Cybersecurity Internship – Week 2 Report

Introduction

This report outlines the activities and tasks completed during the second week of the cybersecurity internship at Developers Hub Corporation. The primary objective of this week was to enhance the security of user authentication mechanisms by implementing modern validation, password encryption, token-based authentication, and secure data transmission techniques using OWASP Juice Shop.

1. Input Validation using Validator.js

To prevent invalid or malicious input during user authentication, input validation was implemented using the `validator` npm package. A custom validation function was created to check for correct email formatting and adequate password length. Although Juice Shop's structure made it difficult to attach this logic directly to the original login handler, the concept was validated through a test route that simulated input validation logic.

2. Secure Password Storage using Bcrypt

Password hashing was implemented using the `bcrypt` package to ensure that raw passwords are never stored or processed in plaintext. The logic was added to the `/api/Users` registration route, replacing plain passwords with securely hashed versions using `bcrypt.hash()`. This ensures that user credentials are resilient to database leaks or server breaches.

3. Token-Based Authentication using JWT

JWT (JSON Web Token) authentication was introduced to replace traditional session-based login mechanisms. While Juice Shop's internal login routing limited direct integration, the `jwt.sign()` function was demonstrated via a custom route that issued

a time-limited token upon simulated login. This helped develop a clear understanding of how JWT tokens are structured, signed, and used to protect API routes.

4. Secure Data Transmission

Secure data transmission is critical in protecting sensitive user information in transit. While HTTPS could not be configured in the local Juice Shop instance, the application was reviewed for secure header configurations. Headers such as `X-Content-Type-Options`, `X-Frame-Options`, and `Access-Control-Allow-Origin` were examined to verify secure defaults. The importance of HTTPS and TLS in ensuring confidentiality and integrity of transmitted data was studied and documented.

Conclusion

Week 2 focused on strengthening backend authentication processes and secure data handling practices, incorporating secure programming techniques that are essential for modern web applications. Despite architectural restrictions within Juice Shop, each security concept was implemented and validated in isolation, providing hands-on experience with input validation, password encryption, token-based authentication, and secure data transmission.