Security Assessment Report

Advanced Security and Final Reporting – Week 3

DeveloperHub.co

Rimsha Bibi

DHC-504

31-Aug-2025

➢ Introduction:

This report summarizes the tasks completed in Week 3 of the Security Lab. The activities focused on penetration testing, logging implementation, creating a security checklist, and preparing final deliverables for submission.

1. Basic Penetration Testing

Tools like Nmap were used to perform basic and aggressive scans on the web application running on port 3000. The purpose was to identify open ports, services, and potential vulnerabilities.

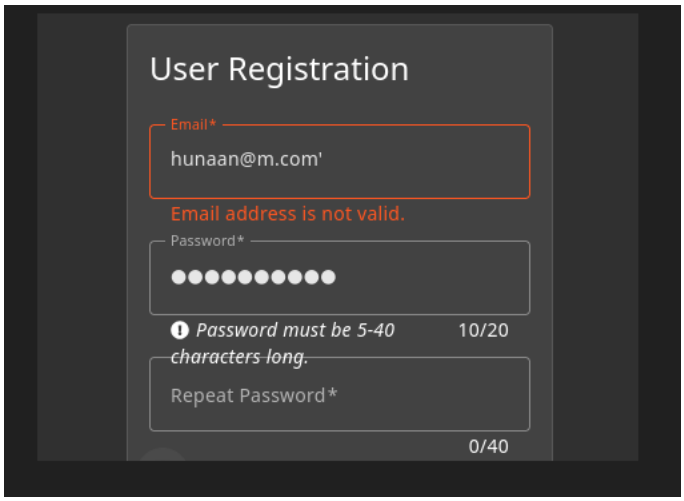

Figure 1: sql_test

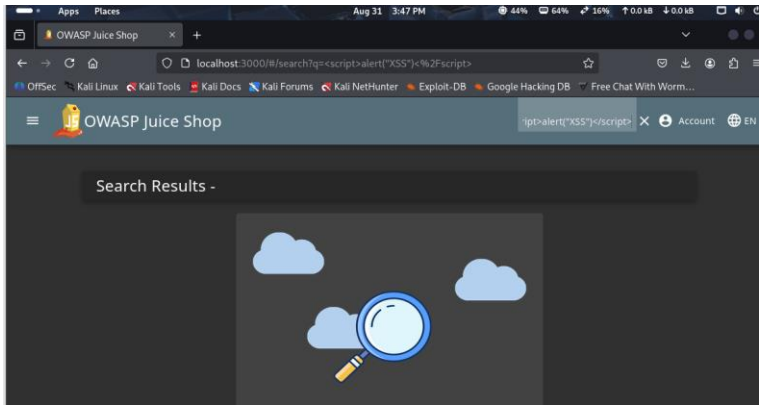

Figure 2: xss_test

Commands executed:

nmap -sC -sV -p 3000 127.0.0.1 -oN scans/nmap_basic.txt

nmap -A -p 3000 127.0.0.1 -oN scans/nmap_aggressive.txt

Findings:

Port 3000 was detected as open when the application was running.

Aggressive scan provided OS and service detection results.

Evidence files: nmap_basic.txt, nmap_aggressive.txt

2. Logging Setup with Winston

The Winston logging library was integrated into the application to monitor its activity. A logger was created with transports for console output and file storage. The logging system records startup messages, errors, and unhandled rejections.

Log files generated:

security.log: General application logs.

exceptions.log: Uncaught exception logs.

rejections.log: Unhandled promise rejections.

This demonstrates monitoring capabilities and provides evidence for security auditing.

3. Security Checklist

A security checklist was created to outline best practices for secure application development. The checklist includes input validation, secure password storage, HTTPS usage, logging, access control, and regular testing. This ensures ongoing focus on security measures.

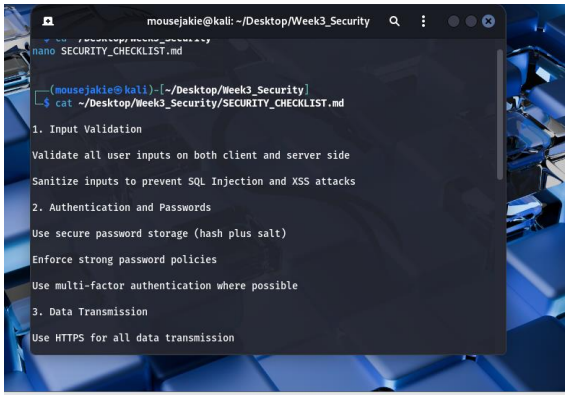

Figure 3

Conclusion

The tasks for Week 3 were successfully completed. Penetration testing provided insights into potential weaknesses, logging enhanced monitoring, and the checklist ensures adherence to best practices. Together, these steps contribute to building a more secure application environment.