**Penetration Testing Report**

**OWASP Juice Shop Company**  
**Report of Findings**

**Prepared by: Emman**

**Lead Penetration Tester at Secured Wellness**

**emman@securedwellness.com**  
Date: 14/07/2025

**Table of Contents**

1. Document Control ……………………………………………………………… 1
2. Confidentiality ……………………………………………………………… 1
3. Disclaimers ………………………………………………………………… 1
4. Proprietary Information …………………………………………………… 1
5. Contact Information ………………………………………………………… 2
6. Executive Summary ………………………………………………………… 2
7. Assessment Summary ……………………………………………………… 2
8. Strategic Recommendation ………………………………………………… 3
9. Technical Summary ………………………………………………………… 3
10. Finding Severity Ratings ………………………………………………… 3
11. Scope ……………………………………………………………………… 3
12. Scope Exclusions ………………………………………………………… 4
13. Post Assessment Clean-up ………………………………………………… 4
14. Findings Overview ………………………………………………………… 4
15. Technical Detail …………………………………………………………… 4
16. Summary of Findings ……………………………………………………… 8
17. Conclusion ………………………………………………………………… 9
18. Appendices ………………………………………………………………… 10

Total pages:12

**Document Control**

**CONFIDENTIALITY**  
This document contains proprietary and confidential information belonging to Owasp Juice Shop Company. It is intended solely for the authorized recipients within the organization and must not be distributed outside without explicit permission. Extreme care should be taken to handle this document appropriately and keep it marked “CONFIDENTIAL.” In no event shall Secured Wellness be liable to anyone for special, incidental, collateral or consequential damages arising out of the use of this information.

Address any questions regarding the use or dissemination of this document to:  
Secured Wellness  
Attention: Contracts Manager  
Email: emman@securedwellness.com  
Phone: (+251) 911222222

**DISCLAIMERS**

The information in this document is provided "as is," without warranty. The penetration test reflects a “point-in-time” assessment; environmental changes or new vulnerabilities may arise post-testing. This report should serve as a security guide and not a comprehensive (100%) or permanent risk assessment threatening your systems, networks and applications.

**Proprietary Information**

The content of this document is considered proprietary information and should not be disclosed outside of the recipient organization’s network. All contents herein are proprietary to OWASP JUICE SHOP Company and SECURED WELLNESS. Copies are permitted solely for internal distribution or regulatory review purposes.

**Contact Information**

| **Name** | **Title** | **Contact Information** |
| --- | --- | --- |
| Emman | Lead Penetration Tester | emman@securedwellness.com |
| Owasp Company IT Manager | IT Manager | itmanager@waspjuiceshop.com |

**Executive Summary**

Secured Wellness conducted an external penetration test of Owasp Juice Shop Company’s website environment, accessed at http://10.10.130.178:3000, from July 7, 2025, to July 14, 2025. The test focuses on six identified key vulnerabilities: SQL Injection, Broken Access Control, Cross-Site Scripting (XSS), Insecure Direct Object References (IDOR), Security Misconfiguration, and Sensitive Data Exposure. These ranged from Critical to Medium severity and demonstrated risk of unauthorized access, data leakage, and potential compromise. All findings were validated using manual techniques and supported by Burp Suite and browser-based exploitation. Immediate remediation of critical issues is strongly recommended.

**Assessment Summary**

Based on the security assessment for Owasp web applications the current status of the identified vulnerabilities set the risk at a “CRITICAL” level, which if not addressed in time (strongly recommended) before going in a live production environment), these vulnerabilities could be a trigger for a Cyber security breach. These vulnerabilities can be easily fixed by following the best practices and recommendations given throughout the report. Our security assessment of the OWASP Juice Shop application revealed vulnerabilities classified as follows:

| **Severity** | **Number of Findings** |
| --- | --- |
| Critical | 2 |
| High | 1 |
| Medium | 3 |
| Low | 0 |

If left unaddressed, these vulnerabilities could enable attackers to escalate privileges, access sensitive data, or disrupt services. The vulnerabilities are exploitable with commonly available tools and limited technical effort.

**Strategic Recommendation**

It is advised that Secured Wellness Company prioritize patching the critical and high vulnerabilities immediately. Medium severity issues should be addressed following this to strengthen overall security posture. Additionally, implementing secure coding practices and regular security assessments will help mitigate future risks.

**Technical Summary**

**Finding Severity Ratings**

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS v3.0 Score Range** | **Description** |
| Critical | 9.0 – 10.0 | Exploitation likely leads to full system compromise; immediate remediation required. |
| High | 7.0 – 8.9 | Serious vulnerabilities that can result in significant unauthorized access or data loss. |
| Medium | 4.0 – 6.9 | Exploitable under certain conditions; moderate impact. |
| Low | 0.1 – 3.9 | Minor issues; lower risk but should be fixed during maintenance. |

**Scope**

**Assessment Details**

* Target Application: OWASP Juice Shop
* Test Type: External Penetration Test
* TryHackMe Juice Shop VM
* URL: http://10.10.130.178:3000

**Scope Exclusions**

* Denial of Service (DoS) attacks were excluded per client request.
* Social engineering tests were not performed.

**Post Assessment Clean-up**

All test accounts created during the assessment have been disabled and removed along with any associated test data.

**Findings Overview**

|  |  |  |
| --- | --- | --- |
| **Ref ID** | **Vulnerability** | **Risk/Severity** |
| OWASP-1 | SQL Injection (SQLi) | Critical |
| OWASP-2 | Broken Access Control (Admin) | Critical |
| OWASP-3 | Brute Force Attack on Admin Password | High |
| OWASP-4 | Insecure Direct Object References (IDOR) | Medium |
| OWASP-5 | Security Misconfiguration | Medium |
| OWASP-6 | Sensitive Data Exposure | Medium |

**Technical Details**

**Vulnerability 1: SQL Injection (SQLi)**

|  |
| --- |
| SQL Injection (SQLi) Ref ID: OWASP-1 Risk/Severity: Critical (CVSS v3.1 Score: 9.1) Affected Component: Login and search input fields Description: Unsanitized user input in the login form allowed injection of malicious SQL code, enabling attackers to bypass authentication and extract sensitive data from the database.  **Proof of Concept:**  By injecting ' OR '1'='1' -- in the username field, login was bypassed successfully, granting access without valid credentials. **Recommendation:** Use parameterized queries or prepared statements to safely handle all user inputs in database commands. Sanitize and validate inputs on both client and server sides. Consider deploying a web application firewall (WAF) to block malicious requests. Regularly test and review your database queries to catch vulnerabilities early. |
|  |

**Vulnerability 2: Broken Access Control**

|  |
| --- |
| Broken Access Control (Admin Page Access) Ref ID: OWASP-2 Risk/Severity: Critical (CVSS v3.1 Score: 9.8) Affected Component: Admin route Description: Hidden admin page was accessible without proper privileges. **Description:** Access controls on administrative APIs were improperly enforced, allowing unauthorized users to perform privileged actions such as modifying or deleting data. **Proof of Concept:**  By directly sending crafted HTTP requests to admin endpoints without authentication tokens, unauthorized data manipulation was successful. **Recommendation:** Implement strict role-based access control (RBAC) that ensures users can only access authorized resources. Always verify permissions on the server side, never rely solely on client-side checks. Use secure authentication tokens that expire and are validated properly. Monitor access logs to detect suspicious activity in sensitive areas. |

**Vulnerability 3:** Brute Force Attack on Admin Password

|  |
| --- |
| Brute Force Attack on Admin Password Ref ID: OWASP-3 Risk/Severity: High (CVSS v3.1 Score: 7.5) Affected Component: Login endpoint  Description: Password brute-forced using Burp Intruder and best1050.txt wordlist. **Proof of Concept**: Used Burp Suite to brute force the Admin password.  A screenshot of a computer  AI-generated content may be incorrect.  **Recommendation:** Apply rate-limiting to restrict the number of login attempts in a short period. Lock accounts temporarily after multiple failed login tries to prevent guessing. Use multi-factor authentication (MFA) for admin accounts to add an extra security layer. Enforce strong password requirements and encourage regular updates. |

**Vulnerability 4: Insecure Direct Object References (IDOR)**

|  |
| --- |
| Insecure Direct Object Reference (IDOR - Jim Reset) Ref ID: OWASP-4 Risk/Severity: Medium (CVSS v3.1 Score: 5.8) Affected Component: Password reset functionality **Description:** Reset another user’s password without authorization **Proof of Concept:**  A screenshot of a computer  AI-generated content may be incorrect. Manipulated input to reset "Jim" user’s credentials.  Recommendation: Ensure every request to access or modify resources checks that the user is authorized for that specific object. Use indirect references or tokens instead of exposing actual database IDs or file paths. Implement strong input validation and output encoding to avoid tampering. |

**Vulnerability 5: Security Misconfiguration**

|  |
| --- |
| Security Misconfiguration (Poison Null Byte) Ref ID: OWASP-5 Risk/Severity: Medium (CVSS v3.1 Score: 4.5) Affected Component: File handler endpoint **Description:** Accessed unauthorized files via %2500 injection.. **Proof of Concept:**  A screenshot of a computer  AI-generated content may be incorrect.  Security header analysis tools confirmed absent or misconfigured headers. **Recommendation:** Harden server and application configurations by disabling unnecessary features and enabling security headers like Content Security Policy. Keep software and dependencies up to date with security patches. Use automated scanning tools to detect misconfigurations. Avoid exposing detailed error messages that could reveal system information. |

**Vulnerability 6: Sensitive Data Exposure**

|  |
| --- |
| Sensitive Data Exposure (Confidential File) Ref ID: OWASP-6 Risk/Severity: Medium (CVSS v3.1 Score: 5.3) Affected Component: Internal document storage **Description:** Downloaded a confidential internal document without credentials.  **Proof of Concept:** A screenshot of a computer  AI-generated content may be incorrect. **Recommendation:** Protect sensitive data and files with strict access controls and permissions. Encrypt sensitive data both in storage and during transmission using strong encryption methods. Regularly audit access logs to detect unauthorized data access. Avoid storing sensitive information unless absolutely necessary.  . |

|  |
| --- |
| **Summary of Findings** |
| | **Issue ID** | **Description** | **Risk Rating** | **Page Reference** | | --- | --- | --- | --- | | OWASP-1 | SQL Injection | Critical | 7 | | OWASP-2 | Broken Access Control (Admin Page Access) | Critical | 7 | | OWASP-3 | Brute Force on Admin Login | High | 8 | | OWASP-4 | IDOR – Jim’s Password Reset | Medium | 9 | | OWASP-5 | Poison Null Byte (Security Misconfiguration) | Medium | 9 | | OWASP-6 | Sensitive Data Exposure (Confidential File Access) | Medium | 10 | |

**Conclusion**

The penetration testing exercise on the OWASP Juice Shop application revealed **six critical to medium vulnerabilities**, all of which were practically exploited during the assessment. These include SQL Injection, Broken Access Control, Brute Force on Admin Login, Insecure Direct Object Reference (IDOR), Poison Null Byte (Security Misconfiguration), and Sensitive Data Exposure. Each vulnerability was successfully demonstrated using standard attacker tools and techniques, confirming that the application's current security posture poses a **high risk of compromise**.

**Immediate remediation** is required for the Critical and High vulnerabilities, particularly the Broken Access Control and SQL Injection, as they enable unauthorized access and full administrative control. The Medium severity issues also warrant prompt attention to reduce attack surface and prevent escalation.

We strongly recommend implementing secure development practices, regular vulnerability scanning, and a robust patch management process. By addressing these vulnerabilities and applying ongoing security measures, Owasp Juice Shop Company can significantly strengthen its web application defenses.

**Appendices**

**Appendix A: Tools and Techniques Used**

During the assessment of the OWASP Juice Shop application, the following tools and techniques were utilized:

* **Burp Suite Community Edition** was the primary tool used to intercept and modify HTTP requests and responses. It was also used to perform brute-force attacks using the Intruder module, identify vulnerabilities in login mechanisms, and analyze application behavior.
* **Built-in browser developer tools (F12)** were used to inspect JavaScript files, discover hidden endpoints like the administration panel, and debug elements of the frontend logic.
* The **TryHackMe OWASP Juice Shop lab environment** provided a safe and controlled environment for conducting the penetration test, simulating real-world application vulnerabilities.
* A **custom wordlist (best1050.txt)** sourced from SecLists was used during brute-force testing to uncover weak credentials.
* **Manual exploitation techniques** were employed to identify and verify all six vulnerabilities. No automated scanners were used; findings were validated through careful observation and crafted input.

**Appendix B: Glossary of Terms**

* **SQL Injection (SQLi)**: A type of attack where malicious SQL code is inserted into input fields to manipulate database queries and extract sensitive information.
* **Cross-Site Scripting (XSS)**: A vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users.
* **Broken Access Control**: Occurs when restrictions on authenticated users are not properly enforced, enabling unauthorized actions.
* **IDOR (Insecure Direct Object Reference)**: A vulnerability where users can access or manipulate resources by modifying input values such as IDs in URLs.
* **Security Misconfiguration**: Improper configuration of security headers, server settings, or components, leaving the application exposed to attacks.
* **Sensitive Data Exposure**: Involves the accidental or intentional leakage of sensitive user data such as passwords, tokens, or personal information.
* **Poison Null Byte**: A technique used to exploit improper input termination, where %00 is injected to trick the application into prematurely ending string processing.
* **Brute Force Attack**: A method of repeatedly attempting different passwords or keys to gain unauthorized access.

**Appendix C: Vulnerability Severity Levels**

Critical: A vulnerability that could lead to full system compromise andimmediate action is required.

● High: A serious vulnerability that could allow unauthorized access or significant disruption.

● Medium: A vulnerability that presents some risk but may require certain conditions or skills to exploit.

● Low: A minor vulnerability that is unlikely to be exploited but should still be remediated as part of best practices.

| **Severity** | **CVSS Score Range** | **Description** |
| --- | --- | --- |
| Critical | 9.0 – 10.0 | Exploitation leads to full compromise; urgent fix. |
| High | 7.0 – 8.9 | Serious risk; prompt remediation required. |
| Medium | 4.0 – 6.9 | Moderate risk; remediation recommended. |
| Low | 0.1 – 3.9 | Minor issues; fix during scheduled maintenance. |

**End of Report**  
Prepared by: Emman – Lead Penetration Tester, Secured Wellness  
Date: July 14, 2025