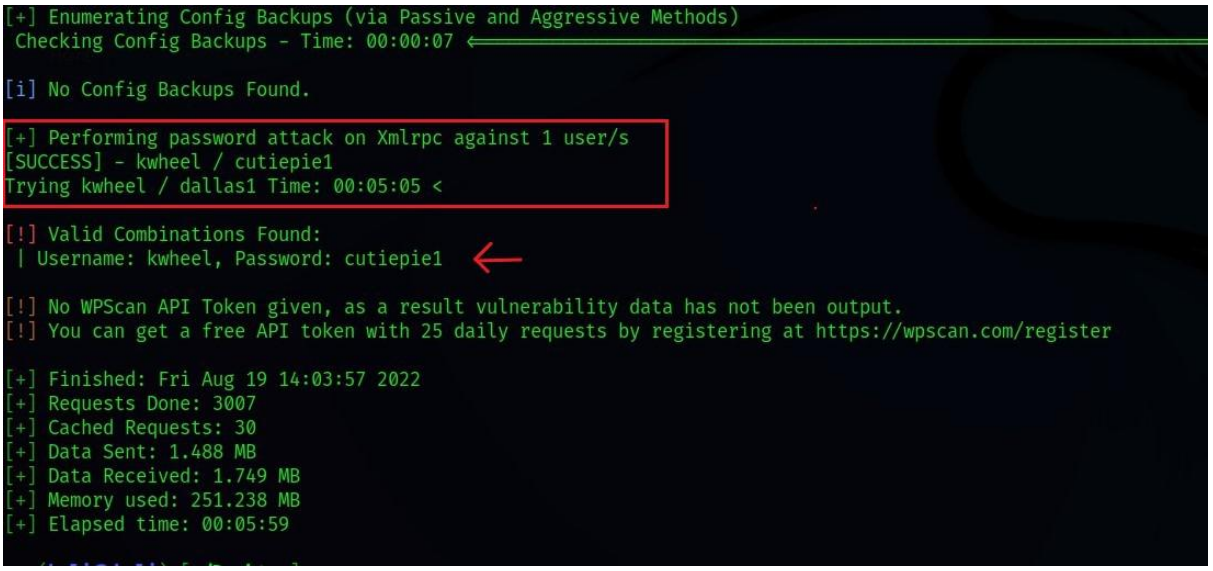
```
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   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: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
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: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.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: ns3.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: 2022-12-29T10:35:50+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.



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.