Project cybersecurity Report

Team Members:

- Radwa Amr Ahmed 2305058
- Jana Adel Maher 2305046

Objectives

- Finding Admin Path
- Finding password for user Admin
- Find XSS in

Description

- project about attacking Owasp juice to exploite vulnerabilities. The owasp juice shop is already designed with vulnerabilities to attack using tools like “burp suite , zap”. Firstly browsing the application to discover hidden paths by guessing or analyzing the url structure then use ZAP to guess the password then get the reflection input to user without sanitization executing the script the victim browser

Vulnerabilities found

- **allowing brute force attacks “absence of rate limiting”**
- **lack of access control in admin**
- **XSS in search input**

Exploitation of these vulnerabilities can result in unauthorized access.

Scope and Methodology

Scope: Testing OWASP juice web application including API’s and key user workflows.

Testing Approach:

1. **Type: Black-box Testing**
2. **Tools: ZAP**

Next Steps:

1. **fix identified vulnerabilities.**
2. **train developers on secure coding practices.**

Vulnerability Findings

1.Finding Admin Path:

- **Description:** application lacks access control exposing admin paths through URL guessing .
- **Risk:** enable attacker to get unauthorized access.
- **Remediation:** implement obfuscation for admin paths.

2.Brute Force on Admin Credentials:

- **Description:** attackers can brute force admin credentials due to the absence of rate-limiting.
- **Risk:** attacker can have full control over the application.
- **Remediation:** Add rate-limiting and account lockouts.

3.XSS in Search input:

- **Description :** Malicious scripts can be executed via unsanitized inputs in the product search.
- **Risk:** Results in theft of sensitive data and session hijacking.
- **Remediation:** use input sanitization and output encoding.

- **Summary:**

The project focuses on exploiting the vulnerabilities in OWASP juice application, we aim to find the admin path,retrieve the admin password, and identify XSS vulnerabilities using tools like Burp Suite and ZAP. The project involves browsing the application to discover hidden paths and executing scripts , tools used to exploit vulnerabilities in the OWASP Juice Shop are Burp Suite and ZAP (Zed Attack Proxy). These tools assist in discovering hidden paths, guessing passwords, and identifying XSS vulnerabilities.

Videos Link:
https://drive.google.com/drive/folders/1f1rqyT6jMsCrow1XVrsRTsKuz25EAmPq?usp=drive_link