**Internship Task:** Final Security Audit & Deployment Hardening

**Intern Name:** Rabia Khawaja  
**Date:** 23th April 2025

### Week 6: Advanced Security Audits & Final Deployment Security

**Goal:**  
Perform security audits, ensure compliance with security standards, and prepare the application for secure deployment.

### Task 1: Security Audits & Compliance

#### What We Did:

**OWASP ZAP:**

Intercepted traffic by setting browser proxy to ZAP.

Ran Active Scan on local Node.js app.

Identified potential XSS and cookie misconfigurations.

Generated and saved full vulnerability report.

**Nikto:**

Command used: nikto -h http://127.0.0.1:3000

Detected outdated headers and server info leakage.

**Lynis:**

Installed and executed: sudo lynis audit system

Provided insights into missing firewall rules and unused services.

**OWASP Top 10 Check:**

Mapped detected issues from ZAP and Nikto to Top 10 risks.

Applied fixes to mitigate Injection, Security Misconfiguration, and Broken Authentication risks.

### 🐳 Task 2: Secure Deployment Practices

#### What We Did:

**Automatic Security Updates:**

Enabled using unattended-upgrades on Ubuntu system.

**Dependency Scanning:**

Ran npm audit fix to automatically resolve vulnerabilities.

Followed by manual resolution of high-risk packages.

**Docker Image Hardening:**

Scanned Docker image using: docker scan <image-name>

Updated base image to node:slim

Ensured app runs with non-root user.

Created .dockerignore to reduce build context size.

### Task 3: Final Penetration Testing

#### What We Did:

**Burp Suite:**

Intercepted and modified login and form submissions.

Attempted CSRF and XSS payloads.

Verified CSRF protection with invalid token tests

**Metasploit:**

Opened msfconsole, scanned for vulnerabilities.

Simulated attacks relevant to Node.js platform.

#### Findings:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability** | **Tool Used** | **Risk Level** | **Fix Applied** |
| XSS in login form | Burp Suite | Medium | Input sanitization + CSP |
| Missing HTTPOnly flags | OWASP ZAP | Medium | Secure cookie configuration |
| CSRF Token Bypass | Burp Suite | High | Implemented csurf middleware |

### Summary:

Completed comprehensive audits with 3 industry tools.

Mapped and fixed OWASP Top 10 vulnerabilities.

Hardened server and Docker container.

Performed full penetration testing.

Documented findings and applied remediations.

**System is now ready for secure deployment.**