Cybersecurity Internship Final Report – Fatima Muhammad

Week 1: Vulnerability Assessment

During Week 1 of the internship at Developers Hub Corporation, I focused on identifying and understanding various vulnerabilities in a web application by using OWASP Juice Shop. I set up the environment using Docker, explored its exposed features, and tested the following:

- **Reflected XSS**: Injected JavaScript via the search bar and confirmed script execution.
- **SQL Injection**: Performed login bypass using `' OR 1=1--` and accessed the admin account.
- **Misconfigurations**: Analyzed HTTP headers for missing security directives.
- **Admin Login Challenge**: Bypassed authentication and captured the server log response.

This week provided foundational experience with real-world vulnerabilities and their potential impact.

Week 2: Secure Coding and Fix Implementation

The second week was focused on implementing defenses against vulnerabilities identified in Week 1. Using Node.js and the Juice Shop environment, the following fixes were applied:

- **Input Validation**: Implemented validation using `validator.js` to check email and password formats.
- **Password Security**: Used `bcrypt` to hash and salt user passwords before storing them.
- **JWT Authentication**: Integrated `jsonwebtoken` to simulate secure token-based authentication.
- **Secure Data Transmission**: Reviewed secure headers (`X-Content-Type-Options`, `X-Frame-Options`) and discussed the importance of HTTPS/TLS for real-world deployments.

These implementations enhanced the app's security posture and helped me understand core backend protection techniques.

Week 3: Advanced Security and Reporting

Week 3 involved simulating attacks, logging security events, and preparing final documentation:

- **Penetration Testing**: Used `nmap` to scan localhost and Juice Shop port 3000, confirming open service exposure.
- **Logging**: Configured `winston` to log security-related actions and simulate real-time monitoring of login attempts.
- **Checklist**: Created a security checklist covering input validation, hashed passwords, JWT, logging, and known vulnerability testing.
- **Final Reporting**: This document, security log, and checklist were prepared for submission. A video recording was also planned to explain each implemented fix and how Juice Shop vulnerabilities were discovered and mitigated.

Tools and Technologies Used

- Kali Linux (Virtual Machine)
- Docker and Node.js
- OWASP Juice Shop
- Nmap (Network scanning)
- Validator.js (Input validation)
- Bcrypt (Password hashing)
- JSON Web Token (Authentication)
- Winston (Logging)

Challenges and Learnings

- Locating and modifying source code in Juice Shop's auto-generated build was complex. This required creative workarounds using custom routes.

- Integrating validation, hashing, and JWT was valuable in learning real-world backend protection.
- Setting up and using tools like Nmap and Winston helped me understand how attackers think and how defenders must monitor and secure their applications.
- This internship enhanced my practical cybersecurity skills and confidence in identifying and remediating vulnerabilities.