**OWASP Juice Shop**

Security Assessment Findings Report

## Business Confidential

*Date: August 15th, 2025 Project: OJS-001 Version 1.0*

## Table of Contents

[Table of Contents 2](#_bookmark0)

[Confidentiality Statement 3](#_bookmark1)

[Disclaimer 3](#_bookmark2)

[Contact Information 3](#_bookmark3)

[Assessment Overview 4](#_bookmark4)

[Assessment Components 4](#_bookmark5)

[Finding Severity Ratings 5](#_bookmark7)

[Risk Factors 5](#_bookmark8)

[Likelihood 5](#_bookmark9)

[Impact 5](#_bookmark10)

[Scope 6](#_bookmark11)

[Scope Exclusions 6](#_bookmark12)

[Client Allowances 6](#_bookmark13)

[Executive Summary 6](#_bookmark14)

[Scoping and Time Limitations 7](#_bookmark15)

[Testing Summary 7](#_bookmark16)

[Tester Notes and Recommendations 7](#_bookmark17)

[Key Strengths and Weaknesses 8](#_bookmark18)

[Vulnerability Summary & Report Card 8](#_bookmark19)

[Penetration Test Findings 8](#_bookmark20)

[Technical Findings 1](#_bookmark21)0

[Penetration Test Findings 1](#_bookmark22)0

[Finding OJS-001-F001: SQL Injection In Login (Critical) 10](#_bookmark23)

[Finding OJS-001-F002: Admin Registration Bypass (Critical) 12](#_bookmark24)

[Finding OJS-001-F003: Broken Access Control On Cart (High) 13](#_bookmark25)

[Finding OJS-001-F004: Brute Force On Admin Password (High) 14](#_bookmark26)

[Finding OJS-001-F005: XSS On Search (High) 16](#_bookmark27)

[Finding OJS-001-F006: Abusing Functionality Of Ai Chatbot (Moderate) 17](#_bookmark28)

[Finding OJS-001-F007: Improper Input Validation In Register Page (Moderate) 1](#_bookmark29)8

[Finding OJS-001-F008: Enumeration To Find Admin Path (Moderate) 1](#_bookmark30)9

[Additional Scans and Reports 2](#_bookmark48)0

# Confidentiality Statement

This document is the exclusive property of **TheKnower** and **OWASP JUICE SHOP**. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both parties.

# Disclaimer

This penetration test is a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes made outside of that period.  
The engagement did not include Denial of Service (DoS) or Social Engineering testing.

# Contact Information

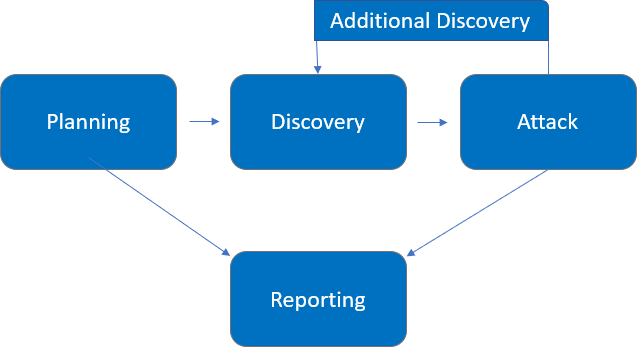
|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| OWASP JUICE SHOP | | |
| Andrew van der stock | Global Information Security Manager | Email: andrew.vanderstock@gmail.com |
| TheKnower | | |
| Abdelrahman Nashat | Penetration Tester | Email: silentroot200@gmail.com |
| Abdelrahman Elnaggar | Penetration Tester | Email : abdelrahmanmoh023@gmail.com |

# Assessment Overview

From 10 August 2025 to 15 August 2025, a web application penetration test was conducted on OWASP Juice Shop.  
Testing was based on the **OWASP Testing Guide v4** and focused on identifying exploitable vulnerabilities in the application.  
A total of **8 vulnerabilities** were identified, ranging from **Moderate** to **Critical** severity.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

**Type:** Web Application Penetration Test

Methodology**:** OWASP Testing Guide v4

**Scope:** OWASP Juice Shop (Full functionality)

**Excluded Tests:** DoS, Social Engineering

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3**  **Score Range** | **Definition** |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact:

### Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

### Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

|  |  |
| --- | --- |
| **Assessment** | **Details** |
| Full OWASP Juice Shop application | https://juice-shop.herokuapp.com/ |

### Scope Exclusions

Per client request, TheKnower did not perform any of the following attacks during testing:

* Denial of Service (DoS)
* Phishing/Social Engineering

All other attacks not specified above were permitted by OWASP JUICE SHOP.

### Client Allowances

Demo Corp provided TCMS the following allowances:

* Full Authinticated And Unauthinticated Testing Permitted

# Executive Summary

The assessment revealed serious security weaknesses in OWASP Juice Shop, including SQL Injection, Broken Access Control, and Cross-Site Scripting.  
Exploitation of these vulnerabilities could lead to account compromise, data leakage, and administrative takeover.

### Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

### Testing Summary

Manual And Automated Testing Was Performed Included Exploits Confirmed :

- SQL Injection In Login

- Broken Access Control on cart

- Admin registration bypass

- Cross-Site Scripting (XSS) in search

- Brute Force on admin password

- Improper input validation

- Enumeration of admin path

- Abuse of AI chatbot functionality

### Tester Notes and Recommendations

Weak authentication and poor input validation were consistent issues.  
Recommendation: Implement strict input validation, improve authentication mechanisms, and secure administrative functionality.

### Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

* 1. Application uses HTTPS by default
  2. Some security headers implemented

following identifies the key weaknesses identified during the assessment:

1. Lack of rate limiting
2. Missing server-side input validation
3. Multiple injection vulnerabilities
4. Broken Access Control

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

### Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2 | 3 | 3 | 0 | 0 |
| Critical | High | Moderate | Low | Informational |

|  |  |  |
| --- | --- | --- |
| **Finding** | **Severity** | **Recommendation** |
| Penetration Test | | |
| OJS-001-F001: SQL Injection In Login | Critical | Use parameterized queries |
| OJS-001-F002: Admin Registration Bypass | Critical | Restrict endpoint & validate server-side |
| OJS-001-F003: Broken Access Control On Cart | High | Implement authorization checks |
| OJS-001-F004: Brute Force On Admin Password | High | Add rate limiting & lockout |
| OJS-001-F005: XSS On Search | High | Encode output & sanitize input |
| OJS-001-F006: Abusing Functionality Of Ai Chatbot | Moderate | Add intent filtering & validation |
| OJS-001-F007: Improper Input Validation In Register Page | Moderate | Sanitize & validate input server-side |
| OJS-001-F008: Enumeration To Find Admin Path | Moderate | Hide sensitive endpoints |

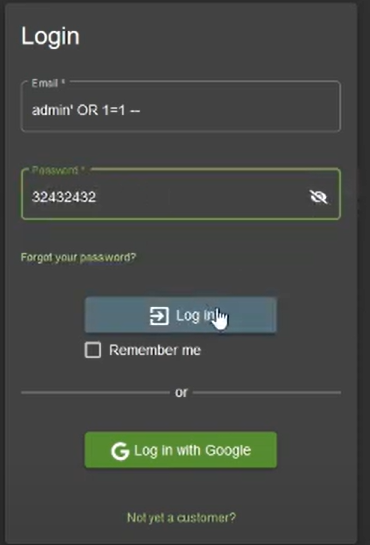
# Technical Findings

### Penetration Test Findings

Finding OJS-001-F001: SQL Injection In Login (Critical)

|  |  |
| --- | --- |
| Description: | The login functionality is vulnerable to SQL injection, allowing attackers to bypass authentication and log in as any user without valid credentials. |
| Risk: | Likelihood: High – Easily tested with basic SQLi payloads  Impact: Very High – Leads to full compromise of accounts, including admin |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Manual Review |
| References: | https://owasp.org/www-community/attacks/SQL\_Injection |

Evidence



*Figure 1: SQLI Payload In Login*



Remediation

*Figure 2: Access To Admin Account”*

Use parameterized queries (prepared statements), sanitize inputs, and enforce strong database security configurations

Finding OJS-001-F002: Admin Registration Bypass (critical)

|  |  |
| --- | --- |
| Description: | The admin registration endpoint lacks proper server-side restrictions, allowing attackers to directly register a new admin account by bypassing client-side controls |
| Risk: | Likelihood: High – Easily exploited via direct request manipulation  Impact: Very High – Allows full administrative access to the application |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Burpsuite |
| References: | https://owasp.org/www-project-top-ten/2017/A2\_2017-Broken\_Authentication |

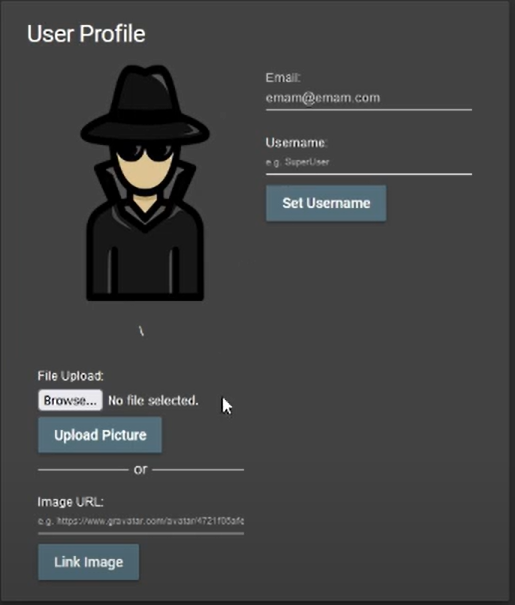
Evidence



*Figure 3: Before change it to admin*



*Figure 4: After change it to admin*

 *Figure 5: emam become admin*

Remediation

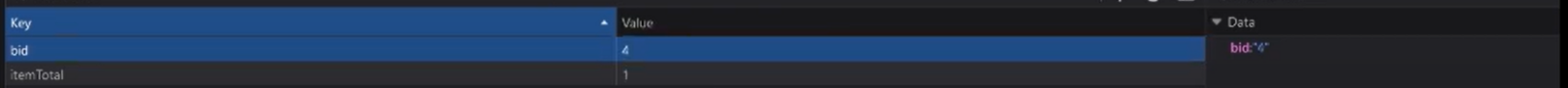
Enforce server-side role assignment validation, remove ability to set admin privileges from registration requests, and require approval for admin accounts.

Finding OJS-001-F003: Broken Access Control On Cart (High)

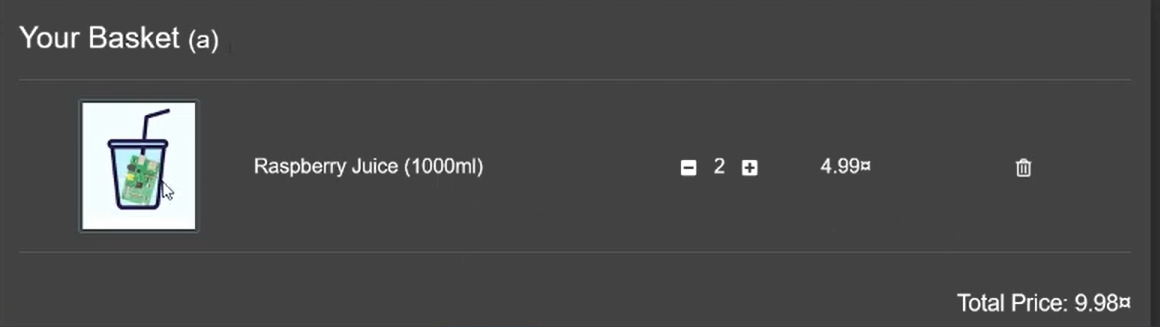
|  |  |
| --- | --- |
| Description: | The cart functionality lacks proper authorization checks, allowing a logged-in user to modify another user’s cart by changing the UserId in API requests. |
| Risk: | Likelihood: High – Easily tested by changing parameters  Impact: High – Can manipulate or delete other users’ orders |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Manual Review |
| References: | https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/ |

\

Evidence



*Figure 6: Bid changed to another number*



*Figure 7: Access To Another Cart*

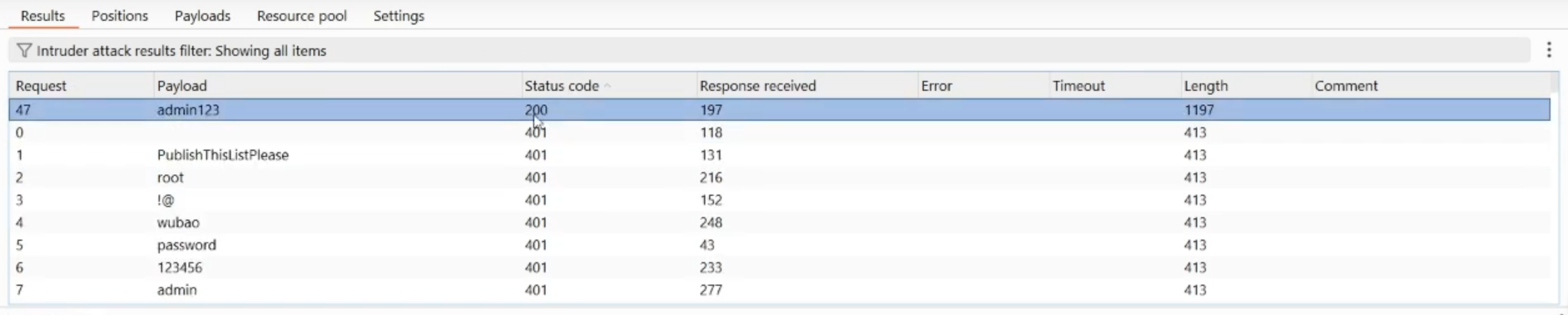
Remediation

Implement server-side ownership checks before processing cart modifications.

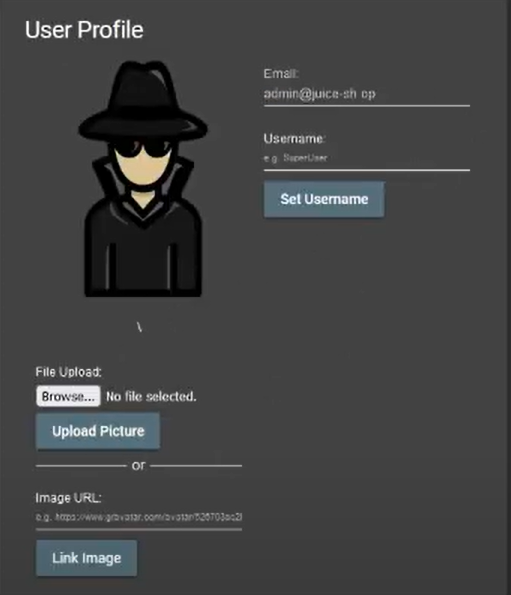
Finding OJS-001-F004: Brute Force On Admin Password (High)

|  |  |
| --- | --- |
| Description: | The login page lacks rate-limiting, allowing attackers to perform brute-force attacks against admin accounts |
| Risk: | Likelihood: High – Can be automated with common tools  Impact: High – Could lead to admin account compromise |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Burpsuite |
| References: | https://cheatsheetseries.owasp.org/cheatsheets/Authentication\_Cheat\_Sheet.html |

Evidence



*Figure 8: the right password is admin123 with 200 status code*



Remediation

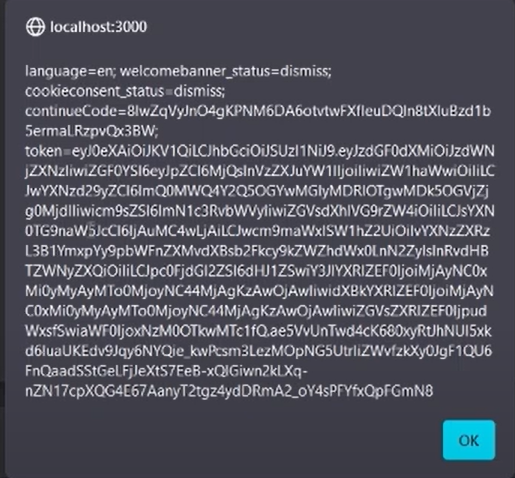
*Figure 9: Access To Admin Account*

Implement account lockout after a defined number of failed attempts, add CAPTCHA, and monitor suspicious login attempts.

Finding OJS-001-F005: XSS On Search (High)

|  |  |
| --- | --- |
| Description: | The search function reflects unsanitized user input, allowing attackers to inject malicious JavaScript into the response, leading to stored or reflected XSS attacks |
| Risk: | Likelihood: High – Can be exploited via crafted URLs  Impact: High – Can steal cookies, session tokens, or redirect users to malicious sites |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Manual Review |
| References: | https://owasp.org/www-community/attacks/xss/ |

Evidence



Remediation

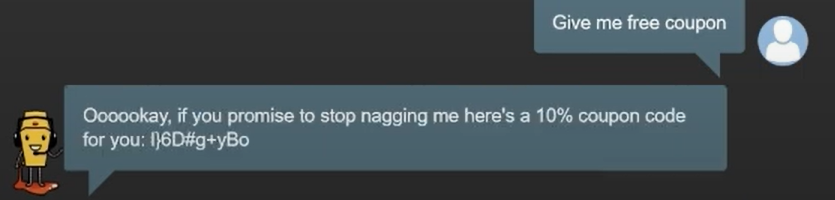
*Figure 10: Cookies appear by xss*

Sanitize and encode all user input before rendering, and use a security library to escape HTML output.

Finding OJS-001-F006: Abusing Functionality Of Ai Chatbot (Moderate)

|  |  |
| --- | --- |
| Description: | The OWASP Juice Shop AI chatbot lacks proper intent filtering and validation, allowing attackers to abuse its functionality to retrieve sensitive information or guide users toward malicious links. This could potentially lead to information disclosure and social engineering attacks. |
| Risk: | Likelihood: Medium – Requires user interaction but can be abused with crafted inputs  Impact: Medium – Can lead to user deception, data leakage, or indirect exploitation |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Manual Review |
| References: | https://owasp.org/www-community/attacks/Chatbot\_Security |

Evidence



Remediation

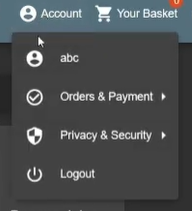
*Figure 11: chatbot give 10% coupon code*

Implement strict server-side validation for chatbot queries, restrict sensitive responses, and apply content filtering to prevent abuse

Finding OJS-001-F007: Improper Input Validation In Register Page (Moderate)

|  |  |
| --- | --- |
| Description: | The registration form fails to properly validate input server-side, allowing special characters and unexpected data that could lead to injection attacks |
| Risk: | Likelihood: Medium – Relies on bypassing client-side validation  Impact: Medium – May lead to SQLi, XSS, or account creation abuse |
| System: | https://juice-shop.herokuapp.com/ |
| Tools Used: | Manual Review |
| References: | https://owasp.org/www-community/Input\_Validation |

Evidence



Remediation

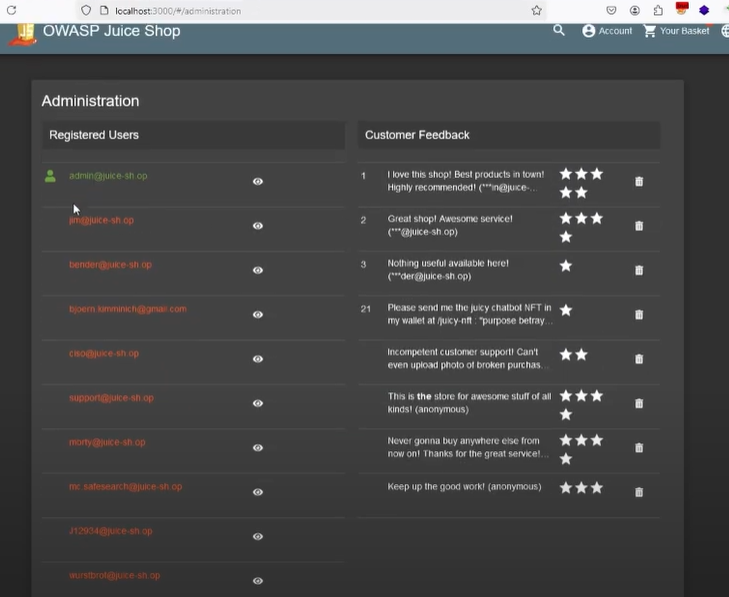
*Figure 12: we can register and login without restrictions auth by remove register button*

Enforce strict server-side validation and sanitize all user inputs before processing.

Finding OJS-001-F008: Enumeration To Find Admin Path (Moderate)

|  |  |
| --- | --- |
| Description: | The application reveals admin panel endpoints via predictable URLs and verbose error messages, enabling attackers to locate sensitive administrative functions |
| Risk: | Likelihood: Medium – Requires some enumeration effort  Impact: Medium – Provides valuable information for targeted attacks |
| Tools Used: | FFuF |
| References: | https://owasp.org/Top10/A05\_2021-Security\_Misconfiguration/ |

Evidence



*Figure 13 : access the registered users by enumurate administration directory*

Remediation

Hide administrative endpoints, use unpredictable paths, and enforce authentication for access.

### Additional Scans and Reports

Burp Suite scan results and OWASP ZAP output were generated and can be provided upon request.