Executive Summary

A comprehensive security assessment of the internal lab environment revealed critical vulnerabilities that allowed complete system compromise across multiple targets. The assessment demonstrated practical attack chains where web application flaws (Stored XSS) were leveraged to gain initial footholds, leading to privilege escalation and full control of affected servers. Multiple OWASP Top 10 vulnerabilities were successfully exploited, underscoring the need for immediate remediation.

Technical Findings

Critical Vulnerability Summary

Finding ID	Vulnerability	CVSS Score	Remediation
F001	Stored XSS → RCE Chain	9.1 (Critical)	**1.** Implement strict output encoding **2.** Set HttpOnly and Secure cookie flags **3.** Harden file upload functionality **4.** Regular security patching
F002	SQL Injection	9.1 (Critical)	**1.** Use parameterized prepared statements **2.** Enforce least privilege on DB accounts **3.** Implement WAF rules
F003	Reflected XSS	8.1 (High)	**1.** Context-aware output encoding **2.** Input validation on all user fields

Detailed Finding Description

F001 - Stored XSS to Remote Code Execution
A Stored Cross-Site Scripting vulnerability was identified in the Mutillidae application's guestbook functionality. This allowed persistent injection of malicious JavaScript that automatically harvested user session cookies. The compromised admin session was then used to upload a malicious PHP web shell, resulting in full remote code execution on the underlying Metasploitable2 server.
***Evidence:** Task 1 Report, Screenshots 01-09*

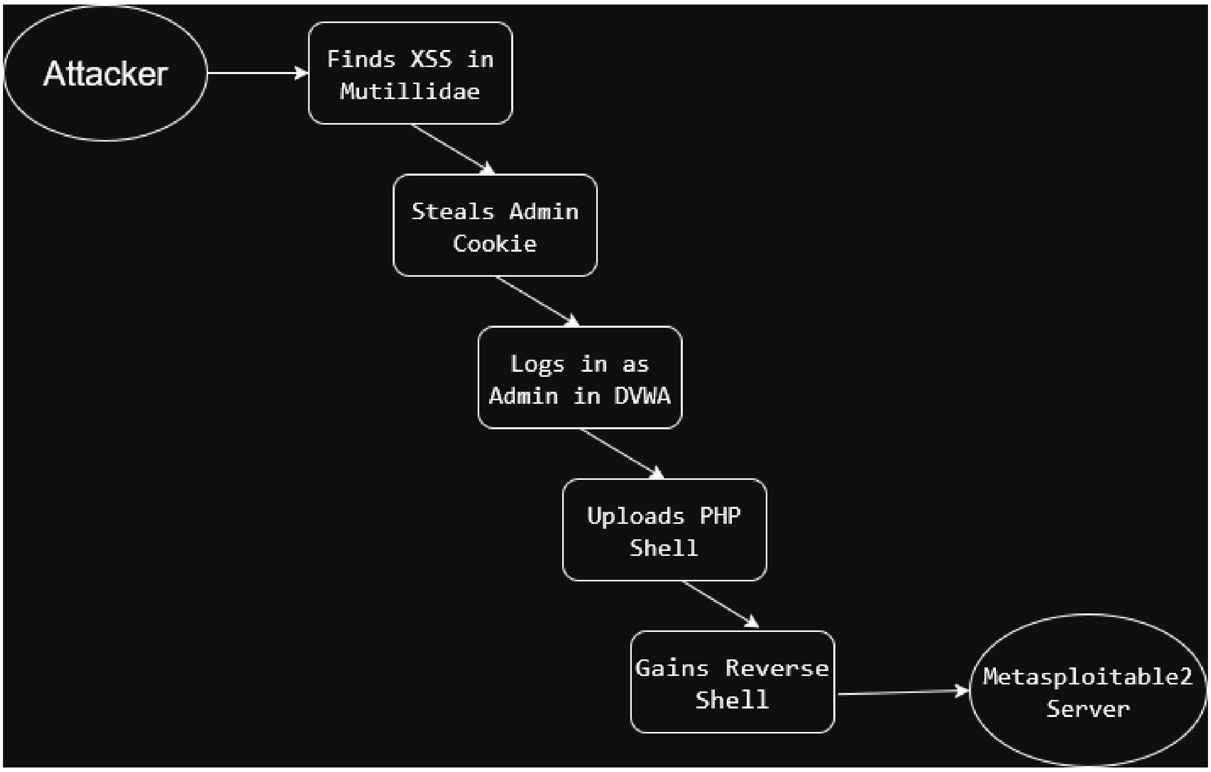
F002 - SQL Injection in DVWA
Automated testing with sqlmap confirmed a critical SQL Injection vulnerability in the DVWA

application's user input parameter. This allowed complete enumeration of database structures and extraction of all user credentials from the database, including administrator accounts.
***Evidence:** Task 2 Report, Screenshots 10-11*

F003 - Reflected Cross-Site Scripting
Manual testing confirmed Reflected XSS in DVWA's input fields, allowing execution of arbitrary JavaScript in victim browsers. This could be leveraged for session hijacking, credential theft, or client-side attacks.
***Evidence:** Task 2 Report, Screenshots 12-14*

Network Attack Path

The following diagram illustrates the attack chain used to compromise the Metasploitable2 server:



Remediation Plan

1. **Input Validation:** Implement server-side sanitization of all user-supplied input
2. **Secure Development Training:** Conduct OWASP Top 10 awareness training for developers
3. **Patch Management:** Establish regular security patching cycle for all frameworks

4. **Access Controls:** Implement principle of least privilege for all database and system accounts
5. **Monitoring:** Deploy WAF solutions and implement continuous security monitoring

Management Summary

Our security assessment revealed critical vulnerabilities that would allow attackers to steal all user passwords and gain complete control of our test systems. The most serious issue involved manipulating our web applications to execute malicious code, providing full access to our servers. We also confirmed that attacker could easily extract our entire user database. We have provided the technical team with a detailed remediation plan. Addressing these findings is essential to prevent data breaches and protect company systems from compromise. Immediate action is required to implement the recommended security controls.

Appendix A: Screenshot Evidence References

- Screenshots 01-09: Task 1 - Exploitation Chain
- Screenshots 10-11: Task 2 - SQL Injection Findings
- Screenshots 12-14: Task 2 - XSS Findings

Distribution List: Security Team, Development Lead, IT Management