Week 5: Vulnerability Assessment Findings

Abdullah Akram
ID: DHC-3606

Task 5: Ethical Hacking & Vulnerability Assessment

July 23, 2025

Cybersecurity Internship Report

Submitted as part of Week 5 deliverables

1 Objective

The goal of Week 5 was to conduct vulnerability assessments on a test PHP web application (home-rental) using ethical hacking tools such as SQLMap, Kali Linux, and Burp Suite to identify exploitable vulnerabilities and document findings for mitigation.

2 Tools Used

- **Kali Linux**: Penetration testing platform for network scanning and reconnaissance.
- **SQLMap**: Automated tool for detecting and exploiting SQL injection vulnerabilities.
- **Burp Suite**: Web vulnerability scanner for testing CSRF and session management.
- **Nmap**: Network exploration tool for port and service enumeration.

3 Findings

3.1 Reconnaissance with Nmap

- **Command**: `nmap -sV -p- localhost`
- **Result**: Identified open ports: 80 (Apache/2.4.41), 3306 (MySQL 5.7), and 22 (SSH). Apache and MySQL were critical for the web application.
- **Screenshot**: [Placeholder: Screenshot of Nmap output displaying open ports and services]

3.2 SQL Injection Testing with SQLMap

- **Command**: `sqlmap -u "http://localhost/home-rental/auth/login.php?username=test&`
  `--forms --dbs --batch`
- **Result**: No SQL injection vulnerabilities detected in login.php or register.php due to the use of PDO prepared statements. Advanced injection techniques (e.g., time-based, error-based) were also unsuccessful.
- **Screenshot**: [Placeholder: Screenshot of SQLMap output confirming no injectable parameters]

3.3 CSRF Vulnerability Testing

- **Tool**: Burp Suite
- **Process**: Intercepted form submissions for login.php and register.php. Initial tests revealed the absence of CSRF tokens, making forms vulnerable to unauthorized submissions.
- **Screenshot**: [Placeholder: Screenshot of Burp Suite intercept showing form submission without CSRF token]

4 Conclusion

The vulnerability assessment identified open ports and services using Nmap, confirmed SQL injection resistance due to prepared statements, and detected CSRF vulnerabilities in form submissions. These findings informed mitigation strategies implemented in Task 5 Report.