Beykoz University

Department of “Computer Engineering”

“Information Systems Security - 60619MEEOZ-CME0147”

Web Application Pentest with Analysis

Project

Interim Report - Part II

Lecturer: DUYGU DEMİRAY

Leyla Abdullayeva - 1904010038

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. Here are some steps you can follow to perform web application penetration testing using online Kali Linux:

Set up a testing environment: You will need a computer or virtual machine with Kali Linux installed, as well as the web application you want to test. It is important to ensure that your testing environment is isolated from your production environment, as you will be simulating an attack on the web application.

Identify the scope of the test: Determine the scope of the test by identifying the web application and its associated systems, networks, and infrastructure. This will help you focus your testing efforts and ensure that you are not missing any potential vulnerabilities.

Gather information about the web application: Before you begin testing, gather as much information as possible about the web application. This may include the version of the application, the technologies it uses, and any public information about known vulnerabilities.

Test for vulnerabilities: Use a range of tools and techniques to test for vulnerabilities in the web application. This may include testing for SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common web application vulnerabilities.

Report on findings: Once you have identified any vulnerabilities, document your findings in a report. Include details about the vulnerabilities, how they were discovered, and any recommendations for how to fix them.

It is important to note that web application penetration testing should only be performed with the permission of the web application owner.

In my case, for this submission, I'm using an Online Cloud based version of Kali Linux. Linuxzoo.net is a website that provides online access to a variety of Linux-based operating systems and applications through a web browser. It is a platform that allows users to explore and learn about Linux without having to install it on their own computer. Users can create an account on the website and then access a variety of pre-configured virtual machines that run different versions of Linux and a range of applications. This can be useful for students and professionals who want to learn about Linux and try out different distributions and applications without having to install and set up the operating system themselves. It can also be a convenient way for developers to test their applications in different environments.

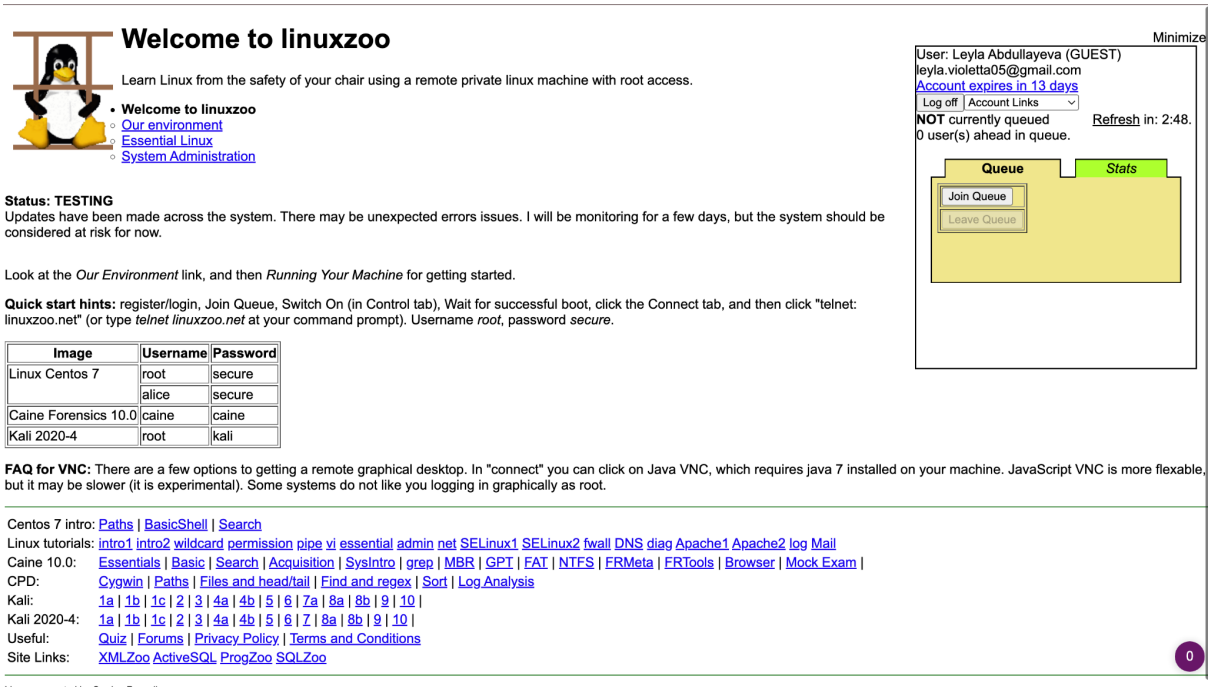
To run Kali Linux in Linuxzoo.net, you will need to follow these steps:

1. Go to the Linuxzoo.net website and create an account if you do not already have one.

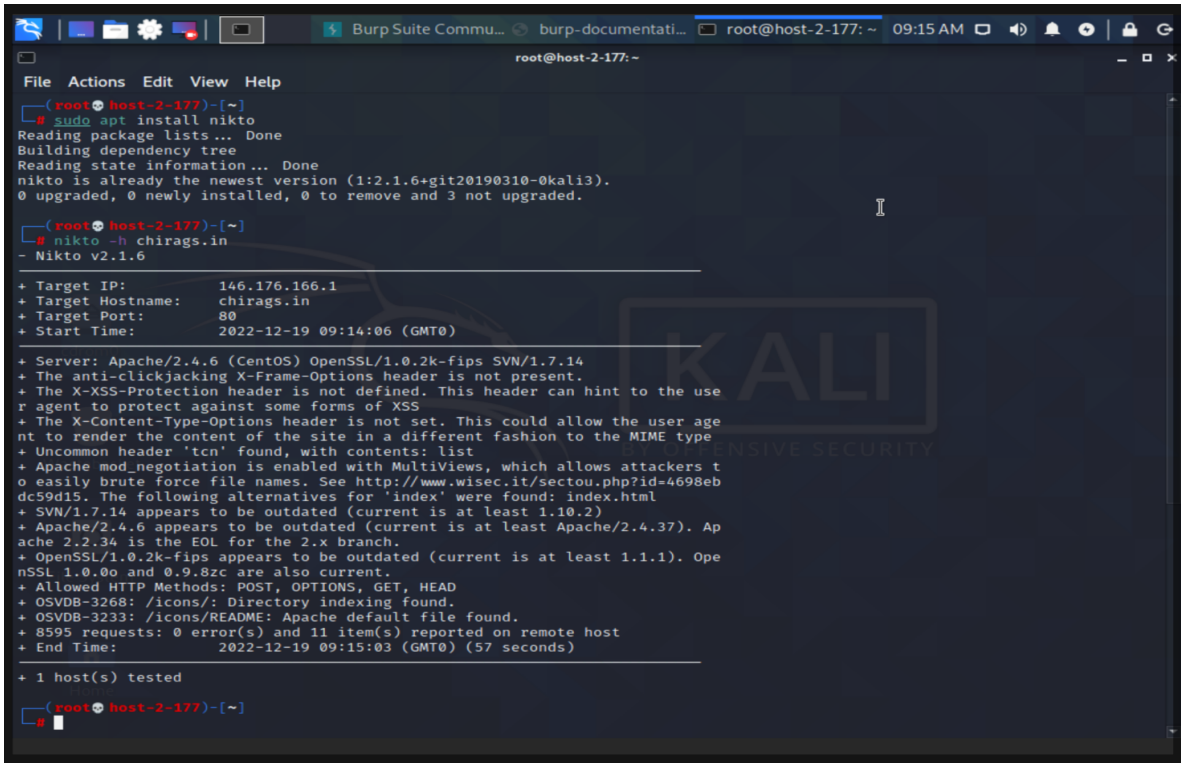
2. Once you have an account, log in to the website and click on the "Linux Virtual Machines" tab.

3. Scroll down the list of available virtual machines until you find Kali Linux. Click on the "Launch" button next to it.

4. 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.

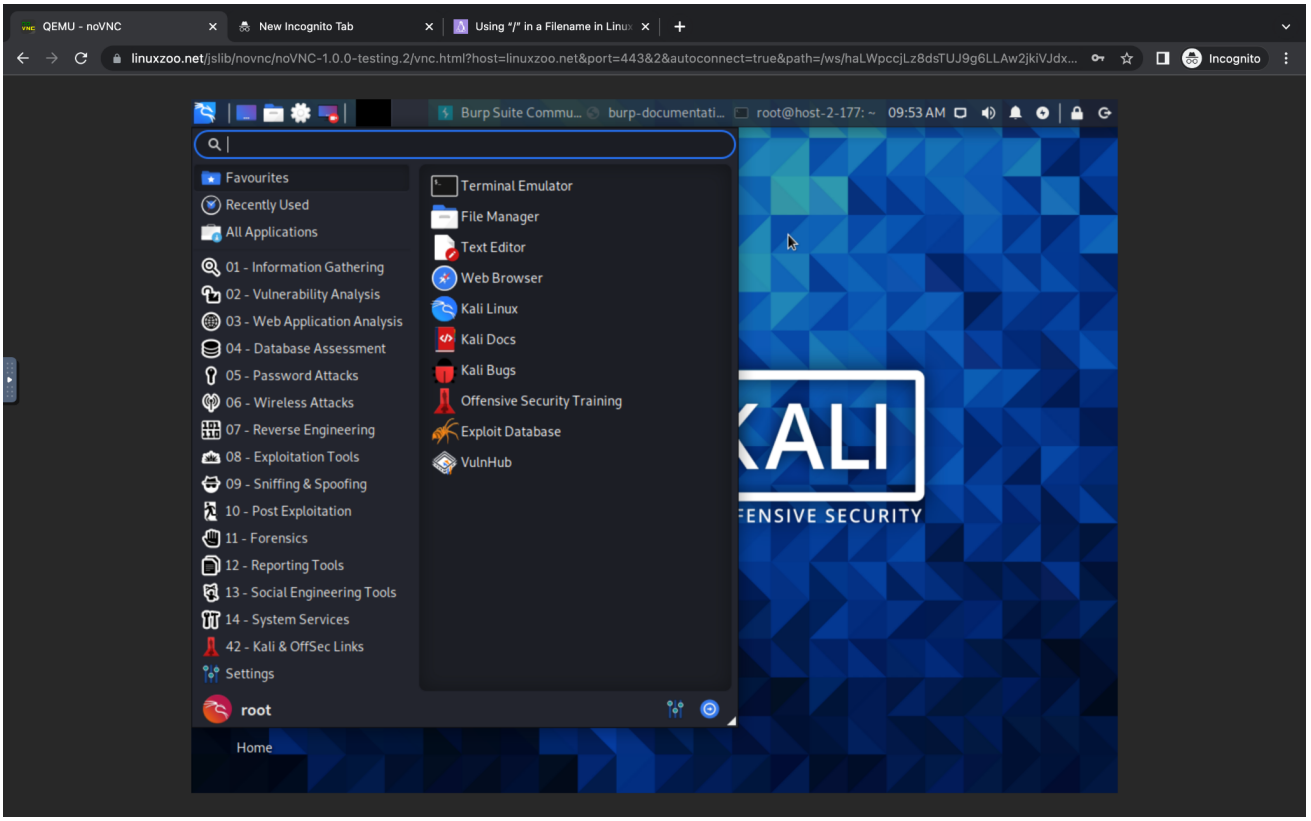


If you want to access the graphical user interface (GUI) of Kali Linux, click on the "Menu" button in the top left corner of the terminal window and then select "Applications" from the menu. From the Applications menu, you can launch different applications and tools that are installed on Kali Linux.



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.

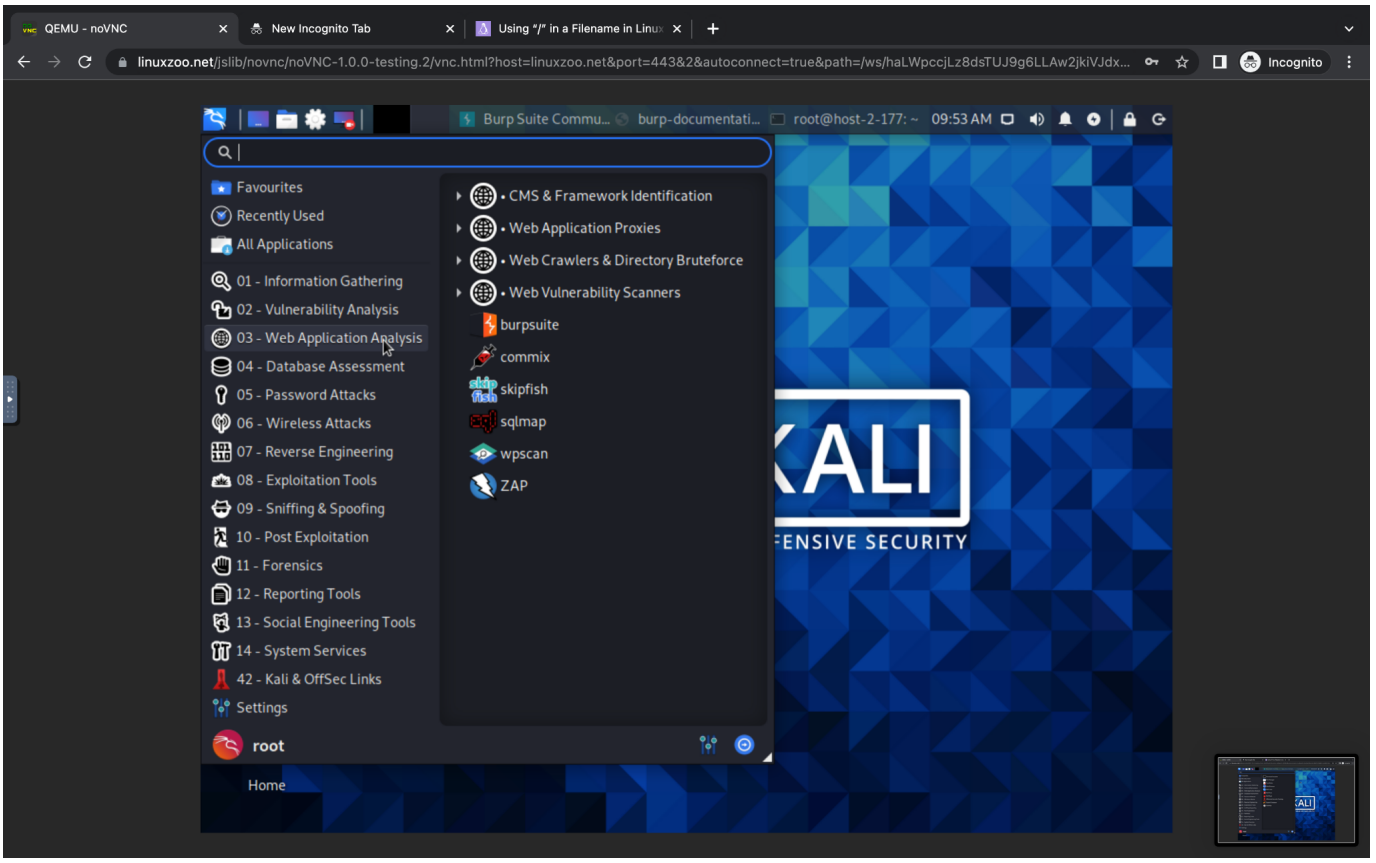
It is important to note that these are just a few examples of the many tools that are available for web application analysis in Kali Linux. It is always a good idea to research and evaluate different tools to determine which ones are best suited for your needs.

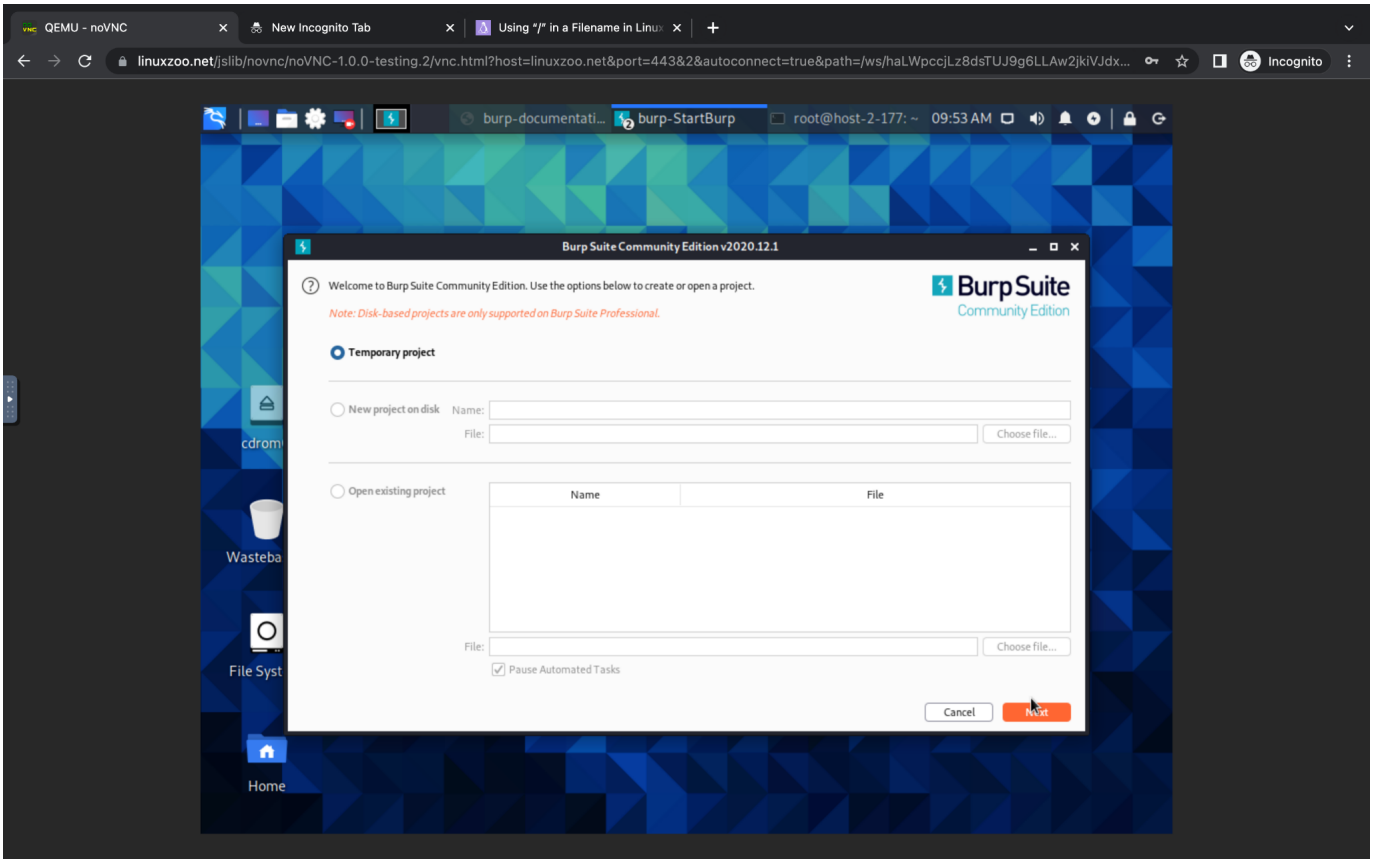
1. Burp Suite processes and analysis

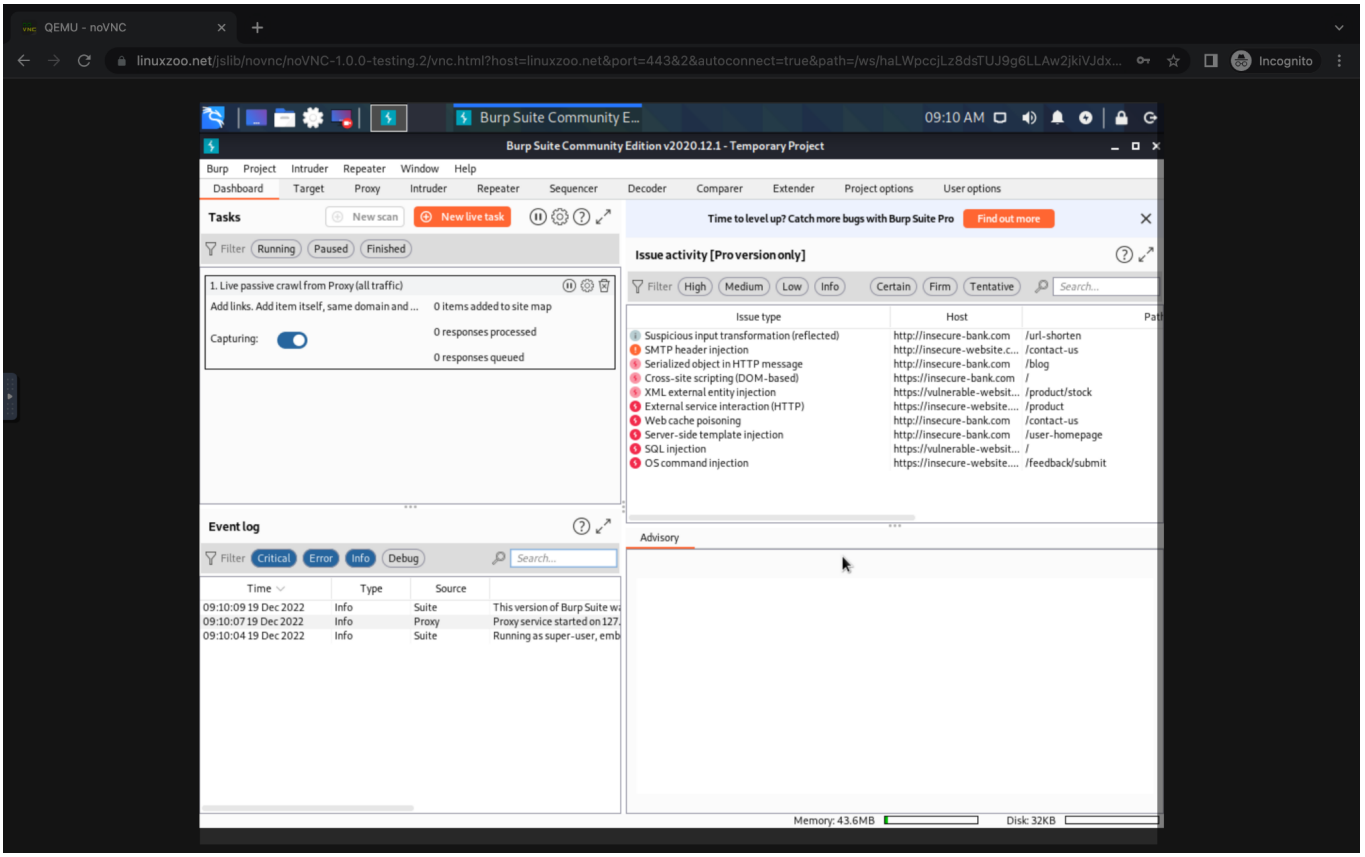
Burp Suite is a comprehensive tool for web application analysis that includes a number of features such as a web proxy, a web application scanner, and a manual testing interface. Here is an example of how you can use Burp Suite for web application analysis in Kali Linux:

- 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:




QEMU - noVNC
New Incognito Tab
Using "/" in a Filename in Linux
linuxzoo.net/jslib/novnc/noVNC-1.0.0-testing.2/vnc.html?host=linuxzoo.net&port=443&2&autoconnect=true&path=/ws/haLWpccjLz8dsTUJ9g6LLAw2jkiVJdx...
Incognito
burp-documentati...
burp-StartBurp
root@host-2-177: ~
09:53 AM
Burp Suite Community Edition v2020.12.1
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
Pause Automated Tasks
Cancel
Next
Wasteba
File Syst
Home


QEMU - noVNC
linuxzoo.net/jslib/novnc/noVNC-1.0.0-testing.2/vnc.html?host=linuxzoo.net&port=443&2&autoconnect=true&path=/ws/haLWpccjLz8dsTUJ9g6LLAw2jkiVJdx...
Incognito
Burp Suite Community E...
09:10 AM
Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Filter Running Paused Finished
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Search...
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and ...
0 items added to site map
Capturing:
0 responses processed
0 responses queued
Issue type
Host
Suspicious input transformation (reflected) http://insecure-bank.com /url-shorten
SMTP header injection http://insecure-website.c... /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-websit... /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-websit... /
OS command injection https://insecure-website.... /feedback/submit
Event log
Filter Critical Error Info Debug
Search...
Time
Type
Source
09:10:09 19 Dec 2022 Info Suite This version of Burp Suite w
09:10:07 19 Dec 2022 Info Proxy Proxy service started on 127.
09:10:04 19 Dec 2022 Info Suite Running as super-user, emb
Advisory
Memory: 43.6MB
Disk: 32KB

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.

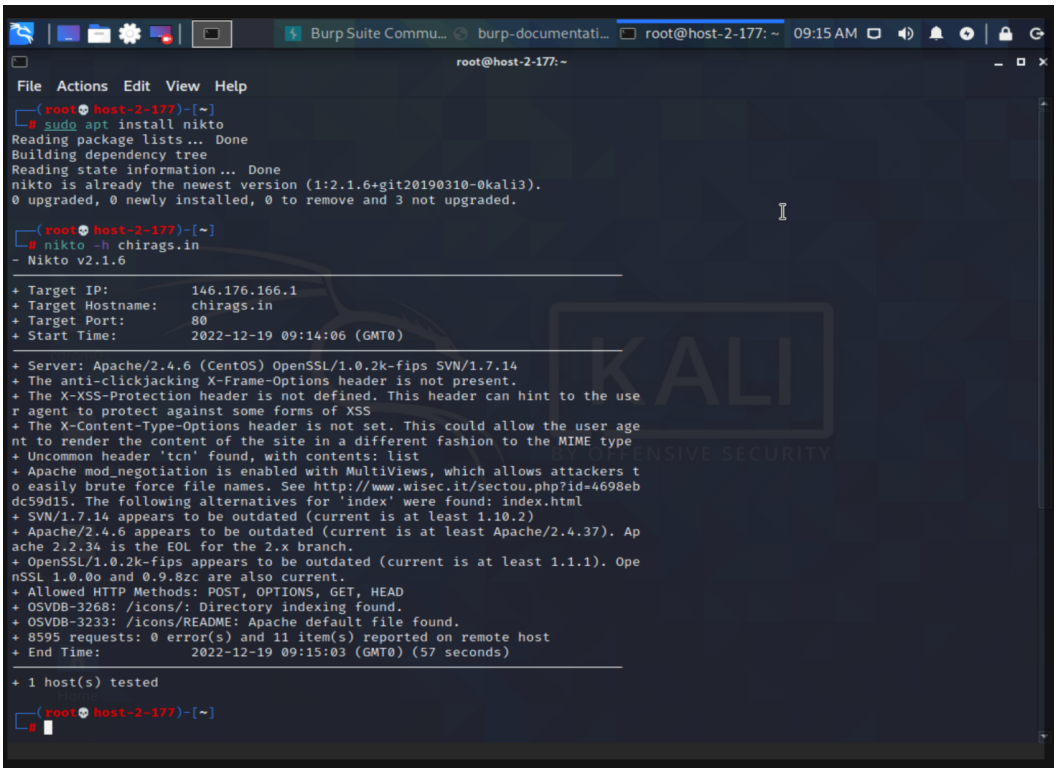
To start a scan, use the following command: `nikto -h <target URL>`

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:



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.

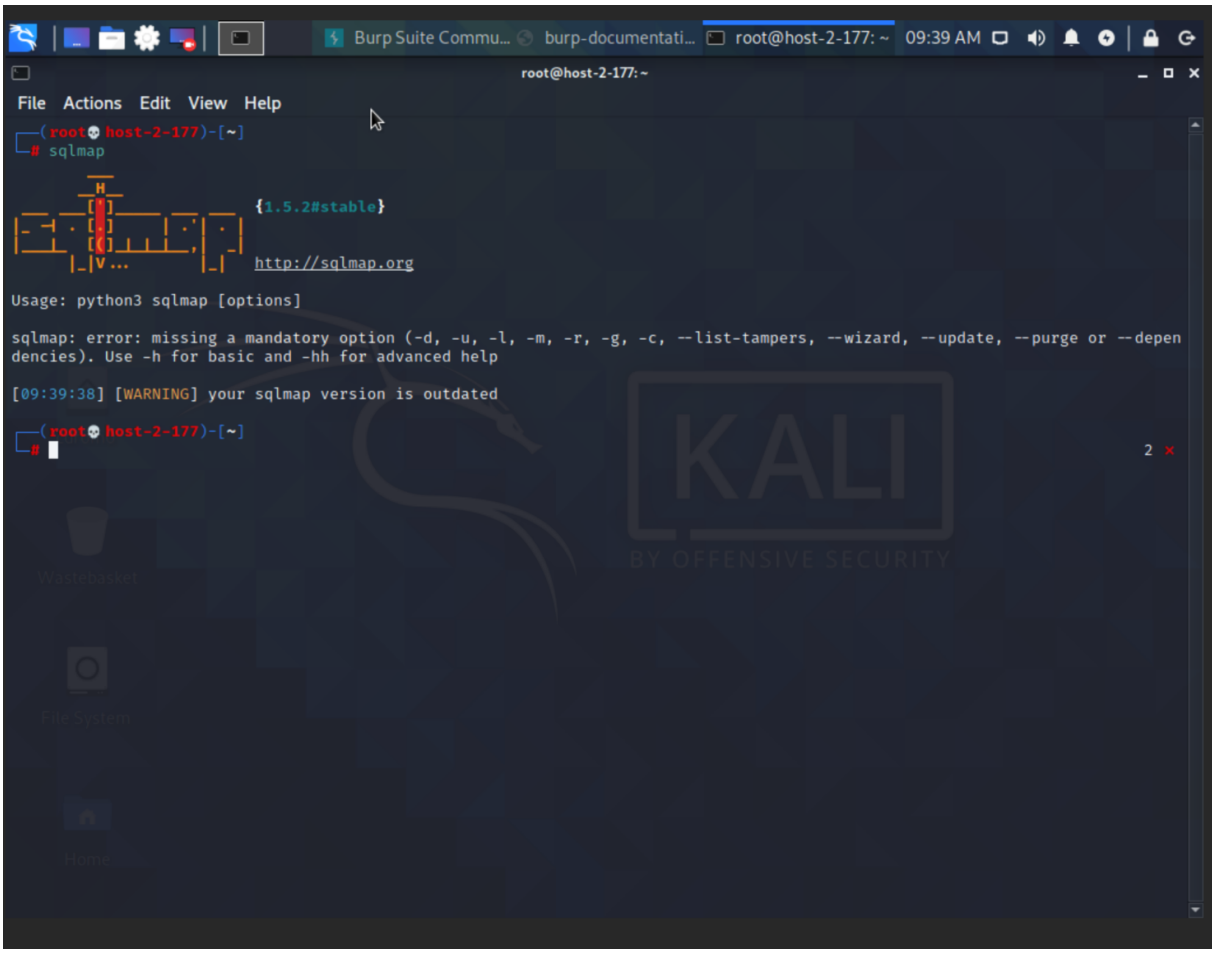
To start a scan, use the following command: sqlmap -u <target URL> --dbs

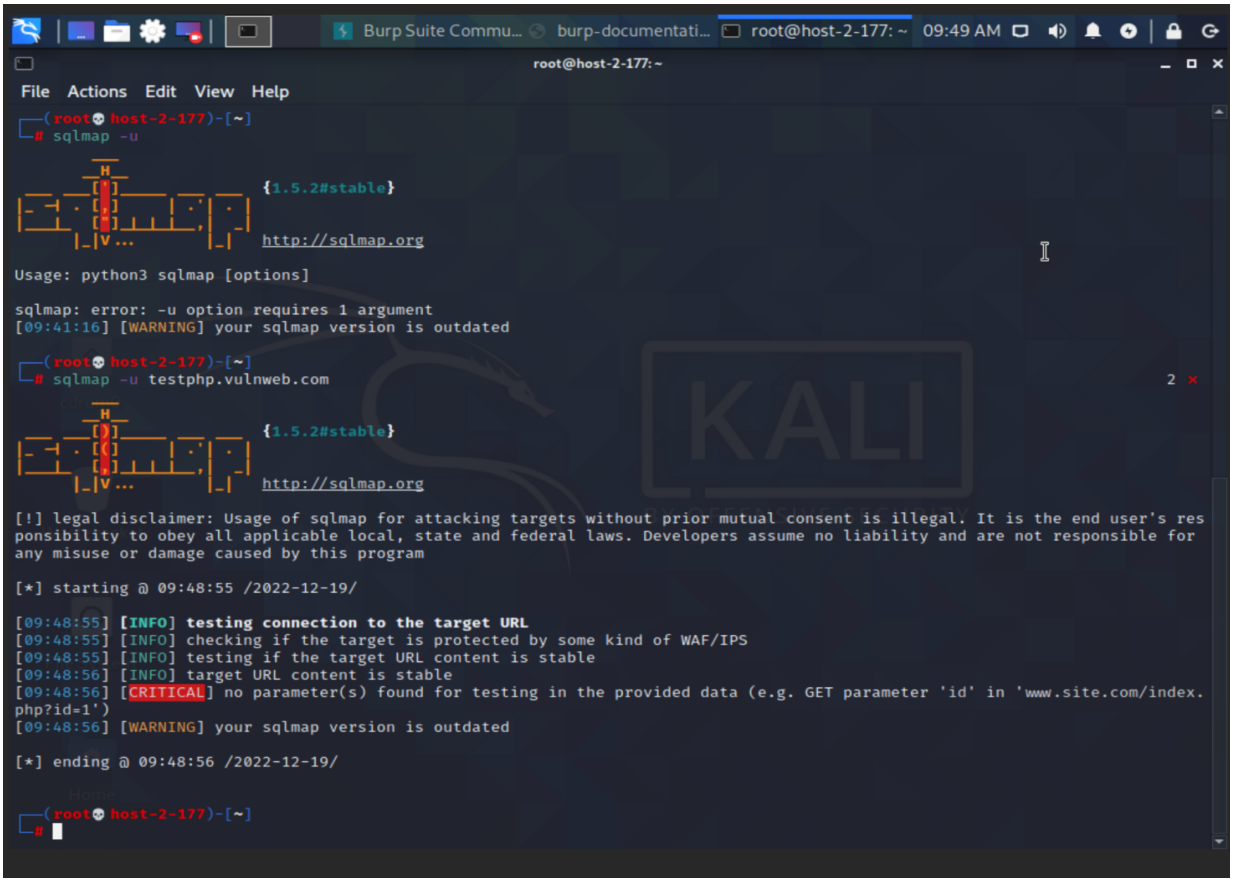
SQLMap will begin scanning the web application and will output the results to the terminal. The results will show any databases that are present on the server and any vulnerabilities that were detected.

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
```

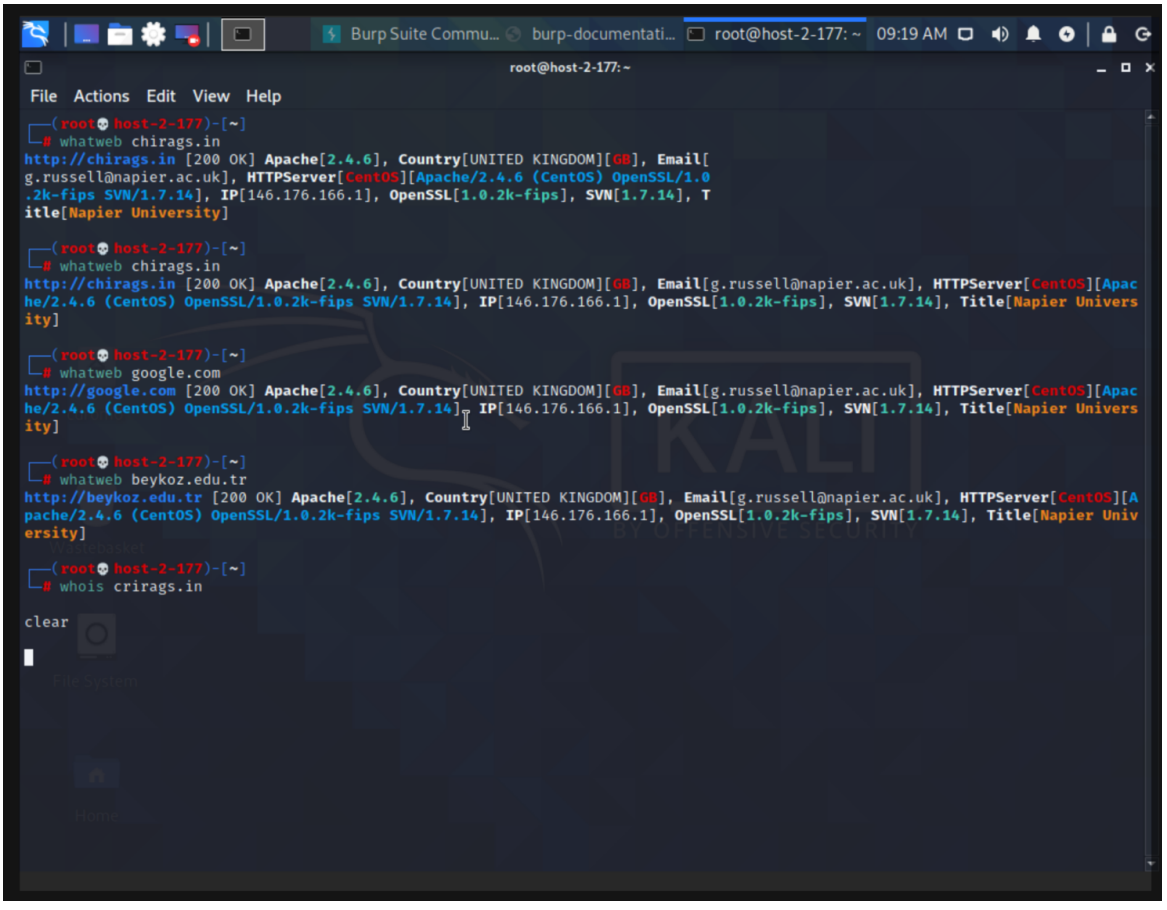
2. Install WhatWeb by running the following command:

```
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:



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.

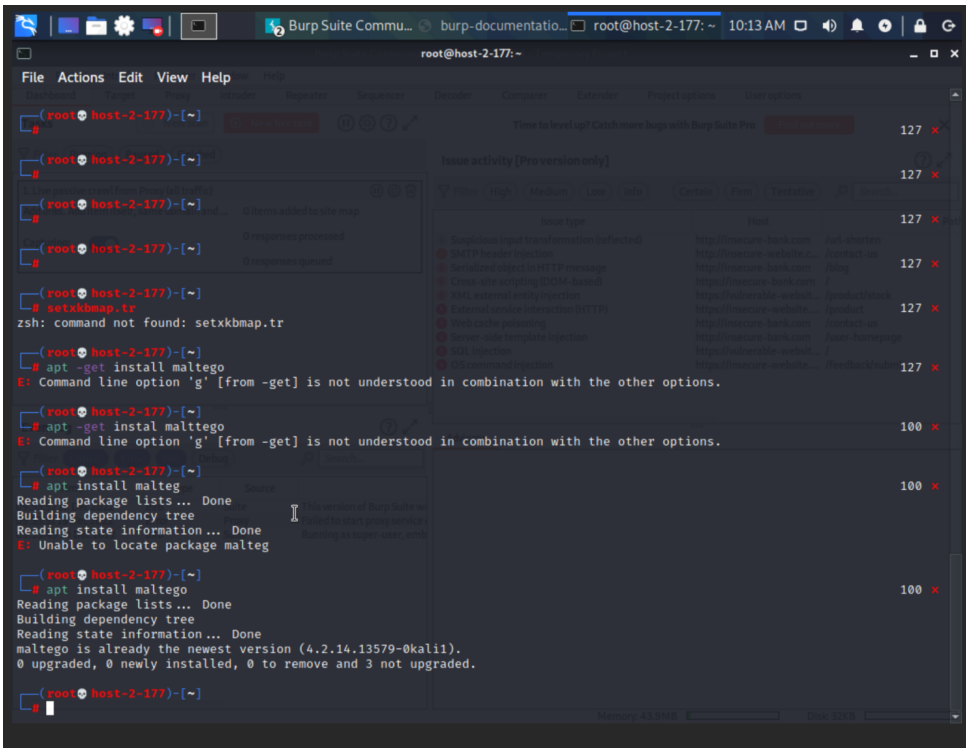
3. Run the transforms to gather information about the web application. As the transforms run, they will create entities in the graph that represent the different elements of the web application, such as domains, IP addresses, and DNS records.

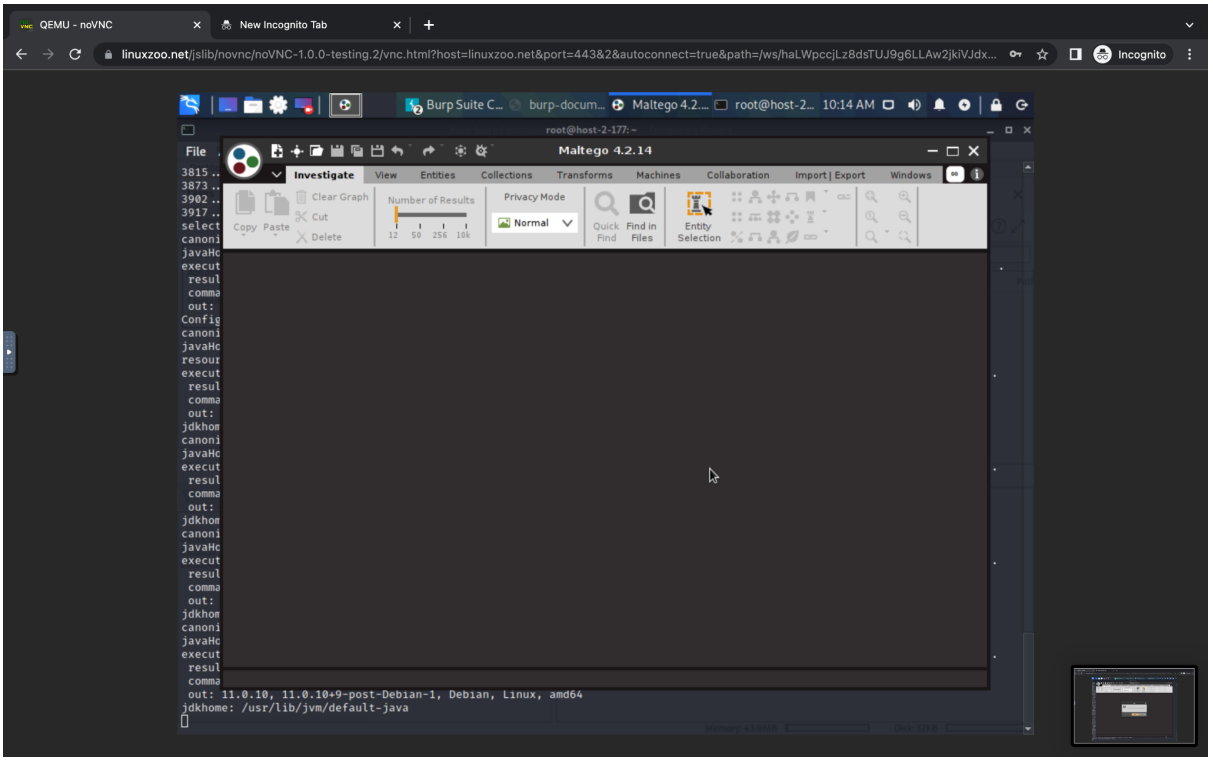
As the entities are created, they will be linked together in the graph to show the relationships between them. You can use these relationships to identify potential vulnerabilities or security risks in the web application.

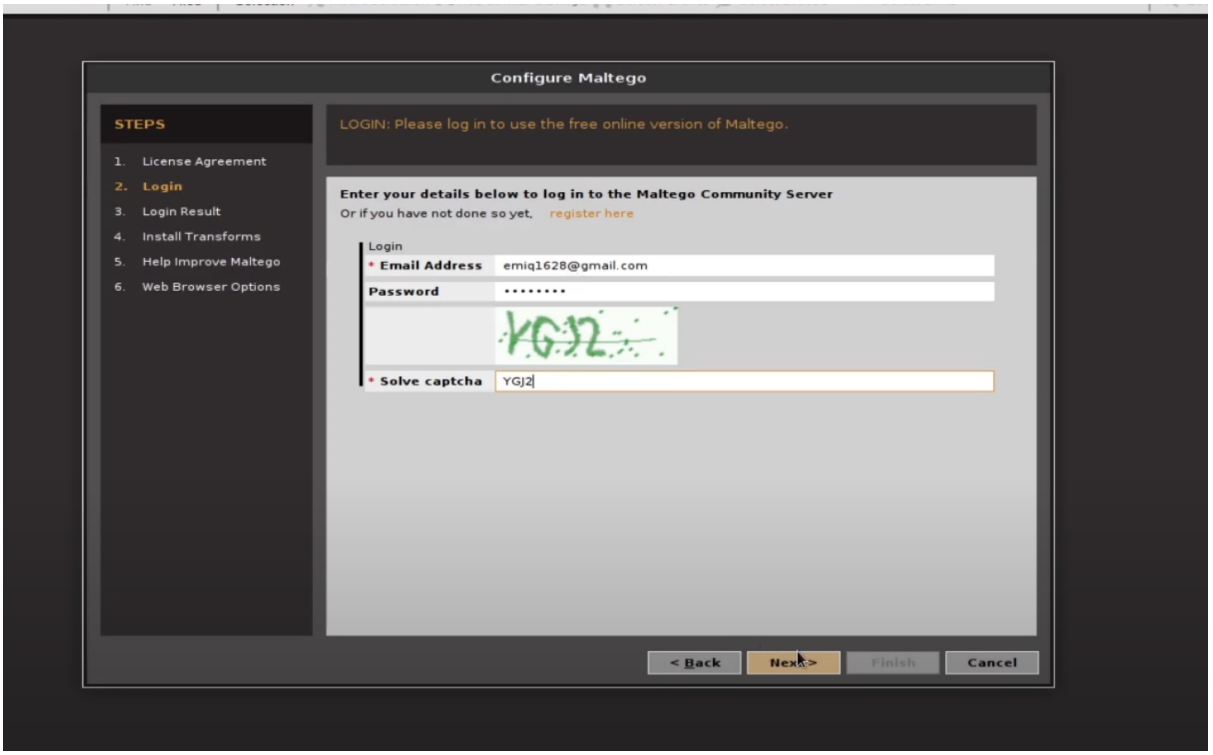
Use the information gathered by the transforms to identify and prioritize any vulnerabilities or risks that need to be addressed. You can also use Maltego to create reports or export the data for further analysis.

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.

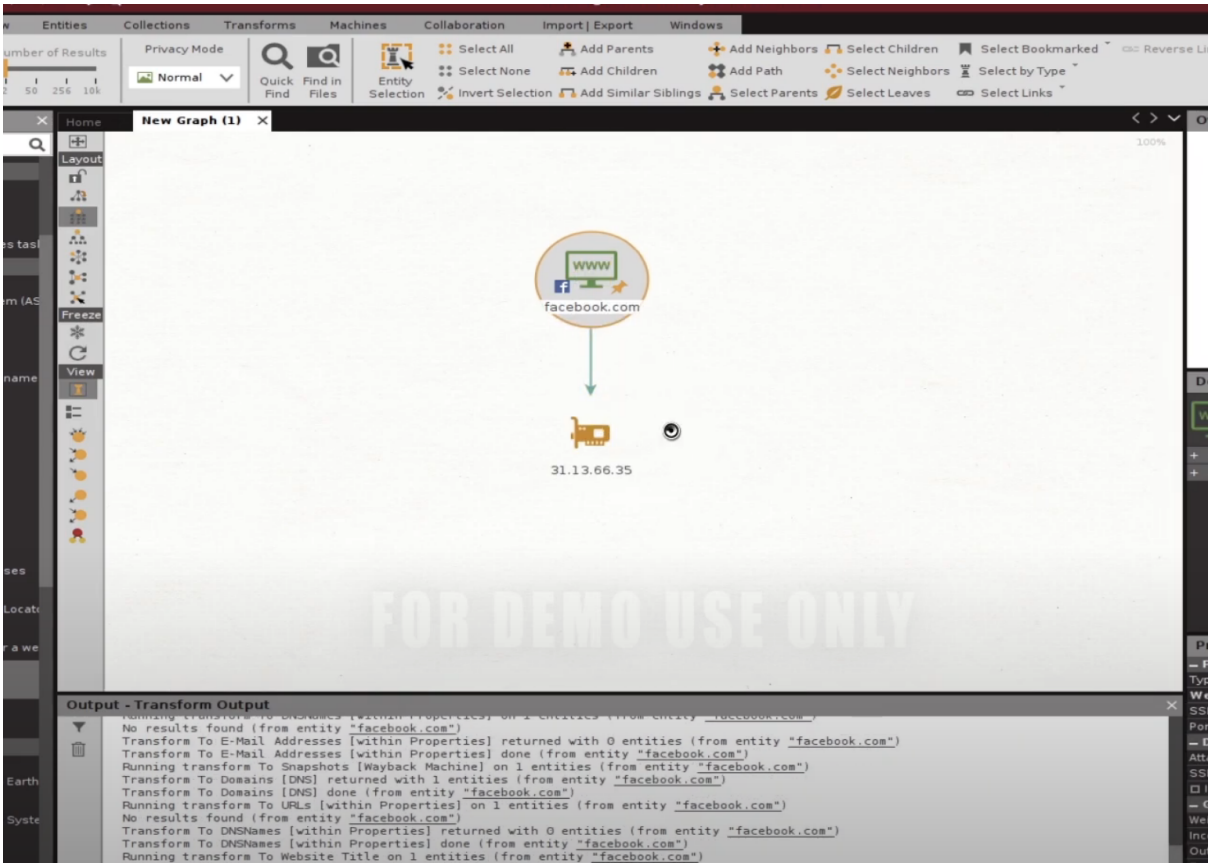




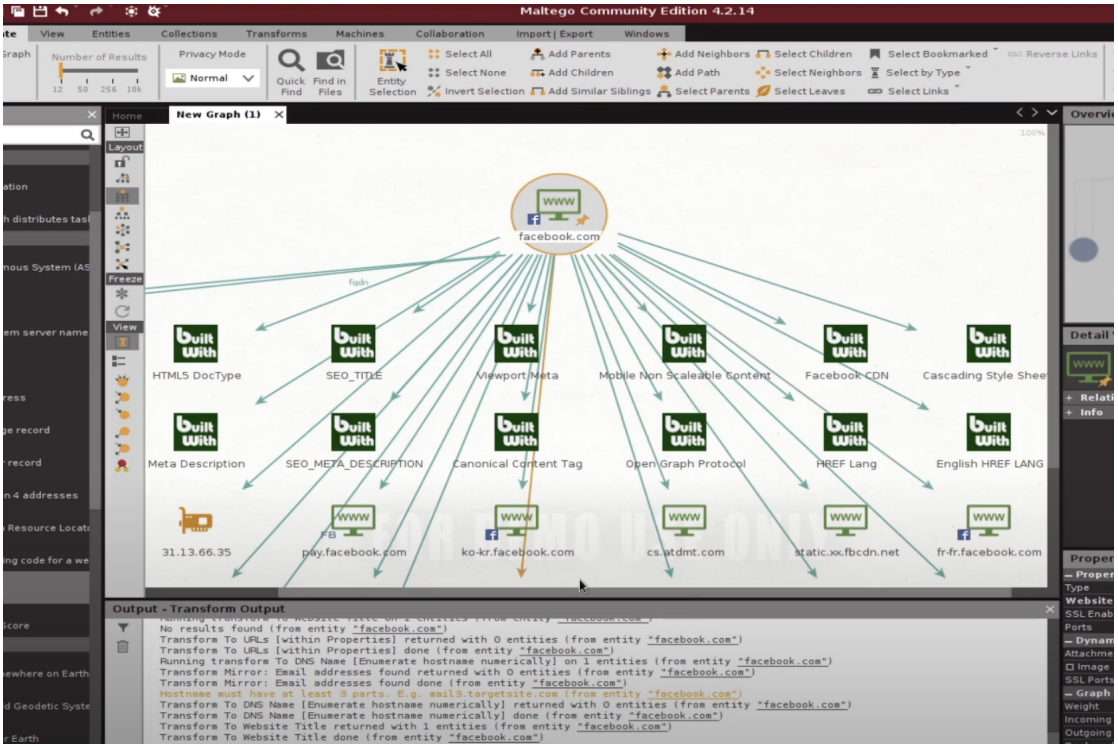


Run the transforms to gather information about the web application:

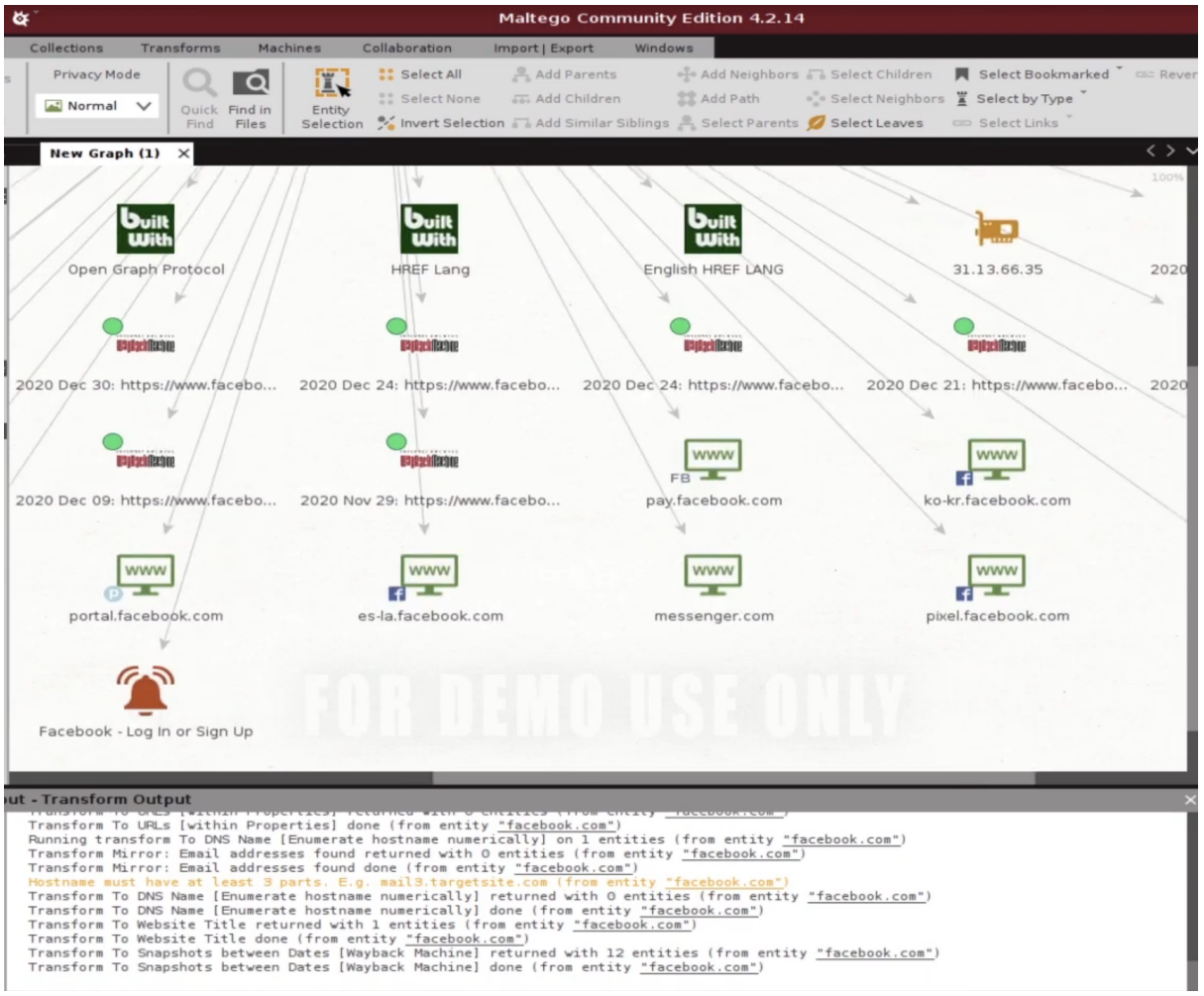
View the results in the graph to identify the relationships between different elements of the web application, such as domains, IP addresses, and DNS records.



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.



REFERENCES:

https://www.kali.org/tools/skipfish/

https://www.geeksforgeeks.org/kali-linux-web-penetration-testing-tools/

https://www.geeksforgeeks.org/kali-linux-tools/#web

https://www.javatpoint.com/kali-linux-web-application-tools

https://www.tutorialspoint.com/kali_linux/kali_linux_website_penetration_testing.htm

https://linuxzoo.net/