Vulnerability Assessment and Penetration Testing

Week 2 Practical Assessment Report

Prepared by: Cinchana S
Role: VAPT Intern
Environment: Controlled Lab
Date: 09-01-2026

Executive Summary (Non-Technical)

This assessment was conducted to evaluate the security posture of web applications and systems in a controlled lab environment. The objective was to identify common security weaknesses and understand their potential impact if exploited by an attacker.

During testing, several high-risk vulnerabilities were identified, including weak input validation, outdated software components, and misconfigurations that could allow unauthorized access. These vulnerabilities could lead to data exposure, service disruption, or full system compromise if not addressed.

All findings were validated using industry-standard tools and methodologies. Addressing these issues through regular patching, secure coding practices, and periodic security testing will significantly reduce overall security risks.

Introduction

This report documents the Vulnerability Assessment and Penetration Testing (VAPT) activities performed during Week 2 of the internship program. The assessment focused on gaining practical experience with real-world security tools while following standard penetration testing methodologies.

The testing was conducted strictly in a controlled lab environment using intentionally vulnerable systems. The purpose of this exercise was educational, aimed at understanding how attackers identify and exploit vulnerabilities, and how such issues can be documented and remediated.

Scope of Assessment

The scope of this assessment included the following targets:

- Metasploitable2 virtual machine
- Damn Vulnerable Web Application (DVWA)

The assessment was limited to:

- Reconnaissance and information gathering
- Vulnerability scanning
- Controlled exploitation
- Post-exploitation validation
- Reporting and remediation recommendations

No real-world systems or unauthorized networks were tested during this activity.

Methodology

The assessment followed the Penetration Testing Execution Standard (PTES), which provides a structured approach to security testing. The phases included reconnaissance, vulnerability analysis, exploitation, post-exploitation, and reporting.

Each phase was performed sequentially to simulate a real penetration testing workflow. This ensured proper documentation, validation of findings, and meaningful remediation recommendations.

Tools Used

The following tools were used during the assessment:

- Kali Linux as the primary testing platform
- Nmap for network scanning and service discovery
- OpenVAS for vulnerability assessment
- Maltego and Shodan for reconnaissance
- Burp Suite for web traffic analysis
- sqlmap for SQL Injection testing
- Metasploit Framework for exploitation

Documentation was prepared using Google Docs and later exported as PDF.

Vulnerability Assessment Findings

The vulnerability scanning phase identified multiple issues across the tested systems. High-severity findings included outdated services, weak authentication mechanisms, and web application vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS).

Each vulnerability was analyzed based on its severity, exploitability, and potential impact. CVSS scores were used to prioritize findings and determine remediation urgency.

Exploitation Overview

Selected vulnerabilities were manually validated to confirm their real-world impact. Exploitation was performed in a controlled manner to avoid system instability.

Successful exploitation demonstrated that an attacker could gain unauthorized access, extract sensitive data, or execute commands remotely. These results confirmed that the identified vulnerabilities posed serious security risks.

Detection – OpenVAS Findings Log

Timestamp	Target IP	Vulnerability	Severity	CVSS
2026-01-05 12:05:00	192.168.0.9	SQL Injection	High	9.1
2026-01-05 12:10:00	192.168.0.9	Reflected XSS	Medium	6.1
2026-01-05 11:45:00	192.168.0.9	Outdated Apache	Medium	6.5

Risk Impact Analysis

If exploited in a production environment, the identified vulnerabilities could lead to:

- Unauthorized data access
- Compromise of system integrity
- Loss of confidentiality
- Service disruption

The combination of multiple vulnerabilities increases overall risk and highlights the importance of defense-in-depth security practices.

Remediation Recommendations

To mitigate the identified risks, the following actions are recommended:

- Apply the latest security patches to all systems
- Implement strong input validation and parameterized queries
- Disable unnecessary services and close unused ports
- Enforce strong authentication mechanisms
- Conduct regular vulnerability assessments

A follow-up OpenVAS scan is recommended after remediation to verify vulnerability resolution.

Developer Escalation Email

Hi Team,

During the recent Vulnerability Assessment and Penetration Testing (VAPT) exercise conducted on the test environment, we identified a few critical security vulnerabilities that require immediate attention.

Most notably, we were able to successfully exploit a SQL Injection vulnerability in the DVWA application and gain unauthorized access to backend data. In addition, outdated services and weak configurations were identified on the Metasploitable2 system, which could allow an attacker to gain remote access if left unpatched.

Proof of concept (PoC) was successfully demonstrated in a controlled lab setup to validate the impact of these issues. Screenshots and technical details have been documented in the attached report for reference.

We recommend prioritizing fixes such as input validation, patching outdated services, and disabling unnecessary services. Please let us know if any clarification or support is required from our side.

Regards,
Cinchana S
VAPT Intern
Cybersecurity Team

PTES Report

A full Vulnerability Assessment and Penetration Testing (VAPT) cycle was conducted on a vulnerable web application within a controlled lab environment, following the Penetration Testing Execution Standard (PTES). The assessment began with vulnerability identification using OpenVAS, which highlighted several web application security issues, including SQL Injection and Cross-Site Scripting.

During the exploitation phase, Burp Suite was used to intercept and manipulate HTTP requests, confirming improper input handling. The SQL Injection vulnerability was then exploited using sqlmap, allowing enumeration of databases and extraction of sensitive user credentials. This demonstrated how an attacker could bypass authentication controls and gain unauthorized access to critical data.

Post-exploitation activities focused on validating the impact of the vulnerabilities and collecting supporting evidence. The results showed that weak input validation and insecure coding practices significantly increased the application's attack surface.

To reduce risk, it is recommended to implement secure development practices, enforce least-privilege access, and conduct regular security assessments. This project highlights the importance of combining automated tools with manual testing to accurately assess application security.

Conclusion

This assessment provided practical exposure to the complete VAPT lifecycle. The exercise demonstrated how minor misconfigurations and outdated software can lead to severe security breaches.

By following proper security practices and performing regular assessments, organizations can significantly reduce their attack surface and protect critical assets.

Disclaimer

All activities documented in this report were performed in a controlled lab environment strictly for learning purposes. Unauthorized testing of real-world systems without permission is illegal and unethical.