



# OWASP Juice Shop-Report

## Team-Members:

- Hatem Harby Mohamed ([Leader](#))
- Mohamed Ahmed Othman Mahmoud
- Ammar Ahmed Mohammed Eid
- Abdul Rahman Nasr Rushdie
- Abdul Hamid Hani Mohamed
- Ahmed Ezzat

## 1. Executive Summary

This report presents the results of a penetration test performed on OWASP Juice Shop, a deliberately insecure web application used for security training.

The objective of the assessment was to evaluate the security posture of the application by identifying and exploiting common vulnerabilities that reflect real-world threats.

Several critical issues were discovered, including **SQL Injection**, **Broken Access Control**, **Cross-Site Scripting (XSS)**, **Account takeover**, and **Security Misconfigurations**.

If exploited by an attacker, these vulnerabilities could lead to data leakage, unauthorized access, account takeover, and full compromise of the application.

Overall, the security posture of the application is considered **High Risk**.

The screenshot shows the OWASP Juice Shop application interface. At the top, there's a navigation bar with 'Back' and 'Learn > OWASP Juice Shop'. Below it is the main title 'OWASP Juice Shop' with a small icon of a juice carton. A descriptive text states: 'This room uses the Juice Shop vulnerable web application to learn how to identify and exploit common web application vulnerabilities.' There are also icons for signal strength, battery, and a timer indicating 120 min. Below this, there are buttons for 'Start AttackBox', 'Save Room', 'Recommend' (with 4629 recommendations), and 'Options'. A progress bar at the bottom indicates 'Room progress (64%)'. The main content area lists six tasks:

- Task 1: Open for business! (Completed)
- Task 2: Let's go on an adventure! (Completed)
- Task 3: Inject the juice (Completed)
- Task 4: Who broke my lock?! (Completed)
- Task 5: AH! Don't look! (Completed)
- Task 6: Who's flying this thing? (Completed)

A small green alien icon is visible in the bottom left corner of the interface.

## 2. Scope of Work

**Target:** OWASP Juice Shop (Local deployment)

**URL:** <http://localhost:3000>

**Testing Type:** Black-box / Manual

Allowed Techniques: Web vulnerability scanning, manual exploitation, injection attacks, enumeration

Tools Used:

- Burp Suite Community
- Dirsearch
- Browser Developer Tools

## 3. Methodology

The testing methodology followed the guidelines of:

- OWASP Top 10
- Manual testing and fuzzing

**The approach consisted of:**

1. **Reconnaissance** – Gathering information about the application
2. **Enumeration** – Identifying input fields, parameters, and hidden functionalities
3. **Vulnerability Testing** – Manual and automated scanning
4. **Exploitation** – Validating vulnerabilities
5. **Reporting** – Documenting findings and recommendations

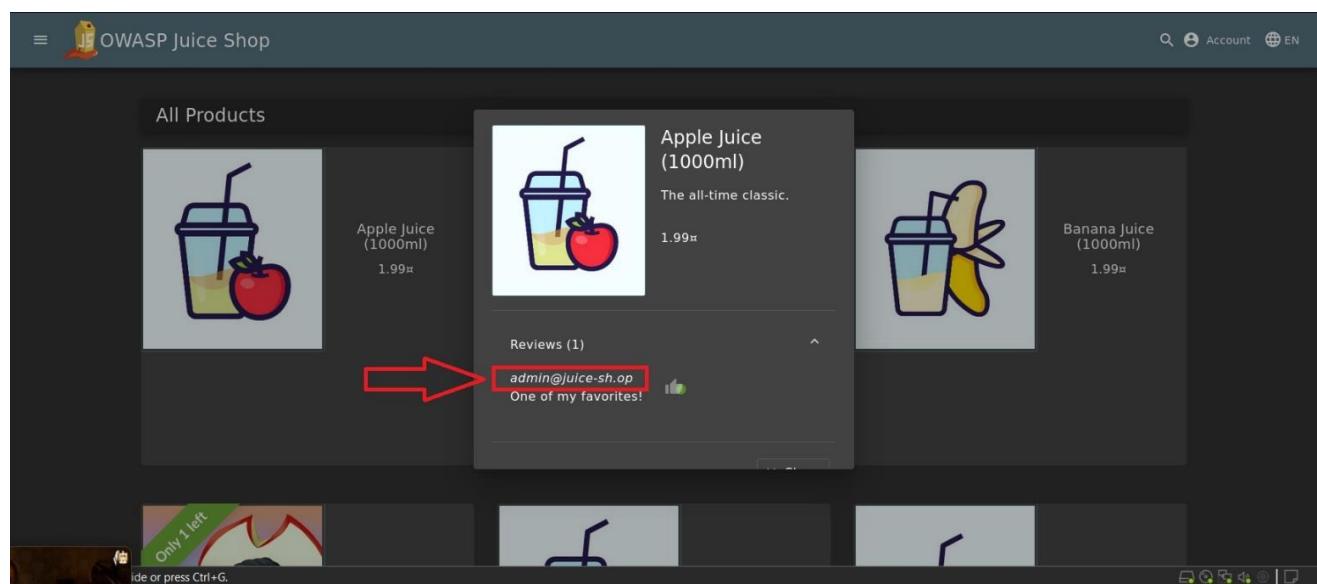
## 4. Findings Summary

| Vulnerability                     | Risk Level | Status    |
|-----------------------------------|------------|-----------|
| SQL Injection                     | High       | Exploited |
| Broken Authentication             | High       | Exploited |
| Broken Access Control             | High       | Exploited |
| Cross-Site Scripting (XSS)        | Medium     | Exploited |
| Sensitive Data Exposure           | Medium     | Confirmed |
| Logic Vulnerability               | High       | Confirmed |
| Cross-Site Request Forgery (CSRF) | Medium     | Exploited |

## Gathering information about the application:

During the information gathering, a collection of emails belonging to users was gathered, including sensitive emails such as the admin's email:

- admin@juice-sh.op
- bender@juice-sh.op
- stan@juice-sh.op
- uvogin@juice-sh.op
- jim@juice-sh.op
- mc.safesearch@juice-sh.op
- accountant@juice-sh.op
- bjoern@owasp.org
- morty@juice-sh.op



The screenshot shows the OWASP Juice Shop application interface. The top navigation bar includes a logo, the title "OWASP Juice Shop", a search icon, an account icon, and language selection (EN). The main content area displays "All Products". One product is highlighted: "Apple Juice (1000ml)" priced at 1.99€. Below the product image is a "Reviews (1)" section. A red arrow points to the review content, which shows the email address "admin@juice-sh.op" and the text "One of my favorites!". Other products listed include "Banana Juice (1000ml)".

## Gathering information about the application:

Using **dirsearch**, a set of paths was discovered :

- `./well-known/security.txt`
- `/api-docs/`
- `/assets/`
- `/common.js`
- `/ftp`

```
Session Actions Edit View Help
from pkg_resources import DistributionNotFound, VersionConflict
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/osman/reports/http_localhost_3000/_25-11-22_01-16-31.txt
Target: http://localhost:3000/
[01:16:31] Starting:
[01:17:02] 200 - 475B - ./well-known/security.txt
[01:19:03] 301 - 158B - /api-docs/ → /api-docs/
[01:19:03] 500 - 3KB - /api-docs/
```

```
[01:19:05] 500 - 3KB - /api/v3
[01:19:05] 500 - 3KB - /api/v4
[01:19:05] 500 - 3KB - /api/version
[01:19:05] 500 - 3KB - /api/vendor/phpunit/phpunit/phpunit
[01:19:05] 500 - 3KB - /api/whoami
[01:19:05] 500 - 3KB - /apibuild.pyc
[01:19:05] 500 - 3KB - /apidoc
[01:19:05] 500 - 3KB - /apidocs
[01:19:05] 500 - 3KB - /apis
[01:19:05] 500 - 3KB - /apiserver-aggregator-ca.cert
[01:19:05] 500 - 3KB - /apiserver-aggregator.cert
[01:19:05] 500 - 3KB - /apiserver-aggregator.key
[01:19:05] 500 - 3KB - /apiserver-client.crt
[01:19:05] 500 - 3KB - /apiserver-key.pem
[01:19:13] 301 - 156B - /assets → /assets/
[01:20:13] 200 - 9KB - /common.js
```

| Name                   | Size | Modified              |
|------------------------|------|-----------------------|
| changes.csv            | 191  | PM 3:55:22 11/16/2025 |
| index.txt              | 116  | PM 3:55:22 11/16/2025 |
| provider-metadata.json | 1023 | AM 1:23:13 11/23/2025 |

## 5. Detailed Findings:

### 5.1 SQL Injection:

#### Definition:

SQL Injection is a web vulnerability that allows an attacker to interfere with the queries an application makes to its database by injecting malicious SQL commands.

**Risk Level:** High

**Affected URL:** <http://localhost:3000/login>

#### Description:

The login functionality is vulnerable to SQL Injection due to improper input validation (email and password)

#### Proof of Concept (Payload): ' OR 1=1 --

The screenshot shows two browser tabs. The top tab is a login page for 'OWASP Juice Shop' at <http://localhost:3000/login#login>. The 'Email\*' field contains the value 'admin@juice-sh.op ' OR 1=1--'. The bottom tab is a product listing page for 'OWASP Juice Shop' at <http://localhost:3000/password.txt#/search>. The user's account information is displayed in the top right corner, showing the email 'admin@juice-sh.op' with a red arrow pointing to it.



## **Impact:**

- 1-Possibility of extracting users' data
  - 2-Can lead to full database compromise

## **Recommendation:**

## Use parameterized queries

## Apply server-side input validation

## Filter user input

## 5.2 Broken Authentication:

We were able to find a **Broken Authentication vulnerability** by :

- Brute Force Attack
- Account Takeover

### Brute Force Attack:

#### Definition:

Brute Force is an attack technique where an attacker repeatedly tries different username and password combinations until the correct credentials are found, exploiting weak authentication controls.

**Risk Level:** High

**Affected Page:** /login

#### Description:

The login functionality is vulnerable to brute force attacks due to the absence of rate limiting, CAPTCHA, and account lockout mechanisms. An attacker can repeatedly attempt multiple username and password combinations without restriction, allowing unauthorized access through credential guessing.



## Proof of Concept:

Screenshot of Burp Suite Community Edition v2025.10.3 - Temporary Project showing an Intruder attack against http://localhost:3000.

The payload list contains the following items:

- zapato
- zirtaeb
- zecob
- zcoob
- zcoobnm
- zcooz
- ZXZXC
- zzzz
- zzzzzz

The payload configuration section shows a simple list of strings used as payloads. The payload position is set to "All payload positions" and the payload type is "Simple list". The payload count is 1,048 and the request count is also 1,048.

The payload being sent is: {"email":"admin@juice-sh.op","password":"**123456**"}

Screenshot of the Burp Suite Results tab showing the response to the 116th request.

| Request | Payload    | Status code | Response received | Error | Timeout | Length | Comment |
|---------|------------|-------------|-------------------|-------|---------|--------|---------|
| 116     | admin123   | 200         | 10                |       |         | 1197   |         |
| 0       | 0          | 401         | 27                |       |         | 413    |         |
| 1       | 00000      | 401         | 6                 |       |         | 413    |         |
| 2       | 000000     | 401         | 5                 |       |         | 413    |         |
| 3       | 0000000    | 401         | 3                 |       |         | 413    |         |
| 4       | 00000000   | 401         | 12                |       |         | 413    |         |
| 5       | 000000000  | 401         | 9                 |       |         | 413    |         |
| 6       | 0987654321 | 401         | 8                 |       |         | 413    |         |

Screenshot of a browser window showing the OWASP Juice Shop login page at http://localhost:3000/login#login.

The login form fields are filled with "admin@juice-sh.op" and "admin123".

Screenshot of a browser window showing the OWASP Juice Shop homepage at http://localhost:3000/password.txt#/search.

The user "admin@juice-sh.op" is logged in, as indicated by the user icon and name in the top right corner.

## Impact:

- Unauthorized access to user accounts
- Potential full account takeover
- Exposure of sensitive user information
- Ability for attackers to escalate privileges if high-value accounts (e.g., admin) are compromised
- Increased risk of automated credential stuffing attacks
- Compromise of the entire system if administrative credentials are guessed

---

## Recommendation:

- Implement rate limiting (e.g., block or delay after multiple failed attempts)
- Add account lockout after repeated failed login attempts
- Enable Multi-Factor Authentication (MFA)
- Use CAPTCHA to prevent automated attacks
- Enforce strong password policies
- Monitor and alert on suspicious login attempts
- Limit login attempts per IP and per username

## Account Takeover:

### Definition:

Account Takeover (ATO) is a security breach where an attacker gains unauthorized access to a user's account by exploiting weaknesses in authentication or access control mechanisms.

**Risk Level:** High

**Affected Page:** /forgot-password

### Description:

The application is vulnerable to Account Takeover through the password reset functionality. The security question used during the reset process is easily guessable, allowing an attacker to provide the correct answer without legitimate knowledge of the user. As a result, an attacker can reset the victim's password and gain full access to their account.

### Proof of Concept:

| <b>Contents</b> <small>hide</small> <ul style="list-style-type: none"> <li>(Top)</li> <li>Depiction           <ul style="list-style-type: none"> <li>Kelvin Timeline</li> <li>Conception and television</li> <li>Films</li> <li>Franchise "reboot"</li> <li><i>Star Trek: Strange New Worlds</i></li> </ul> </li> <li>Reception           <ul style="list-style-type: none"> <li>Cultural impact</li> <li>Fan productions               <ul style="list-style-type: none"> <li><i>Star Trek: New Voyages</i></li> <li><i>Star Trek Continues</i></li> </ul> </li> </ul> </li> <li>Legacy</li> <li>References</li> <li>External links</li> </ul> | <p>promoted to lieutenant junior grade and returned to Starfleet Academy as a student instructor.<sup>[4]</sup> According to a friend, students could either "think or sink" in his class, and Kirk himself was "a stack of books with legs".<sup>[6]</sup> Upon graduating in the top five percent, Kirk was promoted to lieutenant and served aboard the USS <i>Farragut</i>.<sup>[4]</sup> While assigned to the <i>Farragut</i>, Kirk commanded his first planetary survey and survived a deadly attack by a bizarre cloud-like creature that killed a large portion of the <i>Farragut</i>'s crew.<sup>[4]</sup> including his commanding officer, Captain Garrovick. Kirk blamed himself for years for hesitating to fire his assigned weapons upon seeing the threat until a later encounter with the creature showed that firing immediately with conventional weapons would have been useless.</p> <p></p> <p>Publicity photo of William Shatner as Kirk, alongside Leonard Nimoy as Mr. Spock</p> <p>Kirk became <i>Starfleet</i>'s youngest starship captain after receiving command of the <i>USS Enterprise</i> for a five-year mission,<sup>[4]</sup> three years of which are depicted in the original <i>Star Trek</i> series (1966–1969).<sup>[7]</sup> Kirk's most significant relationships in the television series are with first officer Spock and chief medical officer Dr. Leonard "Bones" McCoy.<sup>[8]</sup> McCoy is someone to whom Kirk unburdens himself and is a foil to Spock.<sup>[9]</sup> Robert Jewett and John Shelton Lawrence's <i>The Myth of the American Superhero</i> describes Kirk as "a hard-driving leader who pushes himself and his crew beyond human limits".<sup>[10]</sup> Terry J. Erdman and Paula M. Block, in their <i>Star Trek 101 primer</i>, note that while "cunning, courageous and confident", Kirk also has a "tendency to ignore Starfleet regulations when he feels the end justifies the means"; he is "the quintessential officer, a man among men and a hero for the ages".<sup>[11]</sup></p> | <table border="1"> <thead> <tr> <th>Nickname</th> <th>Jim</th> <th>Appearance</th> </tr> </thead> <tbody> <tr> <td>Title</td> <td>Cadet<br/>Ensign<br/>Lieutenant<br/>Commander<br/>Captain<br/>Admiral</td> <td><small>Text</small><br/><input type="radio"/> Small<br/><input checked="" type="radio"/> Standard<br/><input type="radio"/> Large</td> </tr> <tr> <td>Position</td> <td>Chief of Starfleet Operations<br/><i>USS Enterprise</i>:<br/>Commanding officer<br/><i>USS Enterprise-A</i>:<br/>Commanding officer</td> <td><small>Width</small><br/><input checked="" type="radio"/> Standard<br/><input type="radio"/> Wide</td> </tr> <tr> <td>Affiliation</td> <td>United Federation of Planets<br/>Starfleet</td> <td><small>Color (beta)</small><br/><input type="radio"/> Automatic<br/><input checked="" type="radio"/> Light<br/><input type="radio"/> Dark</td> </tr> <tr> <td>Family</td> <td>George Samuel Kirk Sr.<br/>(father)<br/>Winona Kirk (mother)<br/>George Samuel Kirk Jr.<br/>(brother)<br/>Tiberius Kirk (grandfather)<br/>James (maternal grandfather)<br/>Aurelan Kirk (sister-in-law)<br/>Peter Kirk (nephew)<br/>2 other nephews</td> <td></td> </tr> <tr> <td>Children</td> <td>David Marcus</td> <td></td> </tr> <tr> <td>Origin</td> <td>Iowa, United States, Earth</td> <td></td> </tr> </tbody> </table> | Nickname | Jim | Appearance | Title | Cadet<br>Ensign<br>Lieutenant<br>Commander<br>Captain<br>Admiral | <small>Text</small><br><input type="radio"/> Small<br><input checked="" type="radio"/> Standard<br><input type="radio"/> Large | Position | Chief of Starfleet Operations<br><i>USS Enterprise</i> :<br>Commanding officer<br><i>USS Enterprise-A</i> :<br>Commanding officer | <small>Width</small><br><input checked="" type="radio"/> Standard<br><input type="radio"/> Wide | Affiliation | United Federation of Planets<br>Starfleet | <small>Color (beta)</small><br><input type="radio"/> Automatic<br><input checked="" type="radio"/> Light<br><input type="radio"/> Dark | Family | George Samuel Kirk Sr.<br>(father)<br>Winona Kirk (mother)<br>George Samuel Kirk Jr.<br>(brother)<br>Tiberius Kirk (grandfather)<br>James (maternal grandfather)<br>Aurelan Kirk (sister-in-law)<br>Peter Kirk (nephew)<br>2 other nephews |  | Children | David Marcus |  | Origin | Iowa, United States, Earth |  |
|---|---|---|----------|-----|------------|-------|--|--|----------|---|---|-------------|---|--|--------|--|--|----------|--------------|--|--------|----------------------------|--|
| Nickname  | Jim   | Appearance  |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Title   | Cadet<br>Ensign<br>Lieutenant<br>Commander<br>Captain<br>Admiral  | <small>Text</small><br><input type="radio"/> Small<br><input checked="" type="radio"/> Standard<br><input type="radio"/> Large  |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Position  | Chief of Starfleet Operations<br><i>USS Enterprise</i> :<br>Commanding officer<br><i>USS Enterprise-A</i> :<br>Commanding officer   | <small>Width</small><br><input checked="" type="radio"/> Standard<br><input type="radio"/> Wide   |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Affiliation   | United Federation of Planets<br>Starfleet   | <small>Color (beta)</small><br><input type="radio"/> Automatic<br><input checked="" type="radio"/> Light<br><input type="radio"/> Dark  |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Family  | George Samuel Kirk Sr.<br>(father)<br>Winona Kirk (mother)<br>George Samuel Kirk Jr.<br>(brother)<br>Tiberius Kirk (grandfather)<br>James (maternal grandfather)<br>Aurelan Kirk (sister-in-law)<br>Peter Kirk (nephew)<br>2 other nephews  |   |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Children  | David Marcus  |   |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |
| Origin  | Iowa, United States, Earth  |   |          |     |            |       |  |  |          |   |   |             |   |  |        |  |  |          |              |  |        |                            |  |

Although Kirk throughout the series becomes romantically involved with various women, when confronted with a choice between a



Burp Suite Community Edition v2025.10.3 - Temporary Project

Intruder tab selected. Target set to http://localhost:3000. Payload type is Simple list with 10 items.

Request 1 (POST /rest/user/reset-password):

```
1 POST /rest/user/reset-password HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 74
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-us: "Not A Brand";v="99", "Chromium";v="142"
8 Content-Type: application/json
9 sec-ch-ua-mobile: ?0
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/login
16 Accept-Encoding: gzip, deflate, br
17 Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss
18 Connection: keep-alive
19
20 {"email":"jim@juice-sh.op", "answer":"$names", "new":"osman", "repeat":"osman"}
```

3. Intruder attack of http://localhost:3000

Results tab selected. Filtered results for Request 2 (Status 200 OK).

| Request | Response | Response received | Error | Timeout | Length |
|---------|----------|-------------------|-------|---------|--------|
| 2       | 200 OK   | 24                |       |         | 508    |
| 0       | 401      | 41                |       |         | 503    |
| 1       | 401      | 37                |       |         | 503    |
| 3       | 401      | 41                |       |         | 503    |
| 4       | 401      | 12                |       |         | 503    |
| 5       | 401      | 14                |       |         | 503    |
| 6       | 401      | 11                |       |         | 503    |
| 7       | 401      | 10                |       |         | 503    |

The answer of security question is: **Samuel**

New Password is : **osman**

OWASP Juice Shop login page. Jim's password was successfully changed.

Login page shows Jim's credentials: Email: jim@juice-sh.op, Password: osman.

User profile shows Jim's account information: Name: jim@juice-sh.op, Order & Payment, Privacy & Security, Logout.

## Impact:

- Full compromise of victim user accounts
  - Unauthorized access to personal or sensitive information
  - Ability to perform actions on behalf of the victim
  - Potential privilege escalation if admin or high-privilege accounts are taken over
  - Fraud, data manipulation, or deletion of user data
  - Loss of trust and severe security implications for the system
- 

## Recommendation:

- Strengthen authentication mechanisms (secure password reset, MFA, token validation)
- Enforce strict access control checks on all user actions
- Implement rate limiting and brute force protection
- Use email or phone verification when resetting passwords
- Encrypt and securely store credentials
- Monitor suspicious login behavior and notify users of unusual activity
- Implement secure session management and invalidate old sessions

## 5.3 Broken Access Control:

## **Definition:**

Broken Access Control happens when an application does not correctly enforce user permissions, allowing attackers to access or modify data they shouldn't be able to.

## Types:

- **Horizontal Privilege Escalation:** Occurs when a user can perform an action or access data of another user with the same level of permissions.
  - **Vertical Privilege Escalation:** Occurs when a user can perform an action or access data of another user with a higher level of permissions.

## Risk Level: High

**Description:** data can be accessed without proper authorization check

# Proof of Concept for Vertical Broken Access Control:

The screenshot shows a browser window for the OWASP Juice Shop application. The URL bar displays `http://localhost:3000/#/`. The page title is "OWASP Juice Shop". The navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. Below the title, there's a navigation menu with "Inspector" selected, followed by "Console", "Debugger", "Network", "Style Editor", "Performance", "Memory", "Storage", "Accessibility", and "Application". The "Sources" tab is active, showing a list of JavaScript files: "Main Thread", "cdnjs.cloudflare.com", "localhost:3000", "main.js", "polyfills.js", "runtime.js", and "vendor.js". The "main.js" file is currently being viewed, with its content displayed in the main pane. A red box highlights the word "administration" in the code, which is part of a component definition: `"administration", component: rr, canActivate: [ee], {path: "accounting", component: jl, canActivate: [ee]}`.



The screenshot shows the OWASP Juice Shop application's administration interface. At the top, there is a navigation bar with links like OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. Below the navigation is the OWASP Juice Shop logo and a search bar. A green success message box says "You successfully solved a challenge: Admin Section (Access the administration section of the store.)". The main content area has two sections: "Registered Users" and "Customer Feedback". Under "Registered Users", there are two entries: "admin@juice-sh.op" and "jim@juice-sh.op". Under "Customer Feedback", there are two reviews: "I love this shop! Best products in town! Highly recommended! (\*\*\*\*in@juice-sh.op)" with a 5-star rating, and "Great shop! Awesome service! (\*\*\*@juice-sh.op)" with a 3-star rating.

## Proof of Concept for Horizontal Broken Access Control:

The screenshot shows the OWASP Juice Shop application's basket page. The user is logged in as "admin@juice-sh.op". The basket contains three items: Apple Juice (1000ml), Orange Juice (1000ml), and Eggfruit Juice (500ml). The total price is 21.94. A red box highlights the basket content. In the top right corner, the user's account information is shown: "admin@juice-sh.op", "Orders & Payment", "Privacy & Security", and "Logout".

The screenshot shows the developer tools' Application tab. The "Storage" section is expanded, and the "Session storage" item is selected. A red box highlights the "Value" input field, which contains the value "1". The URL in the address bar is "localhost:3000/#/basket". The developer tools also show tabs for Manifest, Service workers, Storage, Memory, Application (which is selected), Privacy and security, Lighthouse, Recorder, and DOM Invader.

The screenshot shows a browser developer tools interface with the OWASP Juice Shop application. A red box highlights the session storage entry for the key 'bid' with the value '3'. This indicates a session fixation vulnerability where the user's session ID is leaked.

| Key | Value |
|-----|-------|
| bid | 3     |

## Impact:

- Leakage of all users' data
- Privilege escalation

## Recommendation:

- Implement server-side access control
- Validate user roles on every request

## 5.4 Logic Vulnerability:

### Definition:

A Logic Vulnerability occurs when the application's business rules are incorrectly implemented, allowing users to perform actions that violate the intended workflow or financial logic of the system.

### Risk Level: High

### Affected Functionality:

/api/BasketItems

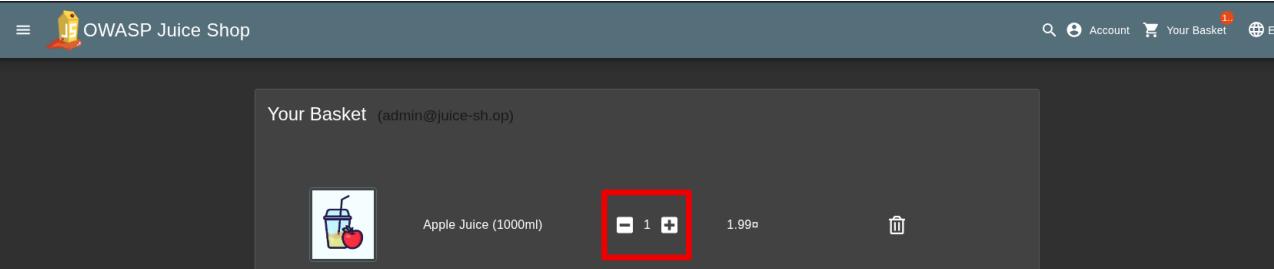
### Description:

The application contains a business logic flaw that allows users to purchase multiple products while the total price is calculated as zero. Due to improper validation of pricing rules, the system fails to enforce the correct calculation of product costs during checkout. As a result, an attacker can exploit this flaw to obtain items without paying, bypassing the intended purchasing logic.



## Proof of Concept:

# Cannot decrease item counter to 0



The screenshot shows the OWASP Juice Shop application's basket page. The basket contains three items: Apple Juice (1000ml), Orange Juice (1000ml), and Eggfruit Juice (500ml). Each item has a quantity selector with minus and plus buttons. The total price is displayed as 70.88¤. The entire basket section is highlighted with a red box.

| Item                   | Quantity | Unit Price |
|------------------------|----------|------------|
| Apple Juice (1000ml)   | 1        | 1.99¤      |
| Orange Juice (1000ml)  | 5        | 2.99¤      |
| Eggfruit Juice (500ml) | 6        | 8.99¤      |

Total Price: 70.88¤

| Request   | Response  |
|---|---|
| Pretty Raw Hex  | Pretty Raw Hex Render   |
| 5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNLcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluOGplaWNlXNoLm9iIiwiicGFzc3dvcnQiOiIwMTkyMDIzYTd1yQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbhV4ZVRva2VujoiiIiwbGFzExvZLlsuXSAoiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOihc3NLdHMvchVibGljL2ltYWdlcy91cGxvYWRzl2RLzrMfBHRBZGlpbi5wbmcilCj0b3RwU2VjcmVOIjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTETMjIgMtGMD06MjQUmjM4ICSwDwMCIsInVzZGF0ZWRBdCI6IjIwMjUtMTETMjIgMtGNDI6MTAUUmzcIcswDwMCIsImRlbGV0ZWRBdCI6bnVsbhOsImLhdCI6MTC2MzgznzcyMn0.QNemQVIuyxMX5kecGvqrKQQW-QyEwmJPkfHqd1N16eMhGPySZ9n2ECVHjij00_mwRDMUc31xsX22Flk_birCrn_-8PJ3oXvK3hy9kaVXSzb-GSR3vKmqDAM1FqaqLjeob0v35btDsFYsqTSt-Dg9FB8CLW24NS5eDDU0nzduQ  | 1 HTTP/1.1 200 OK   |
| 6 Accept-Language: en-US,en;q=0.9   | 2 Access-Control-Allow-Origin: *  |
| 7 sec-ch-ua: "Not_A_Brand";v="99", "Chromium";v="142"   | 3 X-Content-Type-Options: nosniff   |
| 8 sec-ch-ua-mobile: ?0  | 4 X-FRAME-OPTIONS: SAMEORIGIN   |
| 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36   | 5 Feature-Policy: payment 'self'  |
| 10 Accept: application/json, text/plain, */*  | 6 X-Rewriting-URI: /#/jobs  |
| 11 Content-Type: application/json   | 7 Content-Type: application/json; charset=utf-8   |
| 12 Origin: http://localhost:3000  | 8 Content-Length: 154   |
| 13 Sec-Fetch-Site: same-origin  | 9 ETag: "W/9a-3EE1z9iRPGe0fSg1NpNqxFIFxs"   |
| 14 Sec-Fetch-Mode: cors   | 10 Vary: Accept-Encoding  |
| 15 Sec-Fetch-Dest: empty  | 11 Date: Sat, 22 Nov 2025 20:29:48 GMT  |
| 16 Referer: http://localhost:3000/  | 12 Connection: keep-alive   |
| 17 Accept-Encoding: gzip, deflate, br   | 13 Keep-Alive: timeout=5  |
| 18 Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; token=<br>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNLcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluOGplaWNlXNoLm9iIiwiicGFzc3dvcnQiOiIwMTkyMDIzYTd1yQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbhV4ZVRva2VujoiiIiwbGFzExvZLlsuXSAoiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOihc3NLdHMvchVibGljL2ltYWdlcy91cGxvYWRzl2RLzrMfBHRBZGlpbi5wbmcilCj0b3RwU2VjcmVOIjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTETMjIgMtGMD06MjQUmjM4ICSwDwMCIsInVzZGF0ZWRBdCI6IjIwMjUtMTETMjIgMtGNDI6MTAUUmzcIcswDwMCIsImRlbGV0ZWRBdCI6bnVsbhOsImLhdCI6MTC2MzgznzcyMn0.QNemQVIuyxMX5kecGvqrKQQW-QyEwmJPkfHqd1N16eMhGPySZ9n2ECVHjij00_mwRDMUc31xsX22Flk_birCrn_-8PJ3oXvK3hy9kaVXSzb-GSR3vKmqDAM1FqaqLjeob0v35btDsFYsqTSt-Dg9FB8CLW24NS5eDDU0nzduQ;<br>continueCode=4npLe0) VbPWE6397zdLt vfkDuekIBghY1SqBcoLoWvBzgJlaQqk2voXKnMr | 14 {<br>"status": "success",<br>"data": {<br>"ProductId": 1,<br>"BasketId": 1,<br>"id": 1,<br>"quantity": 0,<br>"createdAt": "2025-11-22T18:04:25.701Z",<br>"updatedAt": "2025-11-22T20:29:48.636Z"<br>}<br>} |
| 19 Connection:keep-alive  | 20  |
| 21 {<br>"quantity": 0<br>}  |   |



## Now item counter is 0 and decrease total price

Your Basket (admin@juice-sh.op)

| Item                   | Quantity | Price         |
|------------------------|----------|---------------|
| Apple Juice (1000ml)   | 0        | 1.99€         |
| Orange Juice (1000ml)  | 5        | 2.99€         |
| Eggfruit Juice (500ml) | 6        | 8.99€         |
| <b>Total Price:</b>    |          | <b>68.89€</b> |

Checkout

You will gain 6 Bonus Points from this order!

Burp Suite Community Edition v2025.10.3 - Temporary Project

Repeater

Request

Pretty Raw Hex

Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MSwidXNlcmShbWUiOiiLiLCJlbWFpbCI6ImFkbWluQGplaWNlLXNoLm9wIiwigFzc3dvcmoIoiwMTkyMDIzYtdiYmQ3MzI1MDUxNmYwNjkzjE4YjUwMCIsInJvbGUoiJhZGlpbiisImRlbHV4ZVRva2VuIjoiIwibGFzdExvZ2luXSXaiOixMjcuMC4wLjEiLCJwcmaWxlSW1hZ2UiOihc3NLdhMvchVibGljL2ltYwdlc91cGxvYWRzl2RLzFlfbHRBZGlpb15wbmc1LCJ0b3RwU2VjcmVOijoiiwiiaXNBY3RpdmUiOnRydWUsImNyZWFOZWRBdCI6ijIwMjUtMTETMjIgMTg6MD06MjQuMjM41CswMDovMCIsInWzGF0ZWRBdCI6IjIwMjUtMTETMjIgMTg6NDI6MTAuMzc1CswMDowMCIsimRlbGV0ZWRBdCI6bnVsboHosImlhdcIGMTc2MzgznzcyMn0.QNmQVIuyxMXSkEcGVqrKQGw-QyEWmJPyKfmHqd1NM16emHgPySZ9n2ECVhjij00\_mwRDMUc3lxsX22F1k\_birCn\_-8PJ3oXvk3hy9kaVXszb-GSR3vkMqDAM1FqaqljeOb0v35BtDsFYsqTSt-Dg9FB8CLW24NS5eDDU8nzdu0;

Accept-Language: en-US,en;q=0.9

sec-ch-ua: "Not\_A\_Brand";v="99", "Chromium";v="142"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36

Accept: application/json, text/plain, \*/\*

Content-Type: application/json

Origin: http://localhost:3000

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: http://localhost:3000/

Accept-Encoding: gzip, deflate, br

Cookie: language=en; cookieconsent\_status=dismiss; welcomebanner\_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MSwidXNlcmShbWUiOiiLiLCJlbWFpbCI6ImFkbWluQGplaWNlLXNoLm9wIiwigFzc3dvcmoIoiwMTkyMDIzYtdiYmQ3MzI1MDUxNmYwNjkzjE4YjUwMCIsInJvbGUoiJhZGlpbiisImRlbHV4ZVRva2VuIjoiIwibGFzdExvZ2luXSXaiOixMjcuMC4wLjEiLCJwcmaWxlSW1hZ2UiOihc3NLdhMvchVibGljL2ltYwdlc91cGxvYWRzl2RLzFlfbHRBZGlpb15wbmc1LCJ0b3RwU2VjcmVOijoiiwiiaXNBY3RpdmUiOnRydWUsImNyZWFOZWRBdCI6ijIwMjUtMTETMjIgMTg6MD06MjQuMjM41CswMDovMCIsInWzGF0ZWRBdCI6IjIwMjUtMTETMjIgMTg6NDI6MTAuMzc1CswMDowMCIsimRlbGV0ZWRBdCI6bnVsboHosImlhdcIGMTc2MzgznzcyMn0.QNmQVIuyxMXSkEcGVqrKQGw-QyEWmJPyKfmHqd1NM16emHgPySZ9n2ECVhjij00\_mwRDMUc3lxsX22F1k\_birCn\_-8PJ3oXvk3hy9kaVXszb-GSR3vkMqDAM1FqaqljeOb0v35BtDsFYsqTSt-Dg9FB8CLW24NS5eDDU8nzdu0; continueCode=4npLe0jVbPWEy6397zdLtvfkDuekIBghY1s9Bcol0wBZgJlaQqk2voXKNmr

Connection:...keep-alive

21 {  
 "quantity": -100  
}

Response

Pretty Raw Hex Render

HTTP/1.1 200 OK

Access-Control-Allow-Origin: \*

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Feature-Policy: payment 'self'

X-Recruiting: /#/jobs

Content-Type: application/json; charset=utf-8

Content-Length: 157

ETag: W:/d-1ULX1gk12X4GrhHdmq0oY7MJU"

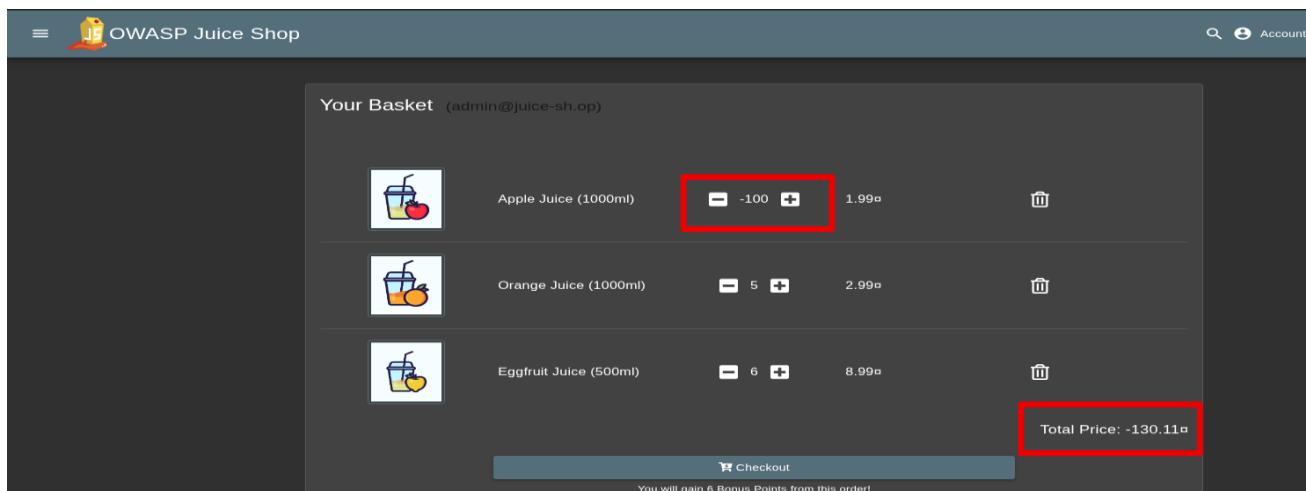
Vary: Accept-Encoding

Date: Sat, 22 Nov 2025 20:33:59 GMT

Connection: keep-alive

Keep-Alive: timeout=5

15 {  
 "status": "success",  
 "data": {  
 "ProductId": 1,  
 "BasketId": 1,  
 "id": 1,  
 "quantity": -100,  
 "createdAt": "2025-11-22T18:04:25.701Z",  
 "updatedAt": "2025-11-22T20:38:59.877Z"  
 }  
}



Your Basket (admin@juice-sh.op)

| Item                   | Quantity | Unit Price | Total Price     |
|------------------------|----------|------------|-----------------|
| Apple Juice (1000ml)   | -100     | 1.99€      | -199.00€        |
| Orange Juice (1000ml)  | 5        | 2.99€      | 14.95€          |
| Eggfruit Juice (500ml) | 6        | 8.99€      | 53.94€          |
| <b>Total Price:</b>    |          |            | <b>-130.11€</b> |

Checkout  
You will gain 6 Bonus Points from this order!

## Impact:

- Allows attackers to complete orders with a total price of 0
- Direct financial loss to the system
- Bypasses core business rules and integrity
- Enables abuse of the e-commerce workflow
- Potential large-scale exploitation by automated scripts
- Loss of trust in the platform's payment system

## Recommendation:

- Recalculate product prices exclusively on the server side
- Do not trust any price or quantity values sent from the client
- Implement server-side validation for: item price , total cost , discounts, quantity
- Enforce integrity checks during checkout
- Ensure no order can be completed unless total price > 0
- Log and monitor suspicious discount or price manipulation behavior
- Add automated tests to validate business rules

## 5.5 Cross-Site Scripting (XSS):

### Definition:

Cross-Site Scripting (XSS) is a vulnerability that allows attackers to inject malicious JavaScript into a web page viewed by other users.

**Risk Level:** Medium

### Types:

- **Dom**: Occurs when the malicious payload is executed entirely on the client side because the JavaScript code modifies the DOM without proper sanitization. The server is not involved in reflecting or storing the payload.
- **Stord** : Occurs when the attacker's payload is permanently stored on the server (e.g., in a database, comment, review, feedback). The script executes when any user views the infected content.
- **Reflect** : Occurs when the malicious input is immediately reflected by the server in the response (usually via URL parameters) without being stored. It executes when the victim clicks a crafted link.

## Proof of Concept:

Payload : <iframe src="javascript:alert('xss')">

The screenshot shows a browser window with two tabs: 'Wigger' and 'OWASP Juice Shop'. The URL in the address bar is 'localhost:3000/#/search?q=<iframe%20src%3D'javascript:alert(%60osman%60)%3E%20'. A red box highlights the address bar. Another red box highlights a modal dialog box in the center of the page that says 'localhost:3000 says osman' with an 'OK' button. Below the search bar, there is a placeholder 'Search Results -'.

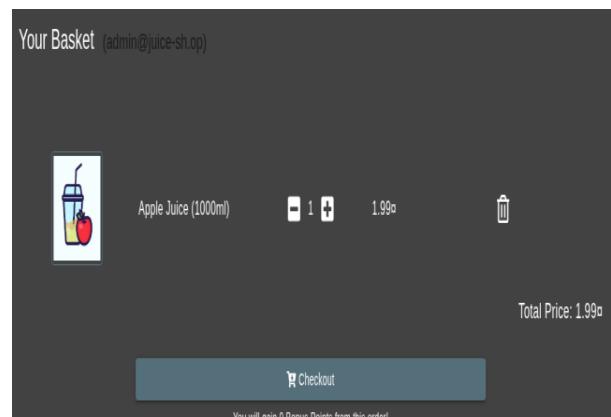
## Payload 2:

Steps: Place order and track order

1



2



3

A form for selecting an address. It shows a radio button next to 'Administrator', an address field with '0815 Test Street, Test, Test, 4711', and a name field with 'Test'. At the bottom are 'Add New Address' and 'Continue' buttons.

4

**Delivery Address**

Administrator  
0815 Test Street, Test, Test, 4711  
Test  
Phone Number 1234567890

**Choose a delivery speed**

|   | Price | Expected Delivery |
|---|-------|-------------------|
| <input checked="" type="radio"/> One Day Delivery | 0.99¤ | 1 Days            |
| <input type="radio"/> Fast Delivery               | 0.50¤ | 3 Days            |
| <input type="radio"/> Standard Delivery           | 0.00¤ | 5 Days            |

[Back](#) [Continue](#)

5

**My Payment Options**

|   |               |        |
|---|---------------|--------|
| <input checked="" type="radio"/> ****4368 | Administrator | 2/2081 |
| <input type="radio"/> *****8108           | Administrator | 4/2086 |

Add new card Add a credit or debit card

Pay using wallet **Wallet Balance 1.00** [Pay 2.98¤](#)

Add a coupon Add a coupon code to receive discounts

Other payment options

[Back](#) [Continue](#)

6

OWASP Juice Shop

**Delivery Address**  
Administrator  
0815 Test Street, Test, Test, 4711  
Test  
Phone Number 1234567890

**Payment Method**  
Card ending in 4368  
Card Holder\* Administrator

**Your Basket** (admin@juice-sh.op)

|  |                      |   |       |
|--|----------------------|---|-------|
|  | Apple Juice (1000ml) | 1 | 1.99¤ |
|--|----------------------|---|-------|

**Order Summary**

- Items
- Delivery
- Promotion
- Total Price**

[Place your order and pay](#)  
You will gain 0 Bonus Points from this order!

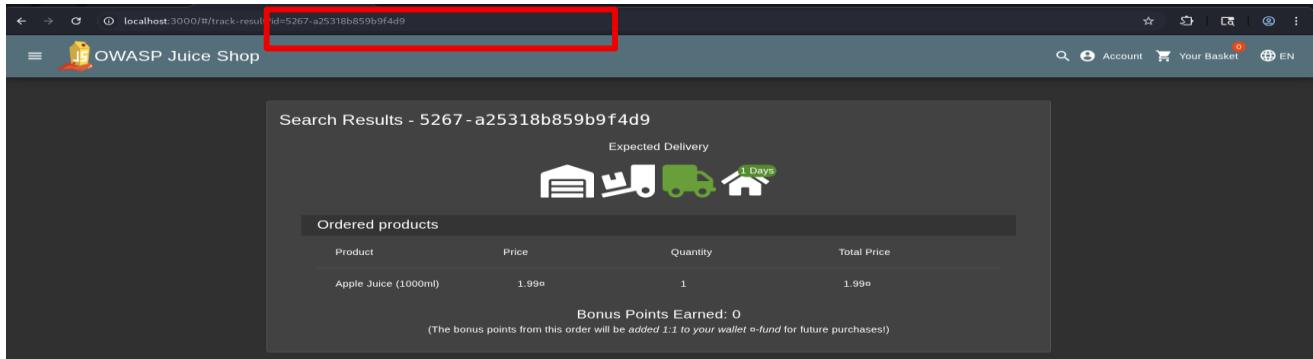
[Order History](#) [Recycle](#) [My saved addresses](#) [My Payment Options](#) [Digital Wallet](#)

[Logout](#)

7

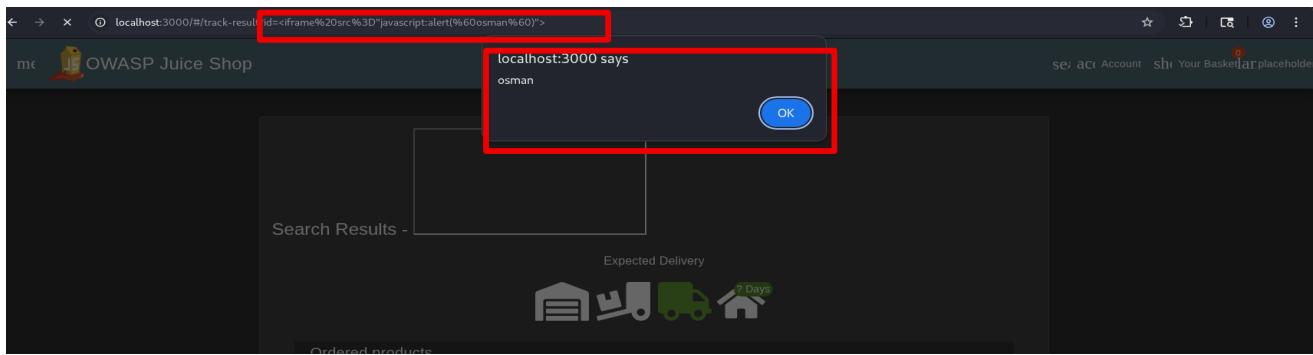
**Order History**

| Order ID               | Total Price | Bonus    | In Transit  |  |
|------------------------|-------------|----------|-------------|--|
| #5267-a25318b859b9f4d9 | 2.98¤       | 0        |             |  |
| Product                | Price       | Quantity | Total Price |  |
| Apple Juice (1000ml)   | 1.99¤       | 1        | 1.99¤       |  |



Now affected parameter is: /track-result?id=

<iframe src="javascript:alert('xss')">



## XSS Impact :

- Theft of user session cookies leading to account takeover.
- Execution of malicious JavaScript in the victim's browser.
- Performing unauthorized actions on behalf of the user.
- Redirecting users to phishing or malicious websites.
- Stealing sensitive data and form inputs (keylogging).
- Defacing pages or injecting unwanted content.
- Potential spread of stored XSS as a self-propagating worm.

### **Recommendations:**

- Validate and sanitize all user inputs using a whitelist approach
- Encode user-supplied data before rendering it in the browser (output encoding).



## Payload 3:

The screenshot shows a dark-themed web interface for the OWASP Juice Shop. A user menu is open, displaying several options: 'admin@juice-sh.op', 'Orders & Payment', 'Privacy Policy', 'Privacy & Security' (which is highlighted with a red box), 'Request Data Export', 'Request Data Erasure', 'Change Password', 'Logout', and '+2 2FA Configuration'. Below the menu, there's a product listing for 'Banana Juice (1000ml)' with a price of '1.99'. At the bottom of the page, a section titled 'Last Login IP' is also highlighted with a red box.

This screenshot shows the Burp Suite interface. The 'Proxy' tab is selected, displaying a list of network requests. One request to 'http://localhost:3000/rest/saveLoginIp' is selected. The 'Inspector' tool is open, showing the 'Headers' tab with various fields like Host, User-Agent, and Sec-Fetch-Site. A specific cookie entry for 'If-None-Match' is highlighted with a red box. The 'Value' field for this cookie contains the value 'W/"158-YsQ4-d8SqN+m3YBcfetkw93c"'. A payload for this cookie is being edited in the 'Value' field, starting with '<iframe src="javascript:alert(`xss`)">'.

This screenshot shows a browser window with a confirmation dialog. The dialog text reads 'localhost:3000 says XSS' and has an 'OK' button. The entire dialog is highlighted with a red box. The background shows the OWASP Juice Shop application with a form for entering an IP address.

## 5.6 Sensitive Data Exposure

### Definition:

Sensitive Data Exposure occurs when an application accidentally reveals confidential information due to weak protections or misconfigurations.

**Risk Level:** Medium

**Affected File:** /ftp directory

### Description:

The application exposes backup files containing sensitive information

```
~ / ftp
├── quarantine
├── coupons_2013.md.bak
├── incident-support.kdbx
├── order_5267-a25318b859b9f4d9.pdf
└── suspicious_errors.yml

      └── acquisitions.md
      ├── eastere.gg
      ├── legal.md
      └── package-lock.json.bak

      └── announcement_encrypted.md
      ├── encrypt.pyc
      └── order_5267-0f8563ccc551dedd.pdf

      └── package.json.bak
```

## 5.7 Cross-Site Request Forgery (CSRF)

### **Definition:**

Cross-Site Request Forgery (CSRF) is a vulnerability that allows an attacker to force a logged-in user to perform unintended actions within a web application. Because browsers automatically include cookies in outgoing requests, the server mistakenly believes the action was performed intentionally by the victim.

**Risk Level:** Medium

**Affected Endpoint:** POST <http://localhost:3000/profile>

### **Description:**

The profile update functionality in the application is vulnerable to CSRF due to the absence of essential protection mechanisms such as:

- No Anti-CSRF token validation
- No verification of request origin
- Reliance solely on session cookies for authentication

This allows an attacker to host a malicious HTML page that automatically sends a crafted POST request. When the victim-while logged into the Website visits the page, the request is executed using their session, resulting in changing the username without their consent.



## Proof of Concept:

The screenshot shows the OWASP Juice Shop login interface. The URL in the browser is `localhost:3000/#/login`. The page features a dark-themed login form. The 'Email\*' field contains the value `mm@mail.com`. The 'Password\*' field contains the value `*****`. Below the fields are links for 'Forgot your password?' and 'Log in'. A 'Remember me' checkbox is present, and a 'Log in with Google' button is available.

Logging in with a normal user account

The screenshot shows the OWASP Juice Shop User Profile page. The URL in the browser is `localhost:3000/profile`. The page displays a user profile with a placeholder profile picture. The 'User Profile' section contains fields for 'Email' (value: `mm@mail.com`) and 'Username' (value: `depi`, highlighted with a red border). A 'Set Username' button is next to the username field. Below the profile section is a 'File Upload' area with a 'Choose File' button and a message indicating 'No file chosen'. There is also a 'Upload Picture' button.



Burp Suite Community Edition v2025.3.4 - Temporary Project

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to http://localhost:3000 [127.0.0.1] Open browser

| Time            | Type | Direction | Method | URL                           | Status code | Length |
|-----------------|------|-----------|--------|-------------------------------|-------------|--------|
| 12:50:56 26 Nov | HTTP | → Request | POST   | http://localhost:3000/profile |             |        |

**Request**

Pretty Raw Hex

```
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en
16 Cache-Control: no-store
17 Content-Type: application/x-www-form-urlencoded
18 Sec-Fetch-Mode: navigate
19 Sec-Fetch-User: -1
20 Referer: http://localhost:3000/profile
21 
```

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

1390

1391

1392

1393

1394

1395

1396

1397

1398

1399

1400

1401

1402

1403

1404

1405

1406

1407

1408

1409

1410

1411

1412

1413

1414

1415

1416

1417

1418

1419

1420

1421

1422

1423

1424

1425

1426

1427

1428

1429

1430

1431

1432

1433

1434

1435

1436

1437

1438

1439

1440

1441

1442

1443

1444

1445

1446

1447

1448

1449

1450

1451

1452

1453

1454

1455

1456

1457

1458

1459

1460

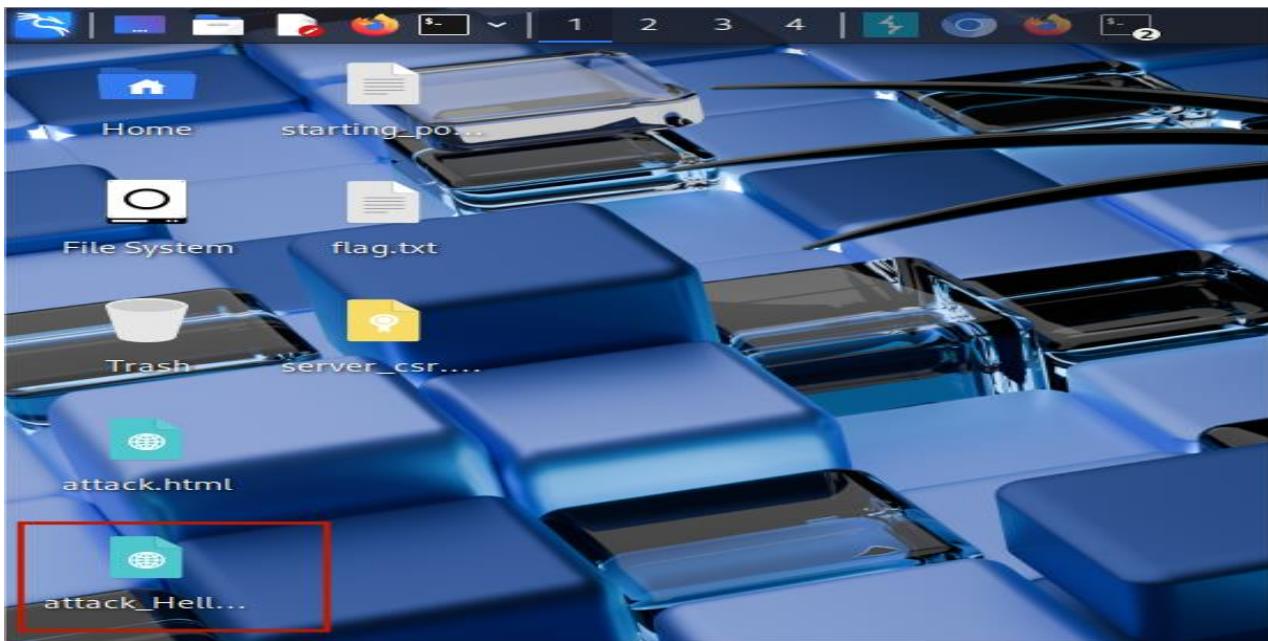
1461

1462

1463

<p

## Intercepted POST Request Showing Vulnerable Parameters



## CSRF Attack HTML File Prepared on the Attacker's Machine



The screenshot shows a code editor window with a dark theme. The title bar says "File Edit Selection View Go Run ...". A message at the top left says "Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More". The main area contains the following code:

```
1 <html>
2 <body>
3 <form action="http://localhost:3000/profile" method="POST">
4   <input type="hidden" name="username" value="HelloFromDepi" />
5 </form>
6 <script>
7   document.forms[0].submit();
8 </script>
9 </body>
10 </html>
11
12
13
```

The line "value="HelloFromDepi"" is highlighted with a red box.

The screenshot shows a web browser window with the URL "localhost:3000/profile". The page title is "User Profile". It displays a placeholder image of a hooded figure and a form with the following fields:

- Email: admin@juice-sh.op
- Username: HelloFromDepi (highlighted with a red box)

A blue button labeled "Set Username" is visible below the form. The browser's address bar shows "localhost:3000/profile".

Username Successfully Modified via CSRF



## Impact:

- Unauthorized modification of user profile data
- Ability to perform actions on behalf of the victim
- Potential escalation to account takeover if sensitive endpoints are affected
- Increased risk when combined with social engineering attacks
- Loss of integrity and trust in the application

## Recommendations:

- Implement server-side **Anti-CSRF tokens** on all state-changing requests
- Use **SameSite=Strict** cookies to prevent cross-site cookie submission
- Validate **Origin** and **Referer** headers
- Restrict CORS to trusted domains only
- Implement CSRF protection middleware
- Reject requests missing CSRF tokens or valid origins