WEB APPLICATION PENTRATION TESTING

TARGET: OWASP JUICE SHOP

OUR TEAM

Mohammed Usama

Mohamed Essam

Fares Ahmed

Mahmoud Emara

AGENDA

Introduction

Methodology

Key Vulnerabilities Identified

Tools

Remediation Recommendations

INTODUCTION

1. What is Our Tack?
2. Hacker Vs Pentration Tester
3. Project Intorduction

OWASP JUICE SHOP

1 **Introduction to OWASP Juice Shop**

Introduction to OWASP Juice Shop
A vulnerable web application for security training.

2 **Purpose**

To learn and practice web application security skills.

3 **Scope**

Identify vulnerabilities within the application.

METHODOLOGY

1 **Information Gathering**
Reconnaissance and footprinting techniques were used.

2 **Vulnerability Analysis**
Automated and manual scanning tools were employed.

3 **Exploitation**
Confirmed vulnerabilities and assessed their impact.

3 **Reporting**
Documented findings and prioritized risks

KEY VULNERABILITIES IDENTIFIED

SQL Injection

Demonstrated with login bypass using `' OR '1'='1`.`

Cross-Site Scripting (XSS)

Reflected and stored XSS attacks were successful

Broken Authentication

Weak password policies and account enumeration were found.

Insecure Direct Object References (IDOR)

Accessed other user data through direct object manipulation.

Cross-Site Request Forgery (CSRF)

Profile updates could be triggered via external malicious sites due to missing CSRF protection mechanisms.

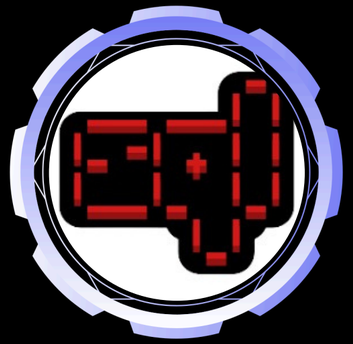
File Upload Misconfiguration

The complaint submission form allowed .xml files, exposing deprecated interfaces and raising risk of XXE attacks.

TOOLS

Wepplazer

Burp Suite

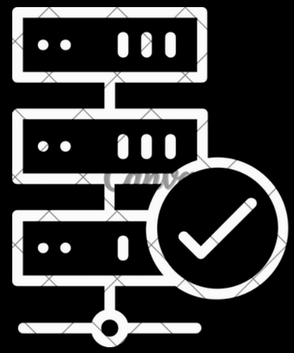


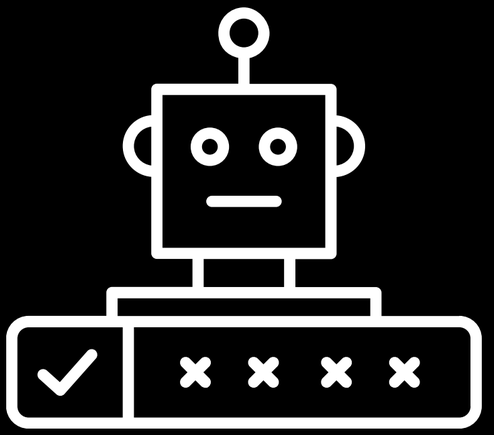
SQLmap

Automated scanner

REMEDIATION RECOMMENDATIONS

1. Enforcing robust server-side validation and authorization.
2. Eliminating deprecated features and legacy file handlers.
3. Strengthening CAPTCHA systems with session-bound tokens.
4. Sanitizing all user inputs and using prepared statements.
5. Applying CSRF protection, secure headers, and role-based access control.

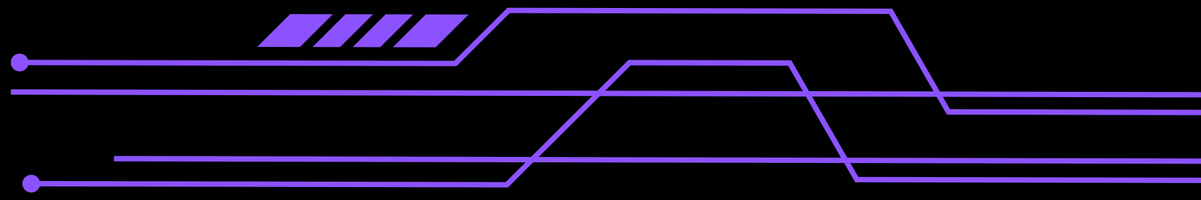




DOCUMENTATION GITHUB

To see the full Documentation, please visit the GitHub Repo

https://github.com/Muhammed-Usama/DEPI-VPT-Project.git



THANKs