Innovation Center for Education

TRUSTED DELIVERY PARTNER for IBM ICE

Yenepoya Institute of Arts, Science, Management & commerce

PROJECT SYNOPSIS

VULNERABILITY ASSESSMENT OF A WEB APPLICATION

BACHELOR OF SCIENCE

COMPUTER SCIENCE

SUBMITTED BY

Abhiraj A -22BCACDC04

DAIVIK RAJESH -22BCACDC16

MUHAMMED HANIN ALFAS M -22BCACDC43

ROBIN PUTHUPARAMPIL ROY -22BCACDC59

VAISHNAVI -22BSCFDC45

GUIDED BY

SASHANK

Table of Contents

Introduction

This project involves performing a vulnerability assessment on a real-world web application as part of an internship-based cybersecurity initiative. The objective was to identify, analyze, and report potential security weaknesses in the target web applications. Tools like Burp Suite,

Dirb, and manual payloads were used to test the application for common vulnerabilities like SQL Injection (SQLi) and Cross-Site Scripting (XSS).

The websites tested include:

https://christhujyothi.com

https://demotestfire.net

The assessment was conducted using ethical hacking techniques under proper authorization.

Technology Used

Burp Suite (for intercepting and testing web requests)

Dirb (for directory enumeration)

Manual SQLi and XSS payloads

Kali Linux (penetration testing environment)

Field of Project

This project falls under the field of Cybersecurity, specifically under Web Application Security Testing.

Special Technical Terms

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing vulnerabilities in a system.

SQL Injection (SQLi): A web security vulnerability that allows an attacker to interfere with the queries an application makes to its database.

Cross-Site Scripting (XSS): A vulnerability that allows an attacker to inject malicious scripts into content from otherwise trusted websites.

Dirb: A web content scanner useful for brute-forcing directories and file names.

Project Goal

The goal of the project is to demonstrate the ability to ethically discover and report vulnerabilities in a live web application, increasing its security posture and awareness of cyber risks.

Methodology/Planning of Work

Project Development Steps

1. Requirement Analysis: Define scope and permissions for testing.

2. Reconnaissance: Gather publicly available information and test input points.

3. Directory Enumeration: Use Dirb to discover hidden paths and sensitive files.

4. Vulnerability Testing:

Inject test payloads for SQLi and XSS.

Analyze web responses using Burp Suite.

5. Report Generation: Document findings with screenshots and possible fixes.

6. Validation: Retest to confirm identified vulnerabilities.

Tools and Resources

Burp Suite Community Edition

Dirb (command-line tool)

Kali Linux (VirtualBox Environment)

SQLi/XSS Payload Lists (Manually crafted)

Timeline

Week 1: Setup environment (VirtualBox, Kali Linux, Tools installation)

Week 2: Recon and Dirb scan

Week 3: Manual testing with payloads for XSS and SQLi

Week 4: Report writing and validation of vulnerabilities

Facilities Required for Proposed Work

Hardware Requirements

System with minimum 8GB RAM

VirtualBox-capable machine

Stable internet for testing and tool usage

Software Requirements

1. Kali Linux (Running in VirtualBox) – A Linux OS used for ethical hacking, running safely in a virtual environment.

2. Burp Suite – A tool for testing web application security by intercepting and analyzing HTTP requests.

3. Dirb – A tool to find hidden directories and files on a web server through brute-forcing.

4. Web Browser – Used for manually testing the web application and executing payloads.

Additional Requirements

References

Permission to test live websites

Network access to the target application

Logging tools (screenshot software, notes)

Study Materials

1. OWASP Testing Guide – A comprehensive manual for testing web application security vulnerabilities.

2. Kali Linux Documentation – Official guide for using and configuring Kali Linux tools and features.

3. The Web Application Hacker's Handbook – A practical guide for finding and exploiting web application vulnerabilities.

4. OWASP Top 10 – A list of the ten most critical web application security risks with explanations and mitigation techniques.

5. Metasploit Unleashed – A detailed resource for learning how to use the Metasploit Framework for penetration testing.

6. Burp Suite Documentation – Official guide for using Burp Suite effectively in web vulnerability

Online Resources

The following online resources were also utilized:

1. Google – for gathering payloads and understanding test results

2. PortSwigger Web Security Academy (Burp Suite Learning)

3. YouTube tutorials and ethical hacking blogs

4. Cybersecurity forums and GitHub repositories