Alexandria National University
CYBER SECURITY ENGINEERING

Cyber Security Project

Name : Ahmed Mohamed Ahmed Attia ID : 2305079
Name : Mohamed Gaber ID : 2305056
Name : Youssef Mohamed Yaser ID 2305038

Web Penetration Testing Report: OWASP Juice Shop

Executive Summary

The purpose of this test is to identify and understand vulnerabilities within the OWASP Juice Shop application. Key findings include critical vulnerabilities such as SQL injection, XSS, and lack of rate-limiting. Recommendations include implementing input sanitization, rate-limiting mechanisms, and secure password policies.

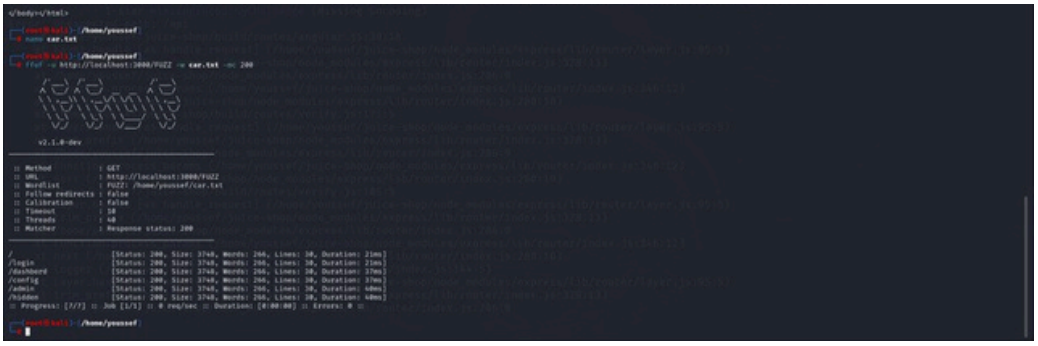
Scope and Methodology

Scope: This assessment tested the OWASP Juice Shop application, its APIs, and exposed endpoints.Methodology: The testing followed a black-box approach.Tools Used: The following tools were used - Hydra, Burp Suite, Gobuster, OWASP ZAP.

Vulnerability Findings

1. Enumeration to Find Admin Path

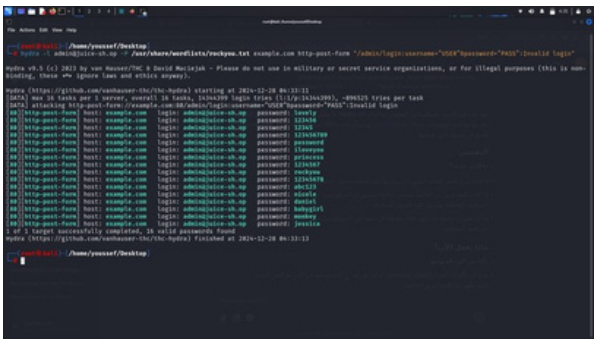
Description: The attacker discovers hidden admin paths by analyzing URL structures or using tools like FFUF (Fuzz Faster U Fool) is a fast web fuzzing tool used to discover hidden directories and endpoints on web applications.

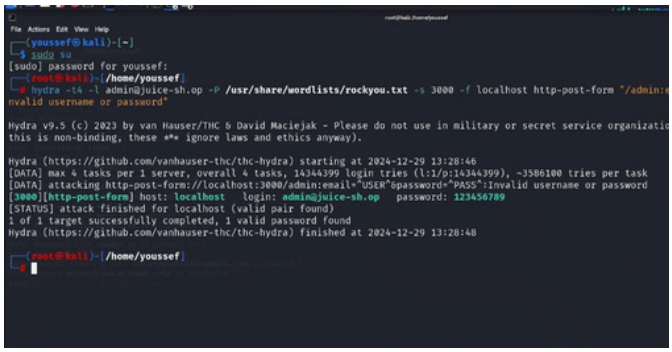


.Remediation: Obfuscate sensitive URLs and implement robust authentication for admin functionalities.

2. Brute Force on Admin Credentials

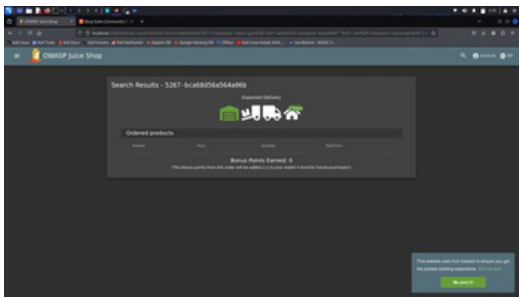
Description: A brute-force tool (e.g., Hydra) is used to guess the admin password due to lack of rate-limiting.Risk: Critical. Successful login grants full control over the application.Implement rate-limiting and account lockout mechanisms.

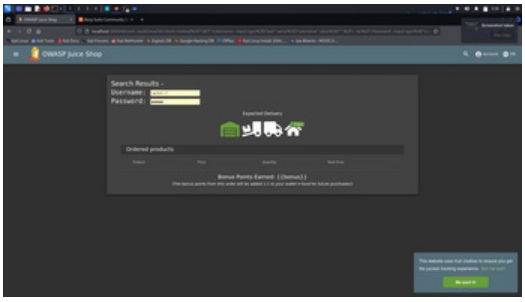




3. XSS in Product Search

Description: Malicious scripts are input into the product search bar, executing in the victim's browser.Risk: High. Enables session theft, redirection, or malicious activities.



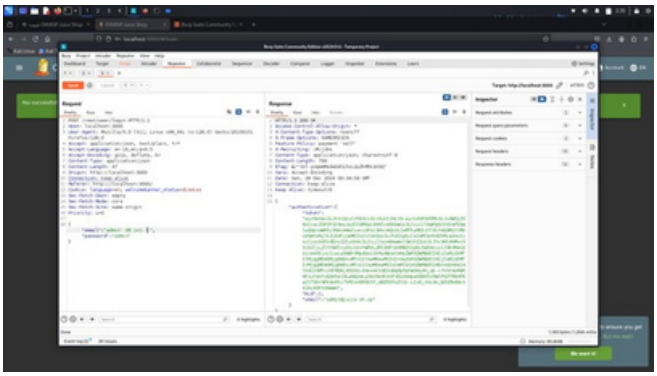


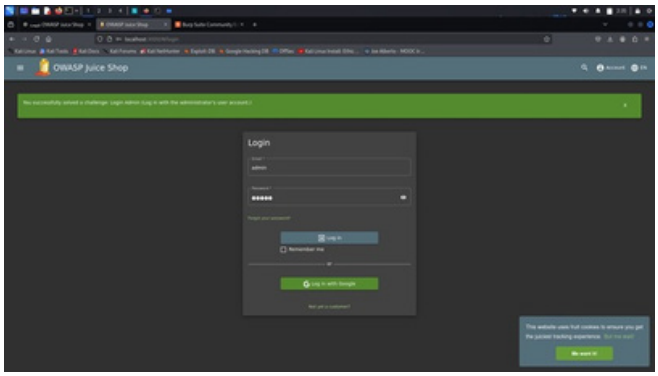
Remediation: Sanitize user inputs and encode outputs.

4. Bonus Questions

1. SQL injection

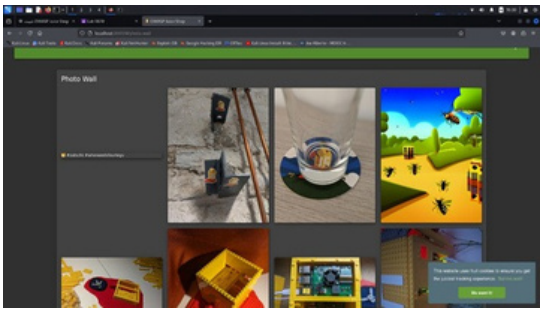
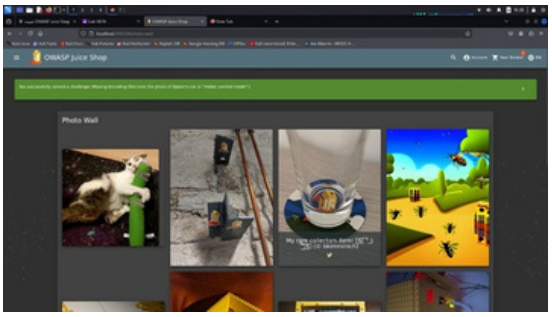
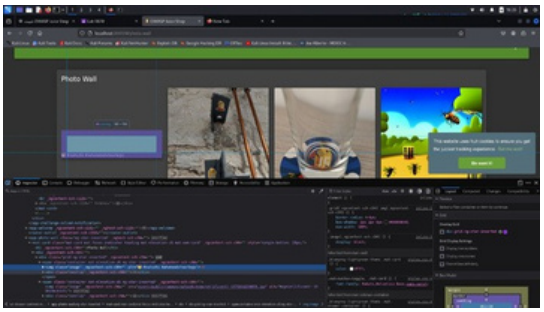
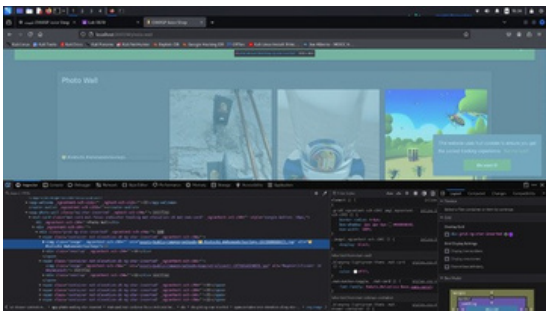
Description: SQL Injection is a cyber attack where malicious SQL statements are injected into input fields to manipulate or access a database. It allows attackers to retrieve, modify, or delete sensitive data without authorization





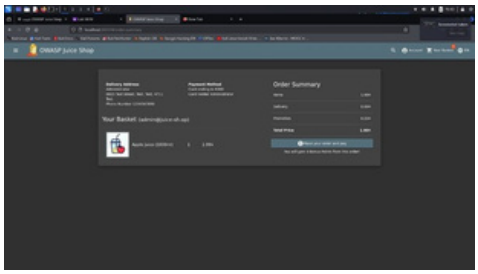
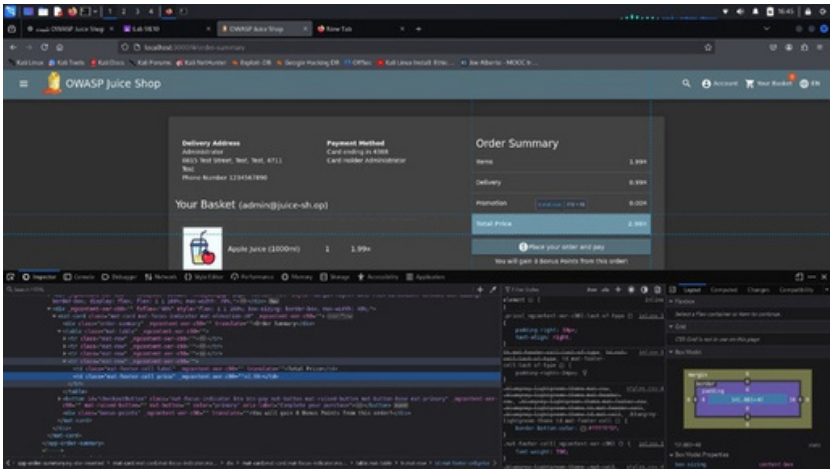
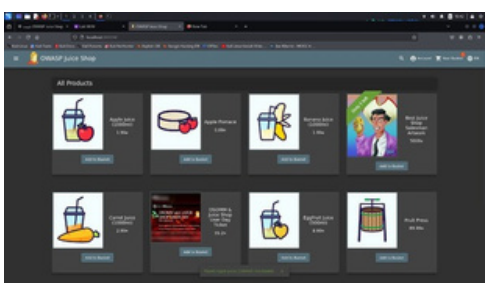
2 . missing logout fuctionallity

Description: Missing Logout Functionality: Verify if the application properly terminates the user session upon logout. Ensure no session tokens remain active after logging out.

3 . overpriced product challenge

Description: Test for vulnerabilities in product pricing mechanisms.

Commands

fuf toll command :	**ffuf -u http://localhost:3000/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 50 -mc 200**
HYADRA TOLL: command	**hydra -l Admin@juice-sh.op -p /usr/share/wordlists/rockyou.txt -s 3000 -f localhost http-post-form "/admin:email =^USER^&password=^PASS^:I**