Beykoz University

Department of "Computer Engineering"

"Advanced Topics in Cyber Security - 60613MEEOS-CME0388"

Project - Final Submission

Web Application Testing - Kali Linux

- Final Report -

Lecturer: SHAHZAD AHMED MEMON

Leyla Abdullayeva - 1904010038

Project Description

Aim of the project:

The aim of the "Web Application Security Testing" project in Kali Linux OS is to provide a comprehensive set of tools for cybersecurity professionals and enthusiasts to identify and mitigate potential vulnerabilities in web applications. The project's tools and software are designed to help prevent attacks such as SQL injection, cross-site scripting, and others, by identifying weaknesses in web application security before they can be exploited by attackers. Ultimately, the goal is to improve the overall security of web applications and protect against potential data breaches or other cyber attacks.

What is Web Application Pen(security) 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.

What is Kali Linux OS?

Kali Linux is a popular Linux-based operating system specifically designed for cybersecurity professionals and enthusiasts. It comes pre-installed with a wide range of security tools and software for various purposes such as network analysis, vulnerability assessment, digital forensics, and penetration testing.

Kali Linux Security Testing Tools:

The tools available in Kali Linux for web application testing include SQL Injection (SQLi), Cross-Site Scripting (XSS), and many others like Skipfish and Burp Suite. SQLi and XSS are common web application vulnerabilities that can be exploited by attackers to gain unauthorized access to sensitive information or execute malicious code. SQLi can be used to inject SQL commands into a web application's backend database, allowing attackers to retrieve or modify sensitive data. XSS, on the other hand, allows attackers to inject malicious scripts into a web page viewed by other users, potentially leading to the theft of user credentials or the execution of malicious code on the user's computer. Skipfish is a web application security scanner that can be used to identify vulnerabilities such as SQLi and XSS by crawling the application and analyzing its responses. Burp Suite is another popular web application security testing tool that can be used to intercept and modify web traffic, test for vulnerabilities, and analyze the application's behavior.

These tools are essential for any cybersecurity professional or enthusiast involved in web application testing and can greatly enhance the security of web applications by identifying and mitigating vulnerabilities before they can be exploited by attackers.

Project Methotolody

- ***Define the scope and objectives of the project:*** In this step, I will identify the target web application(s) and define the goals and objectives of the testing. I will determine the testing approach and methodology, including the tools to be used and the testing techniques to be applied.

- ***Conduct reconnaissance and information gathering:*** In this step, I will collect information about the target web application using tools like WhatWeb, Whois, and Nmap to gather information about its architecture, technology stack, and potential vulnerabilities.

- ***Perform vulnerability scanning:*** In this step, I will use tools like Nikto, Skipfish, and Burp Suite to identify potential security vulnerabilities in the web application, such as SQL injection, cross-site scripting (XSS), and directory traversal.

- ***Exploit and perform penetration testing:*** In this step, I will use tools like SQLMap, XSSer, and BruteXSS to exploit identified vulnerabilities in the web application and test its resilience against various attack scenarios. I will also perform penetration testing to identify any weaknesses in the system's defenses and identify potential attack vectors.

- ***Generate reports and documentation:*** In this step, I will document the results of the testing, including identified vulnerabilities and recommendations for remediation. I will create a detailed report that includes the methodology used, testing results, and any remediation recommendations.

- ***Provide recommendations for remediation and follow-up:*** In this step, I will provide recommendations for remediation of identified vulnerabilities to the client or development team. I will also follow up with the client or development team to ensure that remediation is completed, and the web application is secure.

- ***Record a demo of the testing process:(2nd sub)*** In this step, I will record a demo of the testing process to demonstrate the methodology and techniques used to test the web application's security.

- ***Divide the demo recording into steps:*** In this step, I will divide the demo recording into steps to provide a clear and concise overview of the testing process.

- ***Edit and finalize the demo recording:*** In this step, I will edit and finalize the demo recording to ensure it accurately reflects the testing process and methodology used.

1. Information Gathering

Tool	Description
★ Whois	A tool for querying domain registration information to help identify the owner of a website or domain.
★ Nmap	A network exploration tool that includes various features for scanning and analyzing web applications.

2. Web Application Scanning

Tool	Description
★ Nikto	A web server scanner that checks for potentially dangerous files or programs.
★ Skipfish	A fast and lightweight web application security scanner that is optimized for detecting security issues.
★ WPScan	A WordPress vulnerability scanner that can detect security issues such as weak passwords, outdated plugins or themes, and more.
★ WhatWeb	A tool for identifying the technologies and frameworks used by a website, which can be useful for identifying potential vulnerabilities or attack vectors.
★ Gobuster	A tool for discovering hidden web content, such as directories and files, on a web server.

3. SQL Injection

Tool	Description
★ SQLmap	A powerful tool for detecting and exploiting SQL injection vulnerabilities in web applications.
★ SQLninja	A tool for exploiting SQLi vulnerabilities in web applications, particularly those using Microsoft SQL Server.

4. Cross-Site Scripting (XSS)

★ XSSer	A tool for detecting and exploiting XSS vulnerabilities in web applications.
★ BruteXSS	A tool for testing web applications for XSS vulnerabilities using brute force techniques.
★ Burp Suite	A comprehensive web application security tool for intercepting, testing, and modifying web traffic.

Why I selected these tools and How it will be used:

For my Web Application Security Testing project using Kali Linux OS, I plan to use a variety of tools to detect and exploit vulnerabilities in web applications. Burp Suite will be used for intercepting and modifying web traffic, while Nikto and Nmap will be used to scan web servers for potential security issues. Skipfish will be used for detecting security issues, and SQLmap will be used to detect and exploit SQL injection vulnerabilities in web applications. Whois will be used to identify the owner of a website or domain, WPScan will be used to scan WordPress websites for vulnerabilities, and WhatWeb will be used to identify the technologies and frameworks used by a website. XSSer and BruteXSS will be used for testing web applications for XSS vulnerabilities, while SQLninja will be used to exploit SQLi vulnerabilities, particularly those using Microsoft SQL Server. Finally, Gobuster will be used to discover hidden web content, such as directories and files, on a web server.

Tool	Why selected	How it will be used
Burp Suite	Comprehensive tool for intercepting, testing, and modifying web traffic	To identify and exploit vulnerabilities in web applications by intercepting and modifying web traffic
Nikto	Web server scanner that checks for over 6700 potentially dangerous files or programs	To scan web servers for potential security issues and vulnerabilities
Nmap	Network exploration tool that includes various features for scanning and analyzing web applications	To scan and analyze web applications for potential vulnerabilities
Skipfish	Fast and lightweight web application security scanner that is optimized for detecting security issues	To detect security issues in web applications
SQLmap	Powerful tool for detecting and exploiting SQL injection vulnerabilities in web applications	To detect and exploit SQL injection vulnerabilities in web applications

Whois	Tool for querying domain registration information to help identify the owner of a website or domain	To identify the owner of a website or domain
WPScan	WordPress vulnerability scanner that can detect security issues such as weak passwords, outdated plugins or themes, and more	To scan WordPress websites for vulnerabilities
WhatWeb	Tool for identifying the technologies and frameworks used by a website	To identify potential vulnerabilities or attack vectors
XSSer	Tool for detecting and exploiting XSS vulnerabilities in web applications	To detect and exploit XSS vulnerabilities in web applications
BruteXSS	Tool for testing web applications for XSS vulnerabilities using brute force techniques	To test web applications for XSS vulnerabilities using brute force techniques
SQLninja	Tool for exploiting SQLi vulnerabilities in web applications, particularly those using Microsoft SQL Server	To exploit SQL injection vulnerabilities in web applications
Gobuster	Tool for discovering hidden web content, such as directories and files, on a web server	To discover hidden web content on a web server

Project Description:

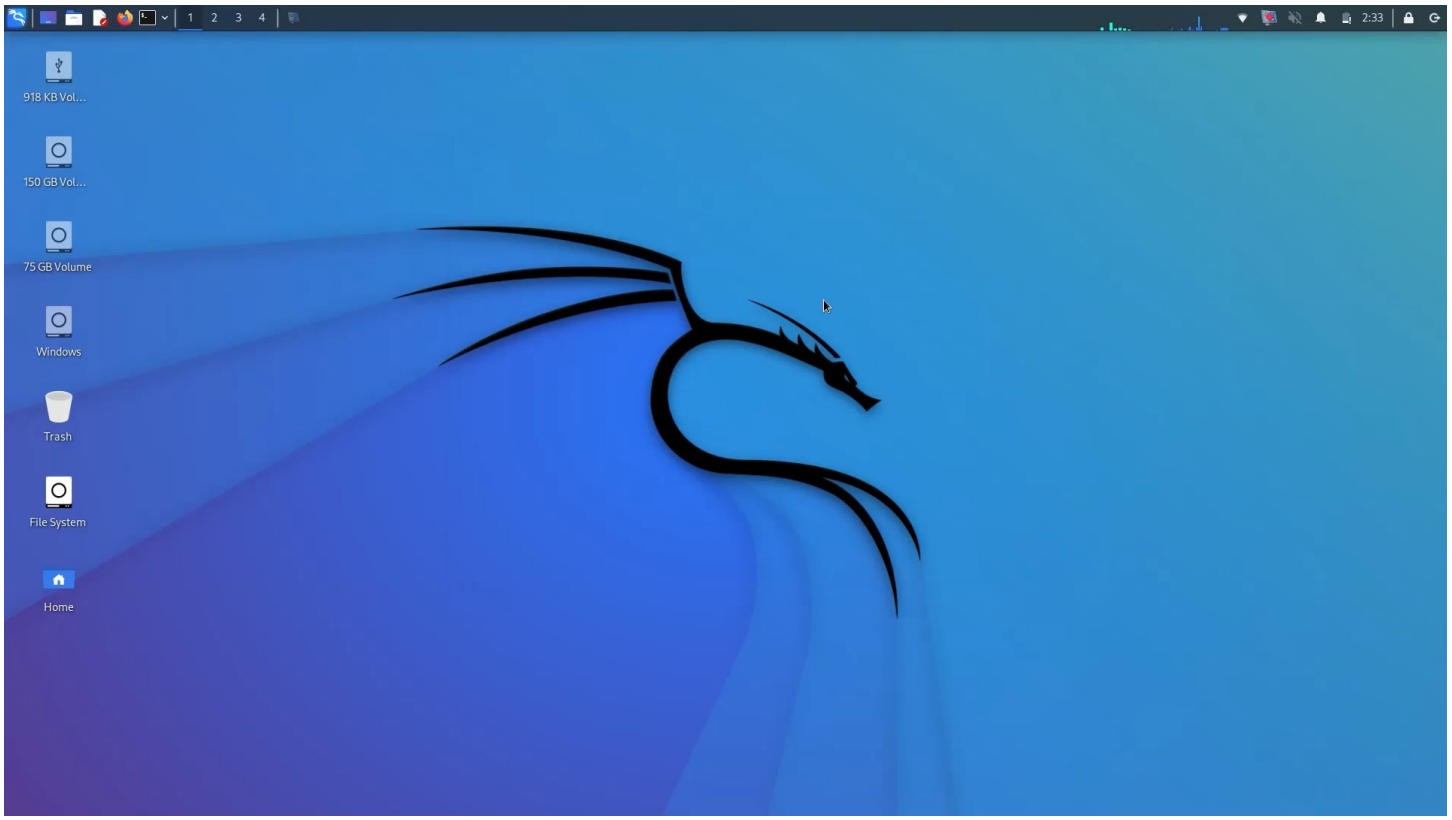
The project "Web Application Security Testing with Kali Linux" aims to assess the security of web applications using various tools available in Kali Linux, such as Nikto, Nmap, and XSSer. The testing involves identifying vulnerabilities in web applications and exploiting them to evaluate the effectiveness of the security controls in place. The project also includes documentation of the testing methodology, findings, and recommendations for improving the security posture of the web application.

Categories of Tools that I'll use for my project:

- Information Gathering
- Web Application Scanning
- SQL Injection
- Cross-Site Scripting (XSS)

Design and Implementation (Demo)

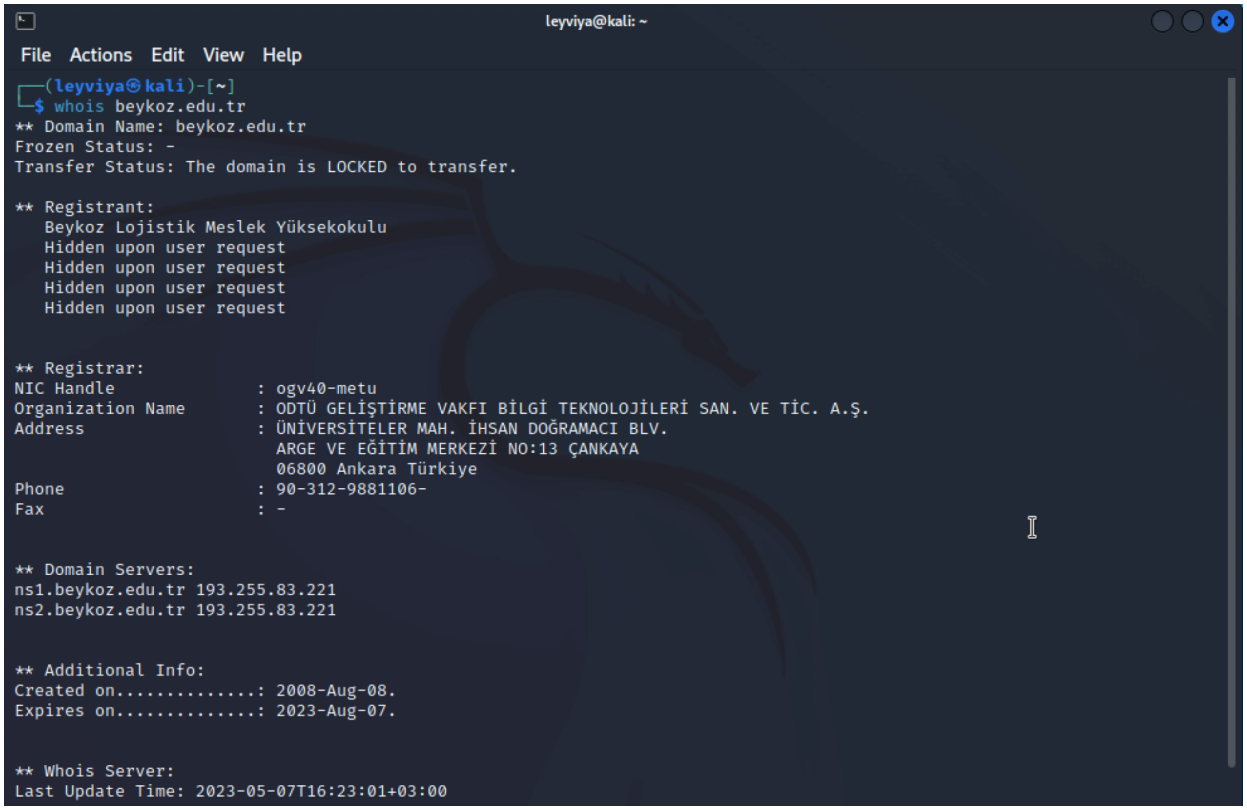
I choose only 1 tool for each category, I'll use more for final submission. I've added snapshots and screenshots of the tools that I've used with Kali Linux. Outcome analysis is provided for each.



1. Information Gathering

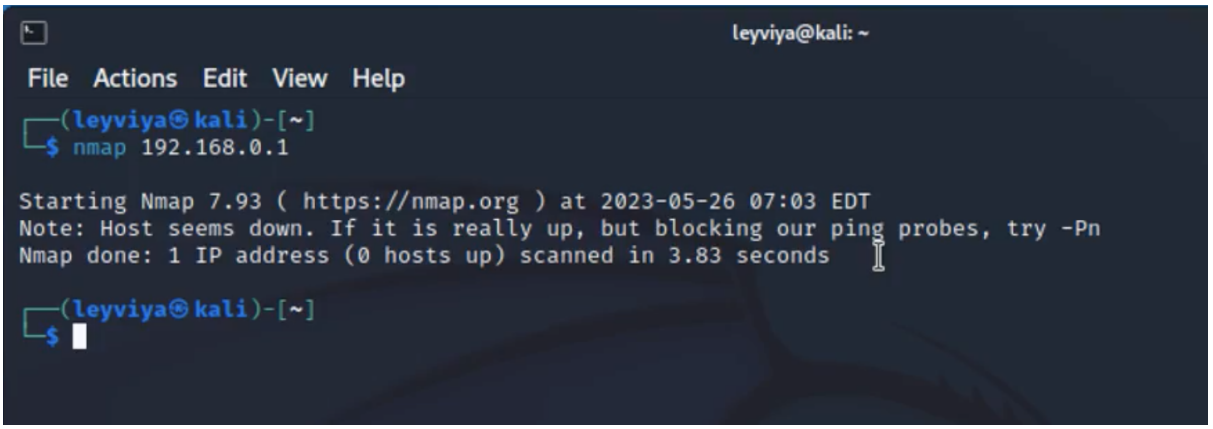
Whois	To identify the owner of a website or domain

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - whois



Nmap	To scan and analyze web applications for potential vulnerabilities

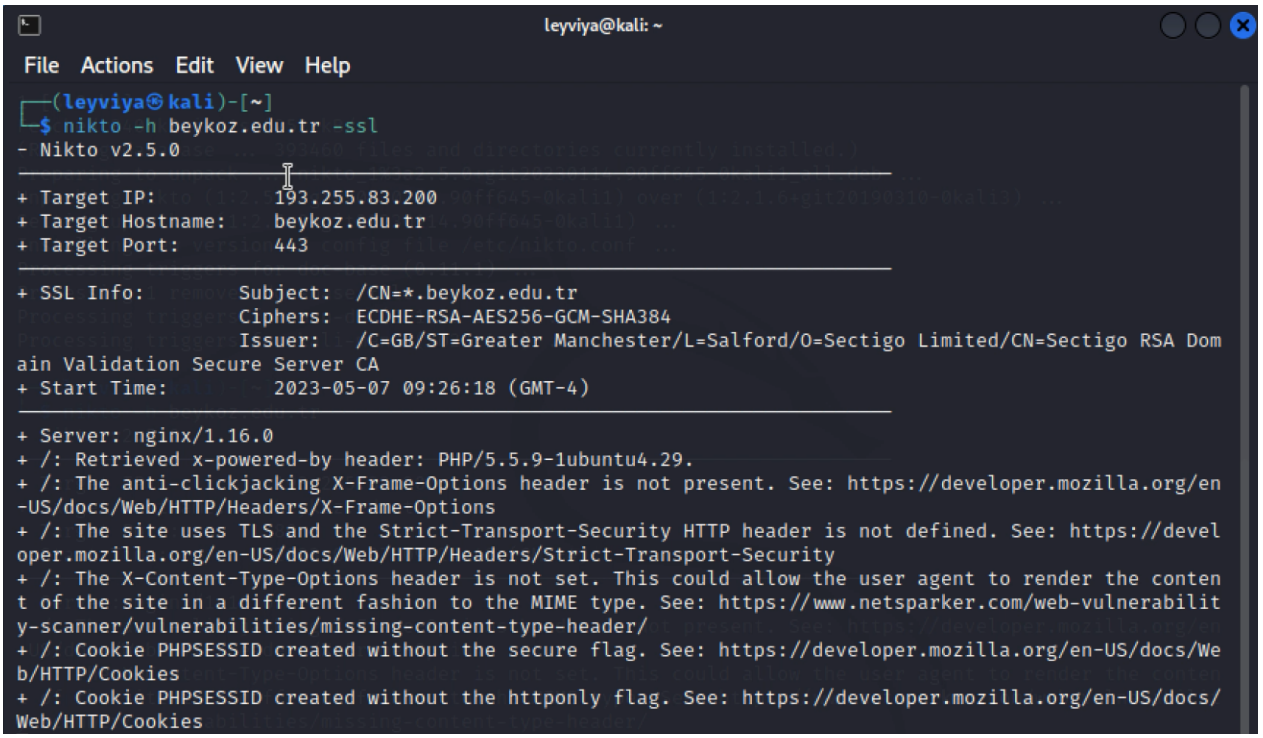
Snapsot & Screenshot from Kali Linux: (Click on the link and video will appear) - nmap



2. Web Application Scanning

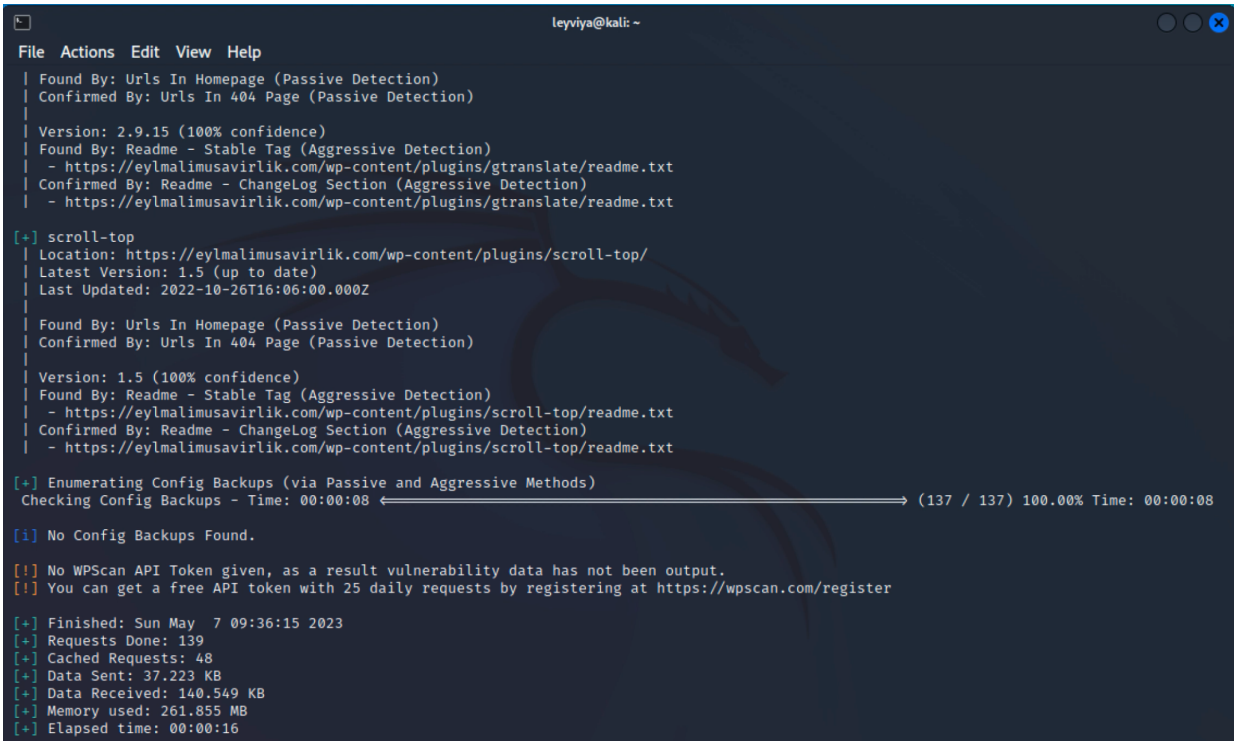
Nikto	To scan web servers for potential security issues and vulnerabilities

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - nikto



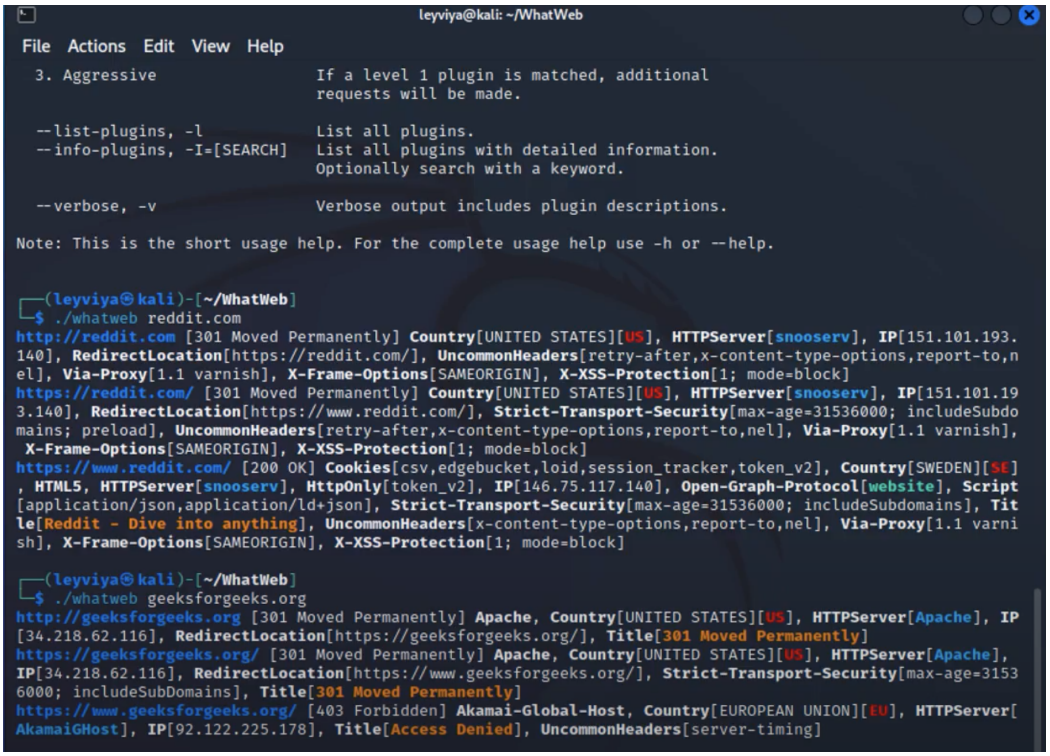
WPScan	To scan WordPress websites for vulnerabilities

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - wpscan



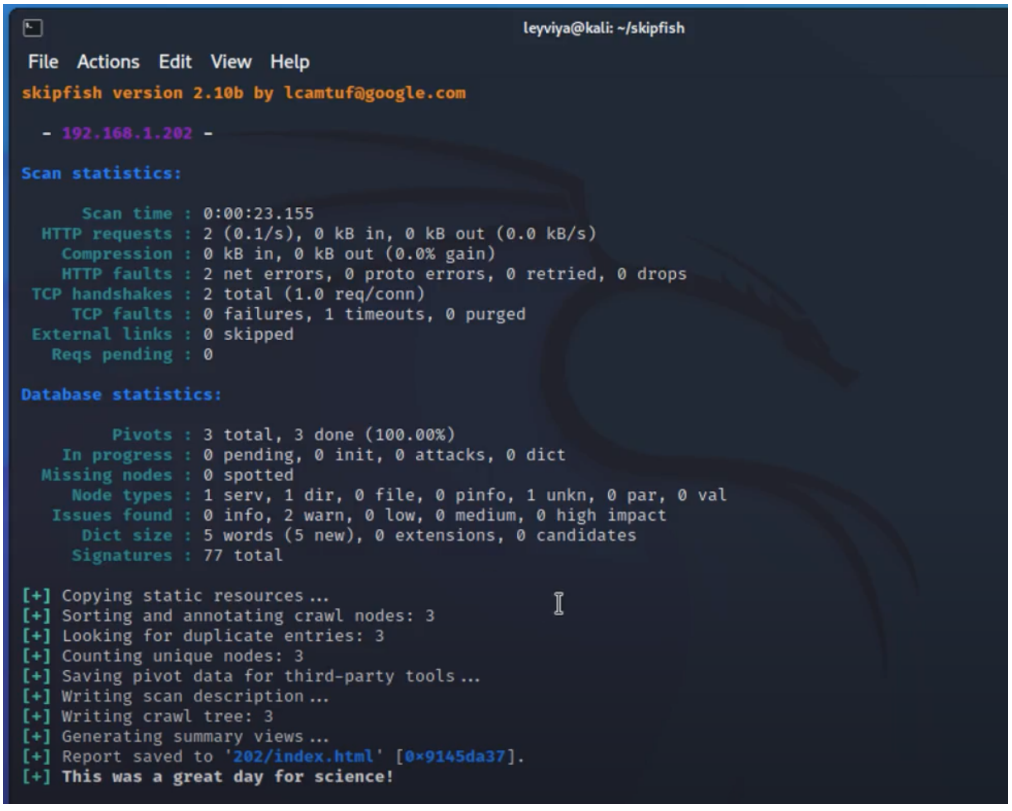
WhatWeb	To identify potential vulnerabilities or attack vectors

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - whatweb



Skipfish	To detect security issues in web applications

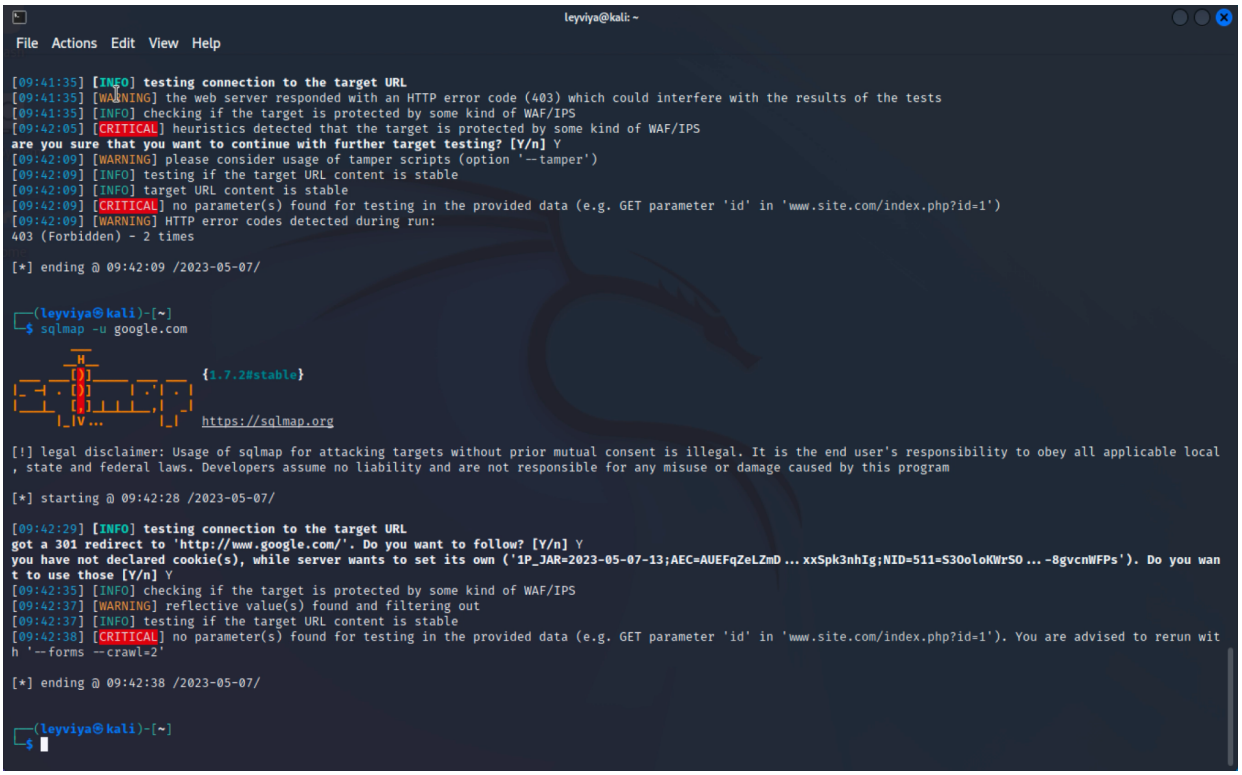
Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - Skipfish



3. SQL Injection

SQLmap	To detect and exploit SQL injection vulnerabilities in web applications

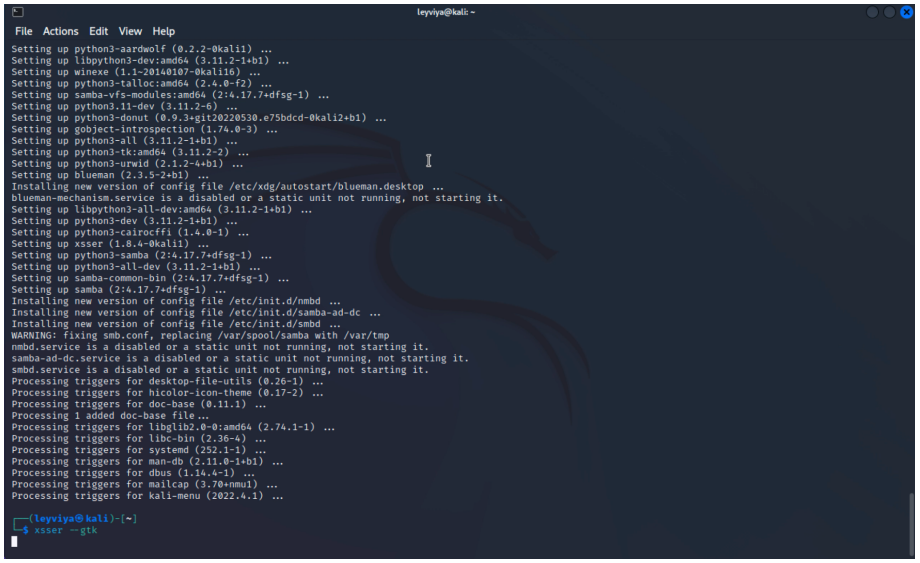
Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - sqlmap



4. Cross-Site Scripting (XSS)

XSSer	To detect and exploit XSS vulnerabilities in web applications

Snapshot & Screenshot from Kali Linux: (Click on the link and video will appear) - xsser



REFERENCES:

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