Week 6: Security Audit Findings

Abdullah Akram
ID: DHC-3606

Task 6: Advanced Security Audits & Deployment

July 23, 2025

Cybersecurity Internship Report

Submitted as part of Week 6 deliverables

1 Objective

The objective was to perform advanced security audits on the home-rental web application using OWASP ZAP, Nikto, and Lynis to identify vulnerabilities, ensure compliance with OWASP Top 10 standards, and prepare for secure deployment.

2 Tools Used

- **OWASP ZAP**: Dynamic application security testing for XSS and other web vulnerabilities.
- **Nikto**: Web server scanner for configuration issues and vulnerabilities.
- **Lynis**: System auditing tool for server security compliance.
- **Burp Suite**: Penetration testing for session management and form submissions.

3 Findings

3.1 OWASP ZAP Scan

- **Command**: Scanned `http://localhost/home-rental`
- **Result**: Detected missing anti-clickjacking headers (X-Frame-Options) and potential XSS vulnerabilities in unsanitized form inputs.
- **Screenshot**: [Placeholder: Screenshot of OWASP ZAP report highlighting XSS alerts]

3.2 Nikto Scan

- **Command**: `nikto -h http://localhost/home-rental`
- **Result**: Identified outdated server headers (Apache/2.4.41) and directory indexing enabled in the web server configuration.
- **Screenshot**: [Placeholder: Screenshot of Nikto output showing server misconfigurations]

3.3 Lynis System Audit

- **Command**: `lynis audit system`
- **Result**: Found weak file permissions on configuration files (e.g., /etc/apache2) and recommended enabling AppArmor for enhanced server security.
- **Screenshot**: [Placeholder: Screenshot of Lynis output showing permission warnings]

3.4 Burp Suite Testing

- **Process**: Intercepted login and registration form submissions to verify CSRF token implementation and session management.
- **Result**: Confirmed CSRF tokens are secure. Identified session fixation risk due to lack of session ID regeneration.
- **Screenshot**: [Placeholder: Screenshot of Burp Suite showing secure form submission]

4 Conclusion

The audits revealed missing security headers, potential XSS vulnerabilities, weak file permissions, and session fixation risks. These findings were addressed through code and server configuration changes documented in the Task 6 Report.