

- Once you have an account, log in to the website and click on the "Linux Virtual Machines" tab.
- Scroll down the list of available virtual machines until you find Kali Linux. Click on the "Launch" button next to it.
- A new window will open in your web browser, showing a terminal window with the Kali Linux command prompt. From here, you can start using Kali Linux as you would on any other computer.

Welcome to linuxzoo

Learn Linux from the safety of your chair using a remote private linux machine with root access.

- Welcome to linuxzoo
- Our environment
- Essential Linux
- System Administration

Status: TESTING

Updates have been made across the system. There may be unexpected errors issues. I will be monitoring for a few days, but the system should be considered at risk for now.

Look at the Our Environment link, and then Running Your Machine for getting started.

Quick start hints: register/login, Join Queue, Switch On (in Control tab), Wait for successful boot, click the Connect tab, and then click "telnet: linuxzoo.net" (or type telnet linuxzoo.net at your command prompt). Username root, password secure.

Image	Username	Password
Linux Centos 7	root	secure
	alice	secure
Caine Forensics 10.0	caine	caine
Kali 2020-4	root	kali

FAQ for VNC: There are a few options to getting a remote graphical desktop. In "connect" you can click on Java VNC, which requires java 7 installed on your machine. JavaScript VNC is more flexable, but it may be slower (it is experimental). Some systems do not like you logging in graphically as root.

Centos 7 intro: [Paths](#) | [BasicShell](#) | [Search](#)
 Linux tutorials: [intro1](#) [intro2](#) [wildcard](#) [permission](#) [pipe](#) [vi](#) [essential](#) [admin](#) [net](#) [SELinux1](#) [SELinux2](#) [fwall](#) [DNS](#) [diag](#) [Apache1](#) [Apache2](#) [log](#) [Mail](#)
 Caine 10.0: [Essentials](#) | [Basic](#) | [Search](#) | [Acquisition](#) | [SysIntro](#) | [grep](#) | [MBR](#) | [GPT](#) | [FAT](#) | [NTFS](#) | [FRMeta](#) | [FRTools](#) | [Browser](#) | [Mock Exam](#) |
 CPD: [Cygwin](#) | [Paths](#) | [Files and head/tail](#) | [Find and regex](#) | [Sort](#) | [Log Analysis](#)
 Kali: [1a](#) | [1b](#) | [1c](#) | [2](#) | [3](#) | [4a](#) | [4b](#) | [5](#) | [6](#) | [7a](#) | [8a](#) | [8b](#) | [9](#) | [10](#) |
 Kali 2020-4: [1a](#) | [1b](#) | [1c](#) | [2](#) | [3](#) | [4a](#) | [4b](#) | [5](#) | [6](#) | [7](#) | [8a](#) | [8b](#) | [9](#) | [10](#) |
 Useful: [Quiz](#) | [Forums](#) | [Privacy Policy](#) | [Terms and Conditions](#)
 Site Links: [XML Zoo](#) [ActiveSQL](#) [ProgZoo](#) [SQLZoo](#)

If you want to access the graphical user interface (GUI) of Kali Linux, click on the "Menu" button in the top left corner of the terminal window and then select "Applications" from the menu. From the Applications menu, you can launch different applications and tools that are installed on Kali Linux.

```

File Actions Edit View Help
[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

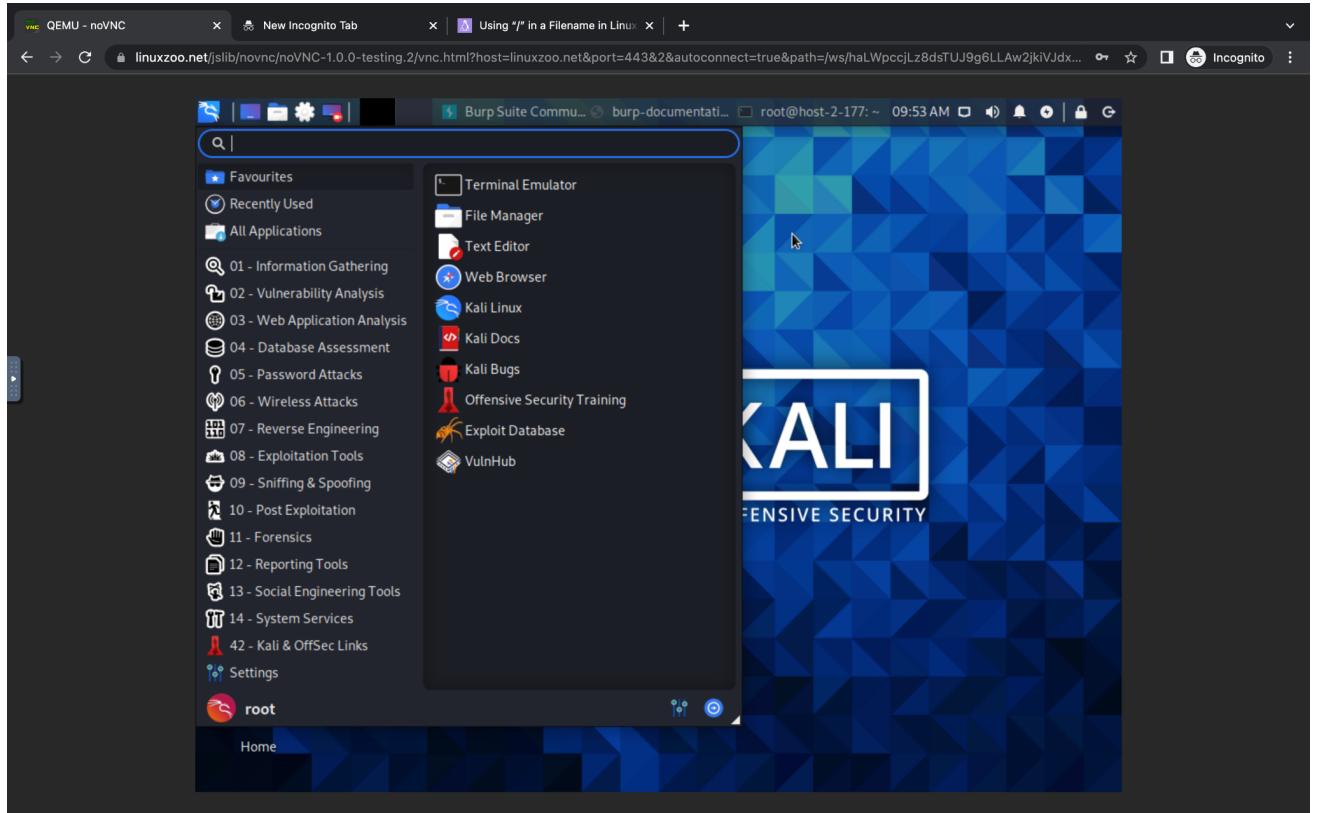
+ Target IP:          146.176.166.1
+ Target Hostname:    chirags.in
+ Target Port:        80
+ Start Time:         2022-12-19 09:14:06 (GMT0)

+ Server: 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 'tcm' 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 EOL for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0 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: ~]
# 
```

Kali Linux is a popular operating system that provides a range of tools for web application analysis. Some of the tools that are commonly used for web application analysis in Kali Linux include:

Homepage screenshot of online Kali Linux from Linuxzoo:



Burp Suite: 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.

sqlmap: sqlmap is a tool for detecting and exploiting SQL injection vulnerabilities in web applications.

wpscan: wpscan is a tool for analyzing WordPress installations and identifying vulnerabilities in WordPress plugins and themes.

nikto: nikto is a tool for identifying vulnerabilities in web servers and web applications.

It is important to note that these are just a few examples of the many tools that are available for web application analysis in Kali Linux. It is always a good idea to research and evaluate different tools to determine which ones are best suited for your needs.

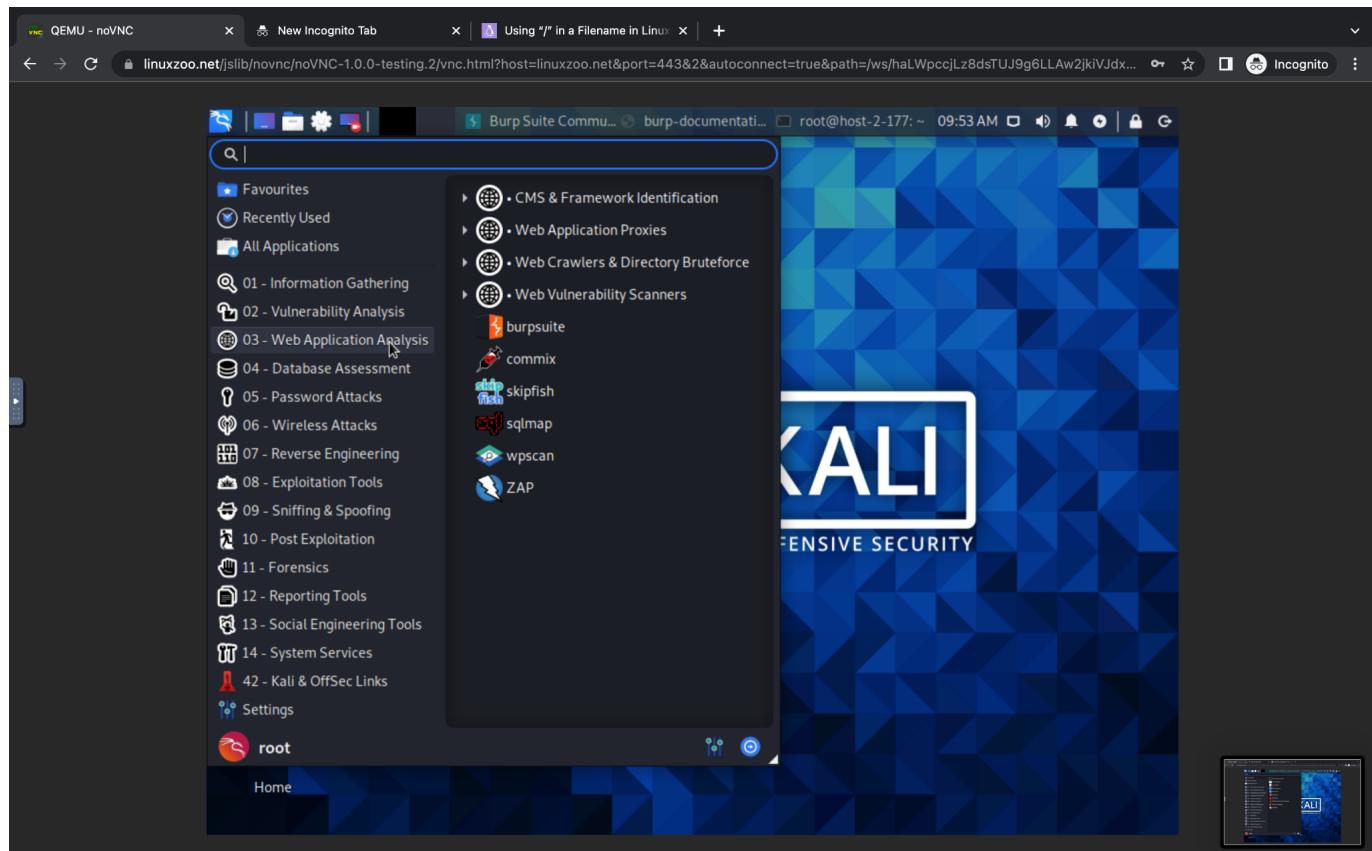
1. Burp Suite processes and analysis

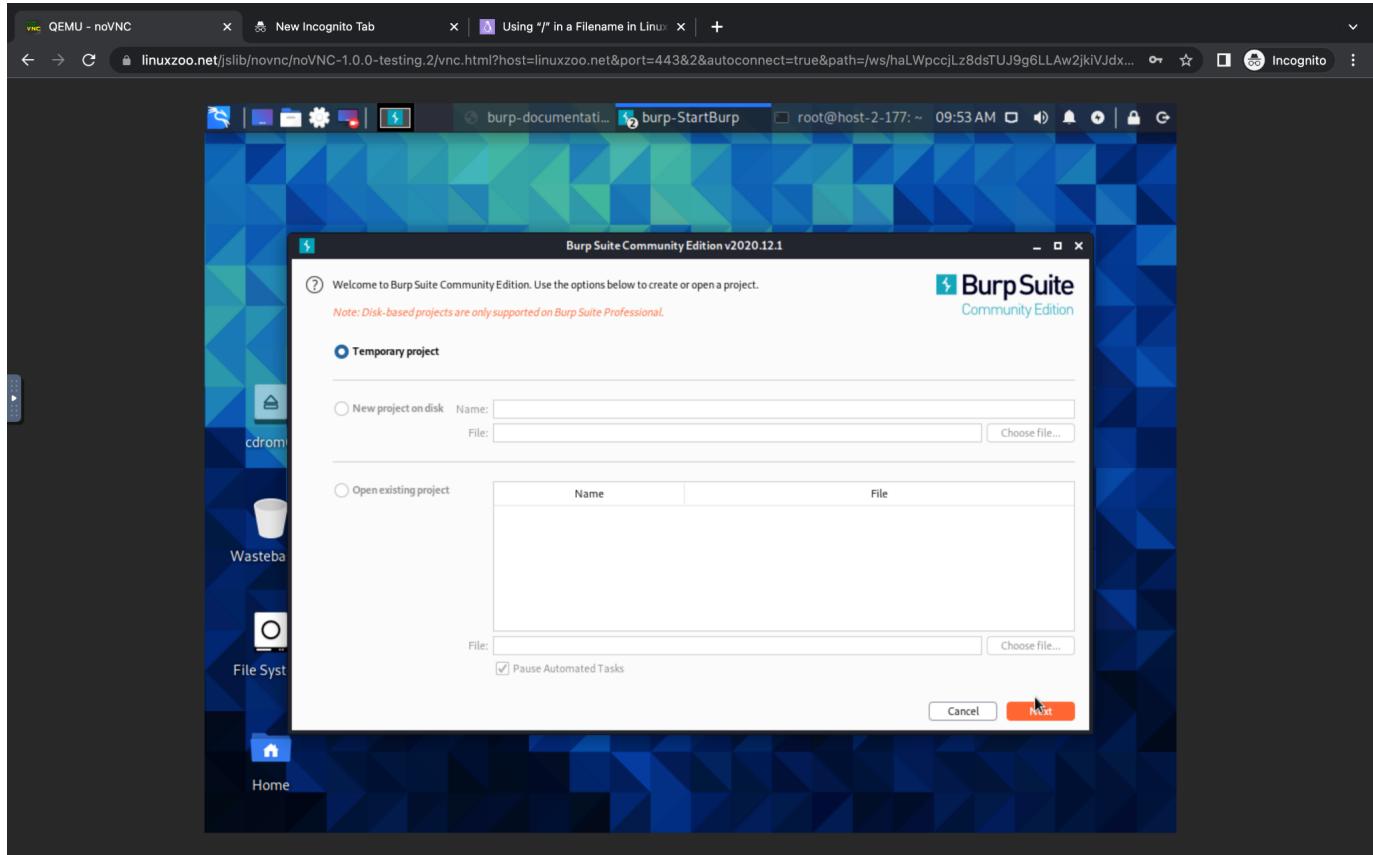
Burp Suite is a comprehensive tool for web application analysis that includes a number of features such as a web proxy, a web application scanner, and a manual testing interface. Here is an example of how you can use Burp Suite for web application analysis in Kali Linux:

- Start by launching Burp Suite and configuring your browser to use the Burp Suite proxy. You can do this by going to the "Proxy" tab in Burp Suite and clicking on the "Options" button.

Navigate to the web application you want to analyze using your browser. As you navigate through the application, Burp Suite will capture and display the traffic in the "Intercept" tab. To begin analyzing the web application, click on the "Scanner" tab in Burp Suite. This will open the web application scanner, which can be used to automatically test for vulnerabilities in the web application. To start the scan, click on the "Start scan" button. The scanner will begin testing the web application for a range of vulnerabilities, such as SQL injection and cross-site scripting (XSS). As the scan progresses, you can view the results in the "Scanner results" tab. The results will show any vulnerabilities that were detected, along with details about the vulnerability and recommendations for how to fix it. Once the scan is complete, you can use the results to identify and prioritize any vulnerabilities that need to be fixed. You can also use the manual testing features in Burp Suite to further analyze the web application and identify any additional vulnerabilities.

Screenshots from online Kali Linux:





The screenshot shows the Burp Suite Community Edition interface after starting a passive crawl. The title bar reads "Burp Suite Community Edition v2020.12.1 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, Help, and several sub-options like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The main window has tabs for "Tasks" (selected), "Issue activity [Pro version only]", and "Event log".

- Tasks:** Shows a single task: "1. Live passive crawl from Proxy (all traffic)". It indicates "0 items added to site map", "0 responses processed", and "0 responses queued".
- Issue activity [Pro version only]:** A table showing various security issues found during the crawl. The columns are "Issue type", "Host", and "Path".

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-website...	/product/stock
External service interaction (HTTP)	https://insecure-website...	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-website...	/
OS command injection	https://insecure-website...	/feedback/submit
- Event log:** A table showing log entries with columns "Time", "Type", and "Source".

Time	Type	Source
09:10:09 19 Dec 2022	Info	Suite
09:10:07 19 Dec 2022	Info	Proxy
09:10:04 19 Dec 2022	Info	Suite

As you can see, the Burp Suite interface includes a number of different tabs and features that can be used for web application analysis. The "Intercept" tab allows you to capture and view traffic as you navigate through the web application, the "Scanner" tab allows you to automatically test for vulnerabilities, and the "Scanner results" tab displays the results of the scan. You can also use the manual testing features in Burp Suite to further analyze the web application and identify any additional vulnerabilities.

The Burp Suite interface includes a number of different tabs and features that can be used for web application analysis. The "Intercept" tab allows you to capture and view traffic as you navigate through the web application. This can be useful for analyzing the requests and responses that are sent between the web application and the client (i.e., your browser).

The "Scanner" tab allows you to automatically test the web application for a range of vulnerabilities, such as SQL injection and cross-site scripting (XSS). To start a scan, you simply click on the "Start scan" button. As the scan progresses, you can view the results in the "Scanner results" tab, which will show any vulnerabilities that were detected along with details about the vulnerability and recommendations for how to fix it.

In addition to the automatic scanning features, Burp Suite also includes a number of manual testing tools that can be used to further analyze the web application and identify any additional vulnerabilities. These tools include a request editor, a response viewer, and a number of other features that can be used to manipulate and analyze the requests and responses sent between the web application and the client.

2. 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:

Open a terminal window in Kali Linux and navigate to the directory where Nikto is installed.

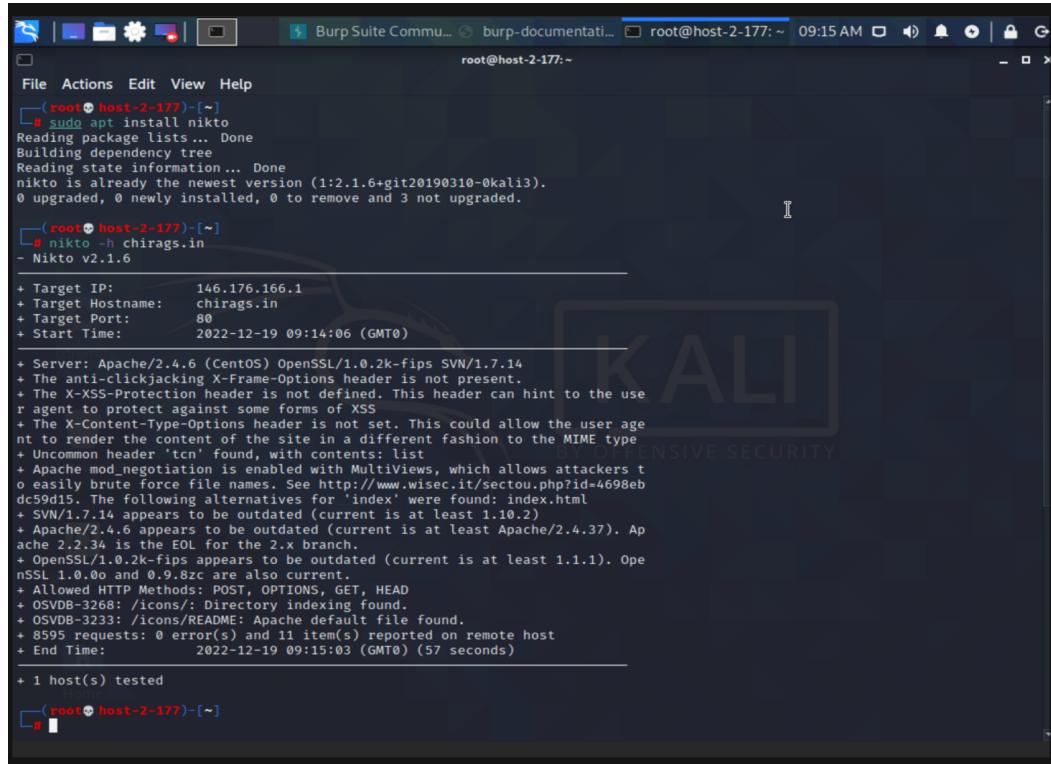
To start a scan, use the following command: `nikto -h <target URL>`

Nikto will begin scanning the web application and will output the results to the terminal. The results will show any vulnerabilities or misconfigurations that were detected, along with details about the vulnerability and recommendations for how to fix it.

To save the results to a file, use the following command: `nikto -h <target URL> > results.txt`

Overall, Nikto is a simple and effective tool for identifying vulnerabilities in web servers and web applications. It is easy to use and can provide valuable information about potential security risks that may be present in a web application.

Screenshots from application:



The screenshot shows a terminal window with the following command and output:

```
(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)

+ Server: 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 EOL 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
Home
[root@host-2-177] ~
#
```

3. 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:

Open a terminal window in Kali Linux and navigate to the directory where SQLMap is installed.

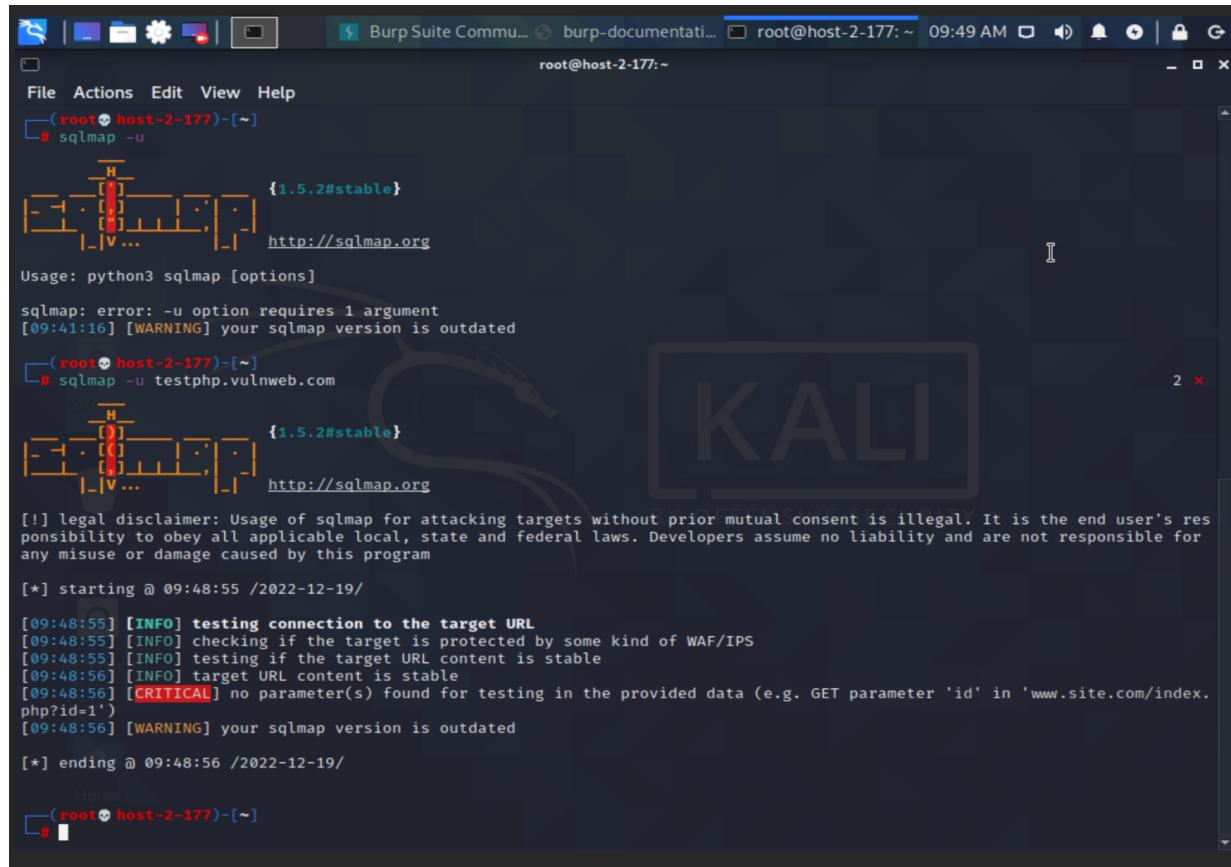
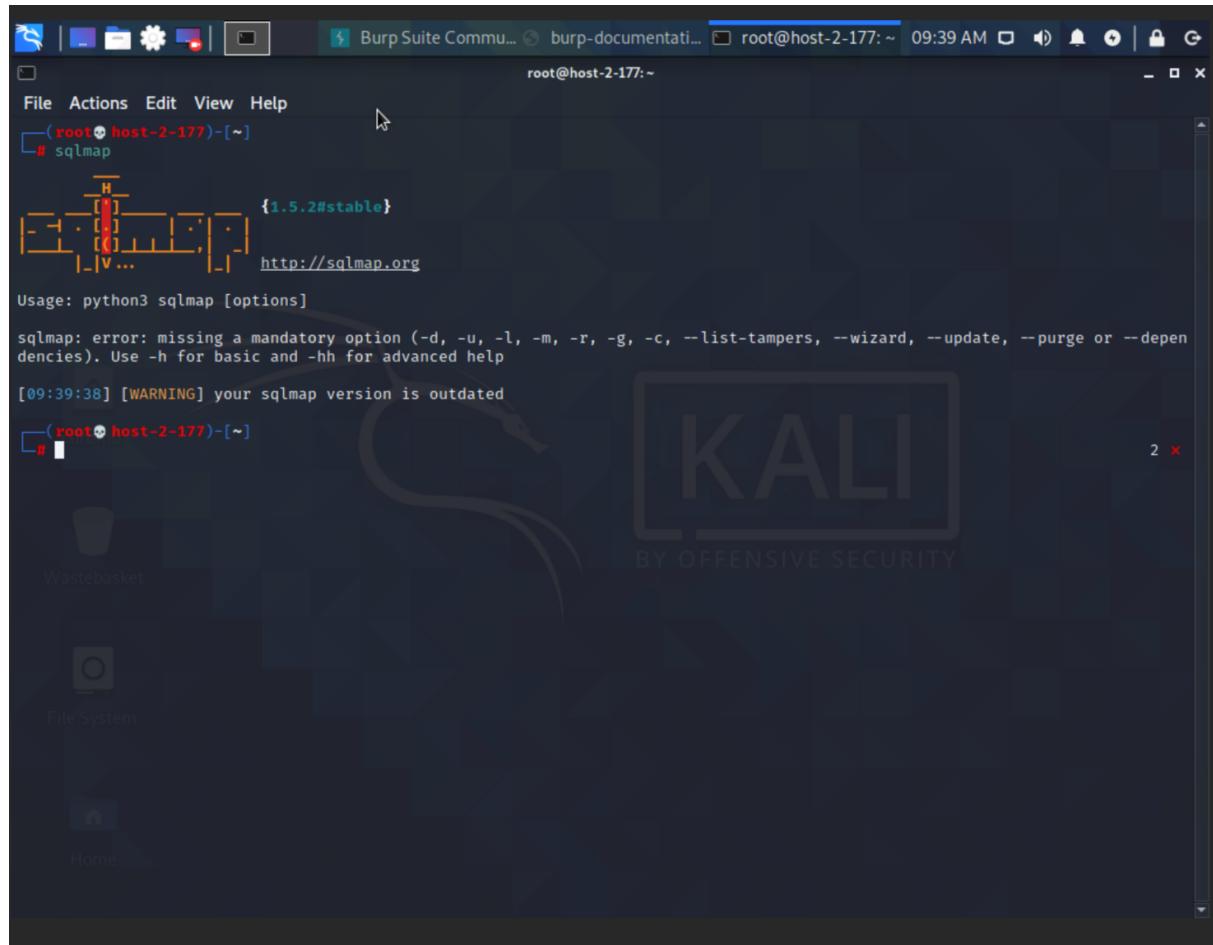
To start a scan, use the following command: `sqlmap -u <target URL> --dbs`

SQLMap will begin scanning the web application and will output the results to the terminal. The results will show any databases that are present on the server and any vulnerabilities that were detected.

To exploit a vulnerability, use the following command: `sqlmap -u <target URL> -D <database name> --tables`

SQLMap will attempt to exploit the vulnerability and will output the results to the terminal. The results will show any tables that are present in the database and any data that was extracted.

Screenshots from Kali Linux:



Overall, SQLMap is a simple and effective tool for detecting and exploiting SQL injection vulnerabilities in web applications. It is easy to use and can provide valuable information about potential security risks that may be present in a web application.

4. 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.

To install WhatWeb on Kali Linux, follow these steps:

1. Open a terminal window and make sure that your system is up to date by running the following command:

```
sudo apt update && sudo apt upgrade -y
```

2. Install WhatWeb by running the following command:

```
sudo apt install whatweb
```

3. Once the installation is complete, you can use WhatWeb by running the whatweb command followed by the URL of the website you want to scan. For example:

```
whatweb example.com
```

Screenshot from Kali Linux:

The screenshot shows a terminal window with the following text output:

```
File Actions Edit View Help
root@host-2-177:~#
# whatweb chirags.in
http://chirags.in [200 OK] Apache[2.4.6], Country[UNITED KINGDOM][GB], Email[g.russell@napier.ac.uk], HTTPServer[CentOS][Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14], IP[146.176.166.1], OpenSSL[1.0.2k-fips], SVN[1.7.14], Title[Napier University]

root@host-2-177:~#
# whatweb chirags.in
http://chirags.in [200 OK] Apache[2.4.6], Country[UNITED KINGDOM][GB], Email[g.russell@napier.ac.uk], HTTPServer[CentOS][Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14], IP[146.176.166.1], OpenSSL[1.0.2k-fips], SVN[1.7.14], Title[Napier University]

root@host-2-177:~#
# whatweb google.com
http://google.com [200 OK] Apache[2.4.6], Country[UNITED KINGDOM][GB], Email[g.russell@napier.ac.uk], HTTPServer[CentOS][Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14], IP[146.176.166.1], OpenSSL[1.0.2k-fips], SVN[1.7.14], Title[Napier University]

root@host-2-177:~#
# whatweb beykoz.edu.tr
http://beykoz.edu.tr [200 OK] Apache[2.4.6], Country[UNITED KINGDOM][GB], Email[g.russell@napier.ac.uk], HTTPServer[CentOS][Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14], IP[146.176.166.1], OpenSSL[1.0.2k-fips], SVN[1.7.14], Title[Napier University]

root@host-2-177:~#
# whois chirags.in
clear
```

5. 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:

1. Open Maltego in Kali Linux and create a new project for the web application you want to analyze.
2. In the "Transforms" panel, select the transforms that you want to use to analyze the web application. These transforms can be used to gather information about the web application, such as its domains, IP addresses, and DNS records.
3. Run the transforms to gather information about the web application. As the transforms run, they will create entities in the graph that represent the different elements of the web application, such as domains, IP addresses, and DNS records.

As the entities are created, they will be linked together in the graph to show the relationships between them. You can use these relationships to identify potential vulnerabilities or security risks in the web application.

Use the information gathered by the transforms to identify and prioritize any vulnerabilities or risks that need to be addressed. You can also use Maltego to create reports or export the data for further analysis.

Overall, Maltego is a powerful tool for performing OSINT analysis and visualizing the relationships between different entities. It can be used to identify potential vulnerabilities or security risks in a web application and help prioritize efforts to mitigate those risks.

Create a new project in Maltego and select the transforms that you want to use to analyze the web application.

The screenshot shows a terminal window with a dark background and light-colored text. The window title is 'Burm Suite Commu...' and the status bar shows 'root@host-2-177: ~' and '10:13 AM'. The terminal content is as follows:

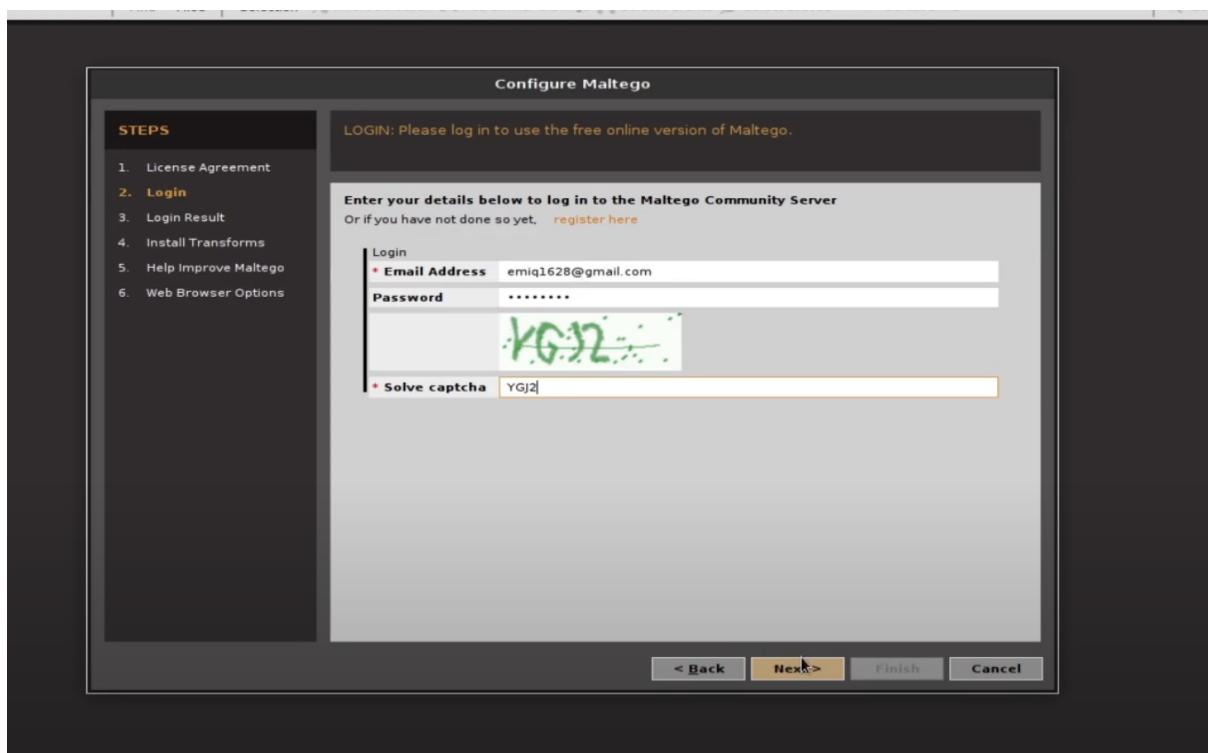
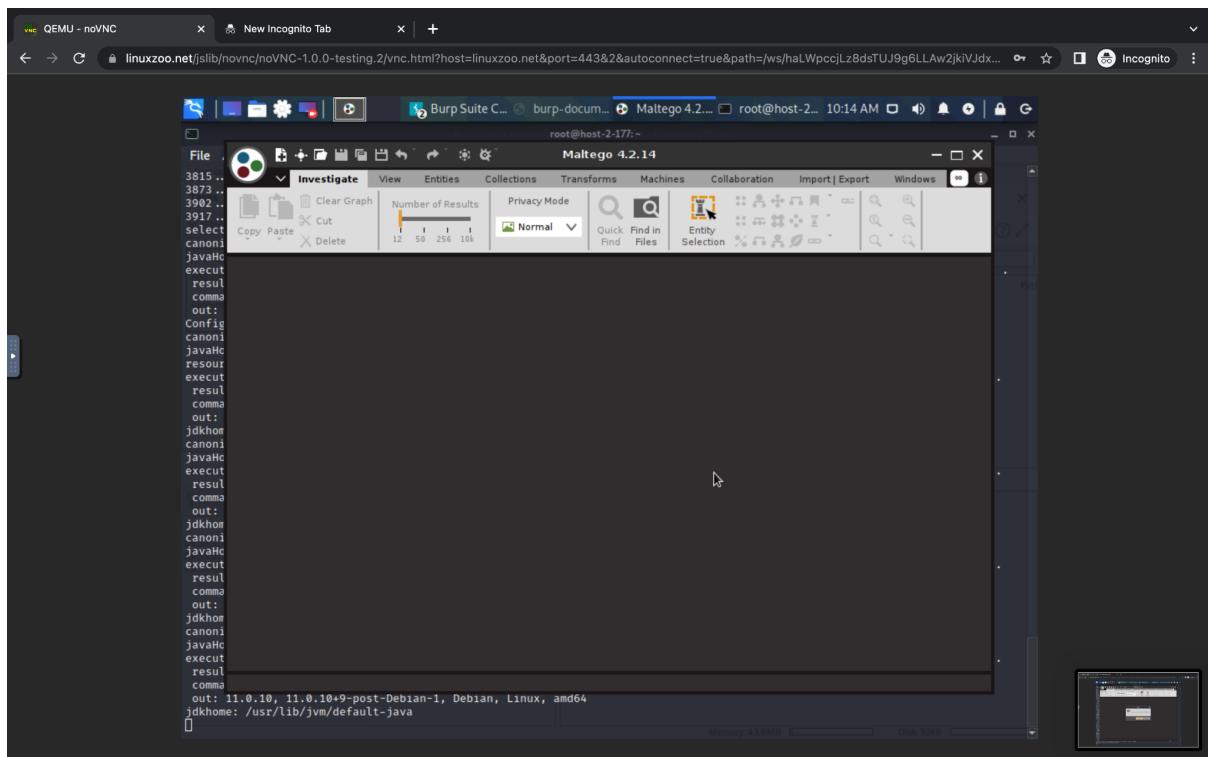
```
(root@host-2-177) [~]
# apt get install maltego
E: Command line option 'g' [from -get] is not understood in combination with the other options.

(root@host-2-177) [~]
# apt install maltego
E: Command line option 'g' [from -get] is not understood in combination with the other options.

(root@host-2-177) [~]
# apt install maltego
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package maltego

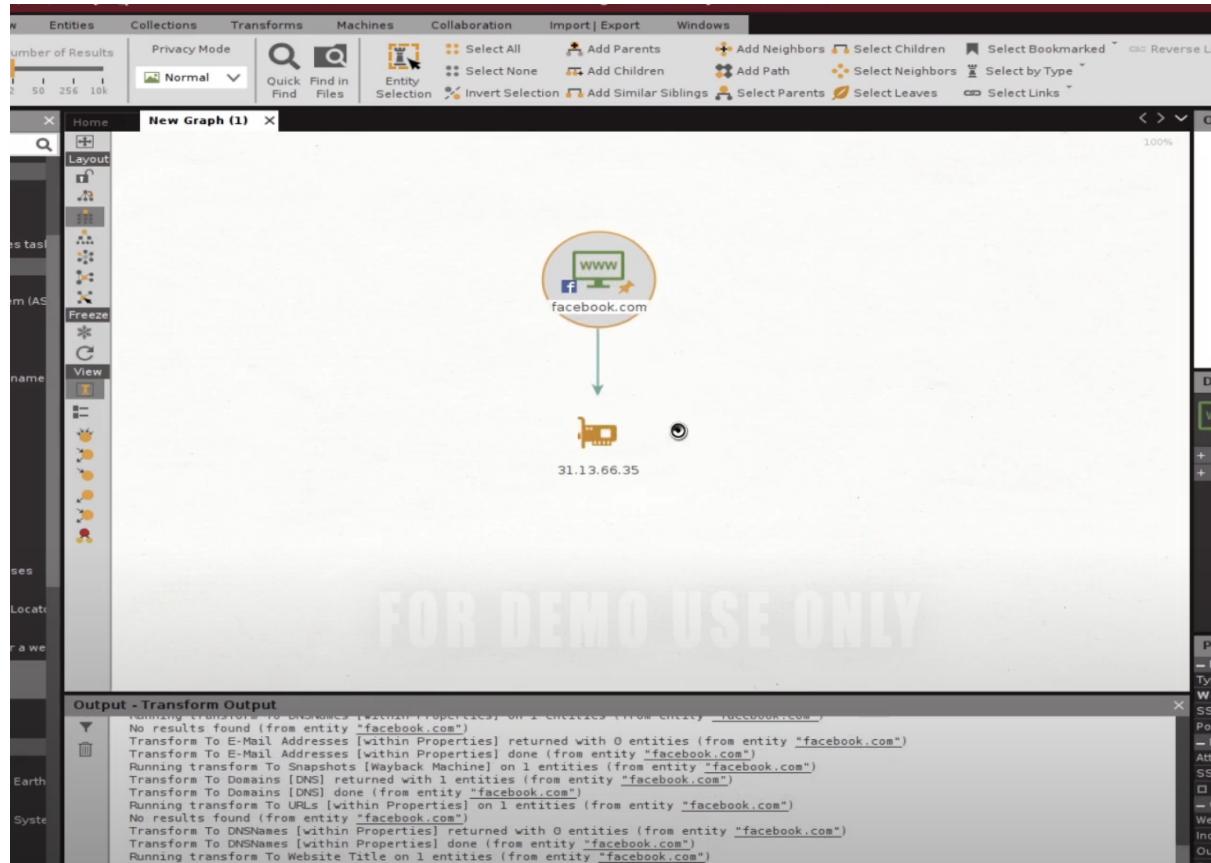
(root@host-2-177) [~]
# apt install maltego
Reading package lists... Done
Building dependency tree
Reading state information... Done
maltego is already the newest version (4.2.14.13579-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.

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

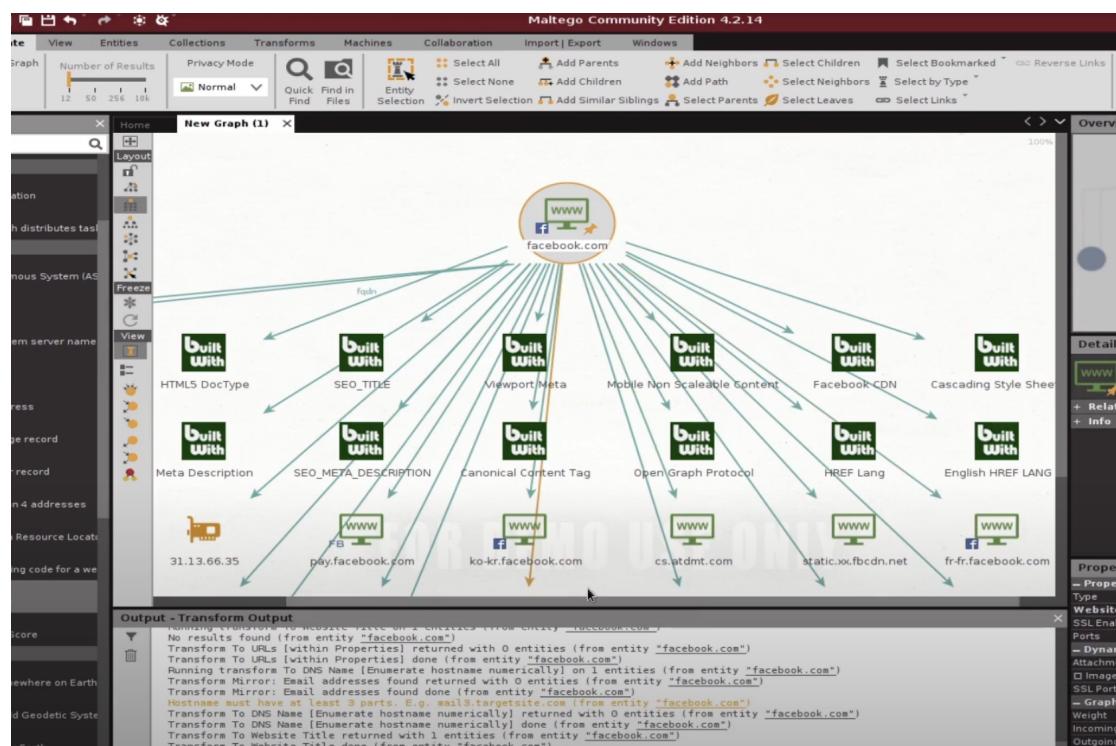


Run the transforms to gather information about the web application:

View the results in the graph to identify the relationships between different elements of the web application, such as domains, IP addresses, and DNS records.



Use the information gathered by the transforms to identify and prioritize any vulnerabilities or risks that need to be addressed.



Maltego is a tool for performing open-source intelligence (OSINT) analysis and visualizing the relationships between different entities. It can be used to identify potential vulnerabilities or security risks in a web application and help prioritize efforts to mitigate those risks.

