🔒 Final Security Audit Report

Cybersecurity Internship – Week 6

Auditor: Rida Mudassar - DHC 377

Application URL: http://localhost:3000

Scan Tool Used: OWASP ZAP

Date of Audit: July 2025

📝 Executive Summary:

A comprehensive security audit was performed using OWASP ZAP on the local application running at `http://localhost:3000`. The scan revealed several security issues, ranging from missing headers to cross-domain misconfigurations. This report summarizes the vulnerabilities found and recommends appropriate mitigations to secure the application.

🗒️ Summary of Findings:

Vulnerability	Risk Level	Instances
Content Security Policy Header Not Set	Medium	13
Cross-Domain Misconfiguration	Medium	28
Hidden Files Found	Low	4
Cross-Domain JavaScript Source File Inclusion	Medium	6
Timestamp Disclosure - Unix	Low	20
Information Disclosure - Suspicious Comments	Low	2
Modern Web Application (informational)	Info	4
User Agent Fuzzer	Info	24

Recommendations & Final Notes:

- Implement all suggested headers such as CSP, HSTS, X-Content-Type-Options.
- Use security linters and scanners in your CI/CD pipeline.
- Conduct regular penetration tests after each major deployment.
- Update dependencies frequently and monitor for CVEs.