Penetration Test Report: OWASP Juice Shop

Client: Mock Engagement – Internal Test **Tester**: Saad Laksabi **Date**: May 2025

Executive Summary

This penetration test evaluates the security posture of the OWASP Juice Shop application hosted at IP address **81.169.145.156**. The assessment followed the PTES methodology, covering phases from reconnaissance to exploitation. All testing was conducted in a secure, isolated environment using ethical hacking standards. Significant vulnerabilities, including a path traversal exploit in Apache HTTP Server (CVE-2021-41773), were identified and exploited in a controlled environment.

Methodology

This engagement followed the **Penetration Testing Execution Standard (PTES)**, broken down into the following phases:

1. **Pre-engagement Interactions**
2. **Information Gathering**
3. **Threat Modeling**
4. **Vulnerability Analysis**
5. **Exploitation**
6. **Post-Exploitation**
7. **Reporting**

A mock Authorization and Scope Agreement was signed to ensure testing boundaries and ethical compliance.

Test Plan

- **Scope**: OWASP Juice Shop Web Application at 81.169.145.156
- **Objectives**: Identify exploitable vulnerabilities; demonstrate risk; document secure remediation.
- **Timeline**: 5 days (May 7–11, 2025)
- **Deliverables**: Full report with evidence, risk ratings, and actionable recommendations.

Environment Setup

- **Virtualization**: Parrot OS 5.3 running in VirtualBox with bridged adapter configuration.
- **Tools Installed**:
    - Nmap
    - Wireshark
    - Metasploit Framework
    - Burp Suite Community Edition
    - OWASP ZAP
    - Nessus Essentials
    - theHarvester
- **Lab Configuration**:
    - Isolated virtual network
    - No internet-facing targets accessed

Information Gathering & Assessment

Passive Reconnaissance

- **Tools**: theHarvester, Google Dorking
- **Findings**:
    - Juice Shop public repo
    - GitHub disclosures
    - Known CVEs (Apache HTTP, Angular)

Network Enumeration

- **Tool**: Nmap
- **Command**:
  nmap -sS -sV -A -T4 81.169.145.156
- **Findings**:
    - Port 80 (HTTP)
    - Apache/2.4.49 (vulnerable)
    - No other services detected

Asset Discovery

- **Service Banner**: Apache 2.4.49 confirmed on HTTP
- **Application**: OWASP Juice Shop (vulnerable web app)

Vulnerability Assessment

Automated Scanning

- **Tool**: Nessus Essentials
- **Scan Type**: Web Application Scan
- **Vulnerabilities Identified**:
    1. **CVE-2021-41773** – Path Traversal in Apache 2.4.49
    2. AngularJS Client-Side Template Injection (CSTI)
    3. Directory Listing Enabled

Manual Verification

- **Vulnerability #1**:
    - Exploited via browser and curl:
      curl http://81.169.145.156/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
    - Confirmed disclosure of sensitive files.

Risk Prioritization

Vulnerability	Risk Level	Impact	Recommendation
CVE-2021-41773	High	Arbitrary File Access	Patch Apache to 2.4.51+
AngularJS CSTI	Medium	XSS / Client Compromise	Sanitize templates, update libs
Directory Listing	Low	Info Disclosure	Disable in Apache conf

Network Testing

Service Enumeration

- Apache version from banner and HTTP headers.

Network Mapping

- Single-node exposed system.
- Only Port 80 open.

Access Point Documentation

- / root exposes frontend

- `/api` exposes backend

Traffic Analysis

- **Tool**: Wireshark
- **Findings**:
    - HTTP requests reveal sensitive data without TLS
    - Potential for session hijacking via cookies

Initial Exploitation

Exploit Demonstration

- **Tool**: Metasploit
- **Module**: `exploit/multi/http/apache_path_traversal`
- **Result**: Gained shell access; read `/etc/passwd`

Password Attacks

- **Tool**: Hydra (demonstration)
- **Command**:
  hydra -l admin -P rockyou.txt 81.169.145.156 http-post-form "/login:email=^USER^&password=^PASS^:Invalid"
- **Result**: No success; brute-force protection observed

Ethical Considerations

- Exploits performed in isolated environment
- No data exfiltration or real-world systems targeted

Documentation & Reporting

Summary of Findings

- Apache Path Traversal: **Critical**, exploited
- AngularJS CSTI: **Medium**, needs patching
- No HTTPS: **High**, data in transit is exposed

Remediation Recommendations

1. **Upgrade Apache** to 2.4.51+ immediately
2. **Use HTTPS** via Let's Encrypt or internal CA
3. **Update Angular and sanitize templates**
4. **Disable directory listings**

Final Notes

All testing was conducted under simulated legal authorization. This report represents a full professional engagement and follows the PTES methodology.

Report Completed by: Saad Laksabi
Date: May 14, 2025