Task 1 – Web Application Security Testing

This repository documents the work completed as part of Task 1 of my Cyber Security Internship. The main objective of this task was to understand how real-world web applications are tested for security vulnerabilities and how weaknesses in application design can lead to serious security risks. The project focuses on identifying common web-based attacks using both manual and automated testing techniques.

The target application selected for this task was OWASP Juice Shop, which is a deliberately vulnerable web application designed for learning web security. The testing process involved identifying input validation flaws, authentication weaknesses, and missing security controls using standard penetration testing tools available in Kali Linux.

During the assessment, multiple high-risk and medium-risk vulnerabilities were discovered, including SQL Injection, Cross-Site Scripting (XSS), Broken Authentication mechanisms, and missing security headers. These vulnerabilities were verified through practical exploitation techniques and documented using screenshots and scanner reports as evidence.

This project helped me gain hands-on experience in real-world security testing methodologies and improved my understanding of how attackers exploit insecure applications and how developers can mitigate such risks by adopting secure coding practices and security-by-design approaches.

Author: Cyber Security Intern