Week 6: Security Implementation Report

Abdullah Akram
ID: DHC-3606

Task 6: Advanced Security Audits & Final Deployment

July 23, 2025

Cybersecurity Internship Report

Submitted as part of Week 6 deliverables

1 Objective

The objective was to conduct advanced security audits, implement security headers, patch vulnerabilities identified by OWASP ZAP, Nikto, and Lynis, and prepare the home-rental PHP web application for secure deployment.

2 Tools Used

- **OWASP ZAP**: For dynamic security testing and XSS detection.
- **Nikto**: For web server vulnerability scanning.
- **Lynis**: For system security auditing and compliance checks.
- **Burp Suite**: For penetration testing and session management validation.

3 Process

1. **Audit**: Conducted scans using OWASP ZAP, Nikto, and Lynis to identify vulnerabilities.
2. **Penetration Testing**: Used Burp Suite to verify form submissions and session security.
3. **Security Fixes**: Implemented security headers, input sanitization, session regeneration, and file permission adjustments.
4. **Deployment Prep**: Configured secure error handling and verified dependencies.

4 Code Implementation

4.1 Security Headers (login.php)

- **Action**: Added HTTP security headers to mitigate XSS, clickjacking, and MIME-type attacks.
- **Code**:

```
<?php
header("X-Frame-Options: DENY");
header("Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'");
header("X-Content-Type-Options: nosniff");
header("Strict-Transport-Security: max-age=31536000; includeSubDomains");
header("X-XSS-Protection: 1; mode=block");
require_once 'config.php';
?>
```