Beykoz University

Department of "Computer Engineering"

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

Project I

Web Application Testing - Kali Linux

- Interim Report -

Lecturer: SHAHZAD AHMED MEMON

Leyla Abdullayeva - 1904010038

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 is widely used in the cybersecurity industry and can be run on various devices such as laptops, desktops, and Raspberry Pi.

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.

Tools I'll use for Web App Security Testing:

★ Burp Suite	A comprehensive web application security tool for intercepting, testing, and modifying web traffic.
★ Nikto	A web server scanner that checks for over 6700 potentially dangerous files or programs.
★ Nmap	A network exploration tool that includes various features for scanning and analyzing web applications.
★ Skipfish	A fast and lightweight web application security scanner that is optimized for detecting security issues.
★ SQLmap	A powerful tool for detecting and exploiting SQL injection vulnerabilities in web applications.
★ Whois	A tool for querying domain registration information to help identify the owner of a website or domain.
★ 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.
★ 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.
★ SQLninja	A tool for exploiting SQLi vulnerabilities in web applications, particularly those using Microsoft SQL Server.
★ Gobuster	A tool for discovering hidden web content, such as directories and files, on a web server.

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

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/