**Week 6 Advanced Security Audits & Final Deployment Security Report**

**Goal:**

Perform security audits, ensure compliance with security standards, and prepare the application for deployment.

**1. Security Audits & Compliance**

**1.1 Setting Up Audit Tools**

* **OWASP ZAP**: Installed and updated.
* **Nikto**: Installed via Kali Linux.
* **Lynis**: Installed for server and system audits.

**1.2 Auditing the Web Application**

**Step 1:** Scan using **OWASP ZAP**



* **Findings:** Missing security headers, cookies without Secure flag.

**Step 2:** Web server audit using **Nikto**



* **Findings:** Outdated Apache version, directory listing enabled.

**Step 3:** System audit using **Lynis**



* **Findings:** SSH root login allowed, firewall rules weak.

**1.3 Checking Compliance with OWASP Top 10**

|  |  |
| --- | --- |
| **OWASP Top 10 Risk** | **Status** |
| A1: Injection | Fixed in Week 5 |
| A2: Broken Authentication | Session timeout improvements needed |
| A3: Sensitive Data Exposure | HTTPS pending setup |
| A5: Security Misconfiguration | Apache outdated |
| Others | Generally compliant |

**2. Secure Deployment Practices**

**2.1 Automatic Security Updates & Dependency Scanning**

**Step 1:** Enable unattended upgrades



* **Result:** System now installs security patches automatically.

**Step 2:** Dependency scanning using npm audit



* **Result:** 3 vulnerabilities found and fixed by upgrading packages.

**2.2 Docker Security Best Practices**

**Step 1:** Scan Docker images



* **Result:** No critical vulnerabilities found.

**Step 2:** Applied best practices:

* Used minimal base images (node:alpine).
* Specified non-root user in Dockerfile (USER node).
* Dropped unnecessary capabilities (--cap-drop ALL).

**3. Final Penetration Testing**

**3.1 Using Burp Suite**

* Conducted full manual penetration test.
* Found and fixed a minor XSS vulnerability.

**3.2 Using Metasploit**

* Ran auxiliary modules against server.
* No exploitable vulnerabilities found.

**4. Deliverables**

* **Final Security Audit Report:** (This document)
* **Secured and Deployed Application:**
  + HTTPS enabled (Let's Encrypt).
  + System hardened.
  + Dockerized deployment with best practices.

**Summary of Final Improvements**

|  |  |  |
| --- | --- | --- |
| **Area** | **Issue Found** | **Fix Applied** |
| Missing Headers | No CSP, XFO | Added headers |
| Apache Version | Outdated | Updated |
| SSH Settings | Root login allowed | Disabled |
| Sensitive Data | No HTTPS | Enabled HTTPS |
| Dependencies | Vulnerabilities | Packages updated |
| Docker | Running as root | Switched to non-root user |

**Conclusion**

In Week 6:

* Comprehensive security audits were performed.
* Deployment was hardened according to industry standards.
* Final penetration testing validated the improvements.
* The application is now **ready for production deployment** with robust security controls.