SAMEER SHAHZAD

DHC-1666

CYBERSECURITY INTERNSHIP TASK 2

Final Security Audit & Penetration Testing Report

1. Executive Summary

This report details the security measures, audits, and penetration testing conducted for the Web API project during Weeks 4–6 of the Cybersecurity Internship. The objective was to identify vulnerabilities, implement fixes, and verify the application's security posture using industry-standard tools. **Final testing confirms that all identified risks have been mitigated, and no critical issues remain.**

2. Security Implementation (Week 4)

To harden the API against common threats, the following defenses were implemented:

- **Intrusion Detection: Fail2Ban** was configured to monitor system logs. It successfully detects and bans IP addresses after 5 failed login attempts.
- **Brute-Force Protection: Rate-limiting** was applied using `express-rate-limit`, restricting users to 100 requests per 15 minutes.
- **Security Headers: Helmet.js** was used to enforce **HSTS** (HTTPS) and prevent clickjacking.
- **CSP:** A strict **Content Security Policy** was implemented to block unauthorized scripts and prevent XSS.

3. Ethical Hacking & Exploitation (Week 5)

We used the "Attacker's Mindset" to find and fix vulnerabilities.

- **Reconnaissance:** Performed using **Nmap** and **Nikto**. No unnecessary open ports or sensitive server signatures were found.
- **SQL Injection (SQLi) Test:** Tested with **SQLMap**.
  - *Result:* Initially, a vulnerability was found.
  - *Fix:* Applied **Prepared Statements**.
  - *Re-test:* **SQLMap now returns "Target is not vulnerable."**
- **CSRF Testing:** Tested using **Burp Suite**.
  - *Fix:* Integrated csurf middleware.
  - *Result:* Unauthorized requests are now successfully blocked with a 403 forbidden error.

4. Advanced Audits & Compliance (Week 6)

A final audit was conducted to ensure compliance with **OWASP Top 10** standards.

A. OWASP ZAP Audit

- **Method:** Automated active and passive scanning.
- **Result:** No "High" or "Medium" risk vulnerabilities detected. Minor "Informational" flags were addressed.

B. Nikto Scan

- **Method:** Web server vulnerability scanning.
- **Result:** No outdated server modules or dangerous files were discovered.

C. Lynis Security Audit

- **Method:** System-level security audit.
- **Result:** The host system shows a high security index, with automatic updates enabled.

5. Final Penetration Test Results

Using **Metasploit** and **Burp Suite Professional**, a final manual penetration test was performed.

- **Authentication Bypass:** Attempted and **Failed**.

- **Sensitive Data Exposure:** Checked logs and headers; all data is encrypted and secure.
- **Dependency Scanning:** Used npm audit.
    - *Result:* **"0 vulnerabilities found."**

6. Conclusion

The application has undergone rigorous testing and auditing. All security layers, from the code level (Prepared Statements, CSRF tokens) to the server level (Fail2Ban, Rate Limiting), are functioning correctly. **The application is verified as secure and ready for deployment.**