# Week 6 Explanation Report

## Advanced Security Audits & Final Deployment Security

## Objective

The goal for Week 6 was to conduct thorough security audits, ensure the application complies with security standards, and apply secure deployment practices to prepare the web application for final release.

## Tasks Performed

### 1. Security Audits & Compliance

Action Taken:

* Performed a full security scan of the web application using OWASP ZAP, Nikto, and Lynis.
* Checked the application for vulnerabilities based on the OWASP Top 10 list.
* Identified issues such as missing security headers, outdated dependencies, and minor input validation weaknesses.

Result:

* Discovered and resolved several medium-priority security issues.
* Ensured compliance with standard security best practices.

### 2. Secure Deployment Practices

Action Taken:

* Enabled automatic security updates on the server.
* Implemented dependency scanning tools like npm audit and GitHub Dependabot alerts.
* Applied Docker security best practices by scanning images for vulnerabilities before deployment using tools like Trivy.

Result:

* Improved application and server resilience against known vulnerabilities.
* Reduced the risk of deploying vulnerable container images.

### 3. Final Penetration Testing

Action Taken:

* Conducted a final penetration test using Burp Suite and Metasploit.
* Tested for vulnerabilities including SQL Injection, XSS, CSRF, Insecure Direct Object References (IDOR), and more.  
  - Documented findings and applied any last-minute patches.

Result:

* Verified that the application was hardened against a wide range of known attacks.
* Ensured secure and robust final deployment.

## Deliverables Submitted

|  |  |  |
| --- | --- | --- |
| Deliverable | Status | Notes |
| Final security audit report | Done | Findings from ZAP, Nikto, and manual penetration testing |
| Secured and deployed application | Done | Dockerized app with updated images and best practices |
| GitHub repository updated with security fixes | Done | All patches committed |
| Recorded project video with explanation | Done | Video length 4-5 minutes with full demonstration |

## Summary of Tools & Techniques Used

* OWASP ZAP — Web application vulnerability scanner
* Nikto — Web server vulnerability scanner
* Lynis — Linux system audit tool
* Burp Suite — Advanced penetration testing
* Metasploit — Vulnerability exploitation framework
* Trivy — Docker image vulnerability scanner
* GitHub Dependabot — Dependency vulnerability management

## Conclusion

By the end of Week 6, a full security lifecycle had been completed for the web application, including auditing, vulnerability fixing, and secure deployment practices. The project now follows industry-standard security guidelines, ensuring a safe experience for users.

## Attachments

GitHub Repository: <https://github.com/Mayra-Ahmer/week6-Advanced-Security-Audits-Final-Deployment-Security>