OWASP Juice Simulated Attack

Introduction

Attacking the OWASP Juice Shop involves exploiting common vulnerabilities to understand web application weaknesses and how attackers exploit them. The Juice Shop is intentionally designed with security flaws, making it an excellent platform for learning penetration testing.

Objectives

Participants will perform attacks against the OWASP Juice Shop to:

- Learn and apply penetration testing techniques.
- Understand the root causes of common web vulnerabilities.
- Document findings and create a video report demonstrating the attacks and their impacts.

Deliverables

Video Report: A 10-15 minute video detailing the attack scenarios, methodology, and outcomes with narration from the THREE team members. Each team member should explain their contribution in the video. The video shall be directly attached to the submission.

GitHub Repository: A repository containing:

- A detailed report of the attack scenarios which contains the following:

Web Penetration Testing Report:

Executive Summary

- Purpose of the test and brief overview of key findings.
- High-level impact and critical vulnerabilities.
- Summary of recommendations.

Scope and Methodology

- Scope: Websites, APIs, and applications tested.
- Approach: Black-box, grey-box, or white-box testing.
- Tools Used: List of tools (e.g., Burp Suite, OWASP ZAP).

Vulnerability Findings

- **Critical Vulnerabilities**:
    1. Description, risk, and potential impact (e.g., SQL injection, XSS).
    2. Evidence: Screenshots, logs, or proof of concept.
    3. Remediation steps: Specific actions to fix each vulnerability.

Exploitation and Attack Simulation

- Tools and techniques used for exploitation.
- Outcome and impact of the attack.

Conclusion

- Summary of security posture based on findings.
- Overall risk level and next steps for remediation.

Team Composition

- Each team will consist of 2 to 3 members s registered in this romr.

Attack Scenarios:

---

1. Enumeration to Find Admin Path

- **Scenario**: An attacker browses the application and discovers hidden paths by guessing or analyzing the URL structure.
- **Outcome**: The attacker discovers the admin functionality, which can be used for further exploitation.

---

2. Brute Force on Admin Credentials

- **Scenario**: After discovering the admin login page, the attacker uses a brute-force tool like Hydra with a valid email (`admin@juice-sh.op`) to guess the password. The lack of rate-limiting or account lockouts allows the attacker to successfully guess the password.
- **Outcome**: The attacker gains admin access, allowing full control over the application.

---

3. XSS in Product Search

- **Scenario**: The attacker inputs a malicious script into the product search bar. The application reflects this input back to the user without sanitization, executing the script in the victim's browser.
- **Outcome**: The attacker can execute arbitrary JavaScript, potentially stealing session cookies, redirecting users, or performing other malicious actions.

—

Resources

- OWASP Juice Shop Website
- Kali Linux
- Tools: Hydra, Burp Suite, Gobuster, OWASP ZAP, Dirb