

OWASP Juice Shop Pentesting Report

OWASP Juice-shop is an interactive vulnerable platform where entry-level pentesters can apply their skills and knowledge **and put theory into practice**.

The first step is to install Node.js and npm. This allow access the site whenever needed.

1. Install Node.js and npm via the terminal

```
| sudo apt install nodejs npm
```

2. Clone Juice-shop from GitHub

```
| git clone https://github.com/juice-shop/juice-shop.git
```

3. Navigate to the Juice-shop directory

```
| cd juice-shop
```

4. Install project dependencies

```
| npm install
```

5. Start the Juice Shop application

```
| npm start
```

6. Open the site in a browser on port 3000

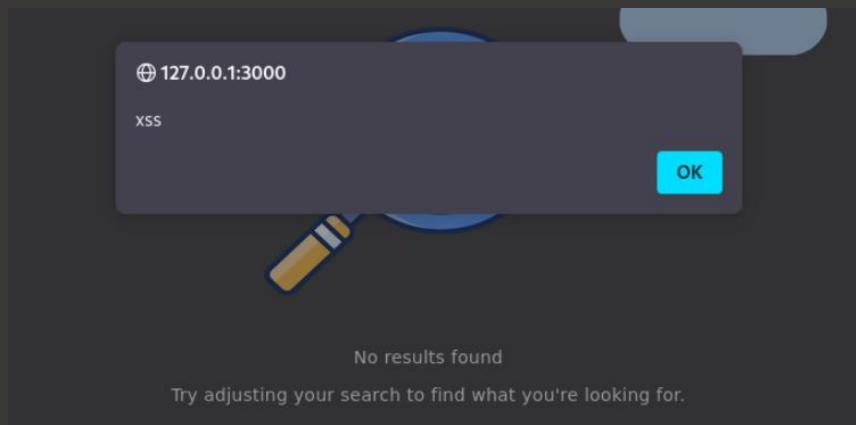
```
| http://127.0.0.1:3000/
```

1. XSS Injection

XSS (Cross-Site Scripting) is a web-security that allows an attacker to inject malicious scripts into trusted websites.

To determine whether the site is vulnerable to XSS injection we can use the search field. For this we enter <h1>owasp. If the input is rendered without sanitization, it indicates that the site does not properly resist XSS attacks. Therefore, we can use the following script:

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



As a result we can observe the following changes in the address bar:

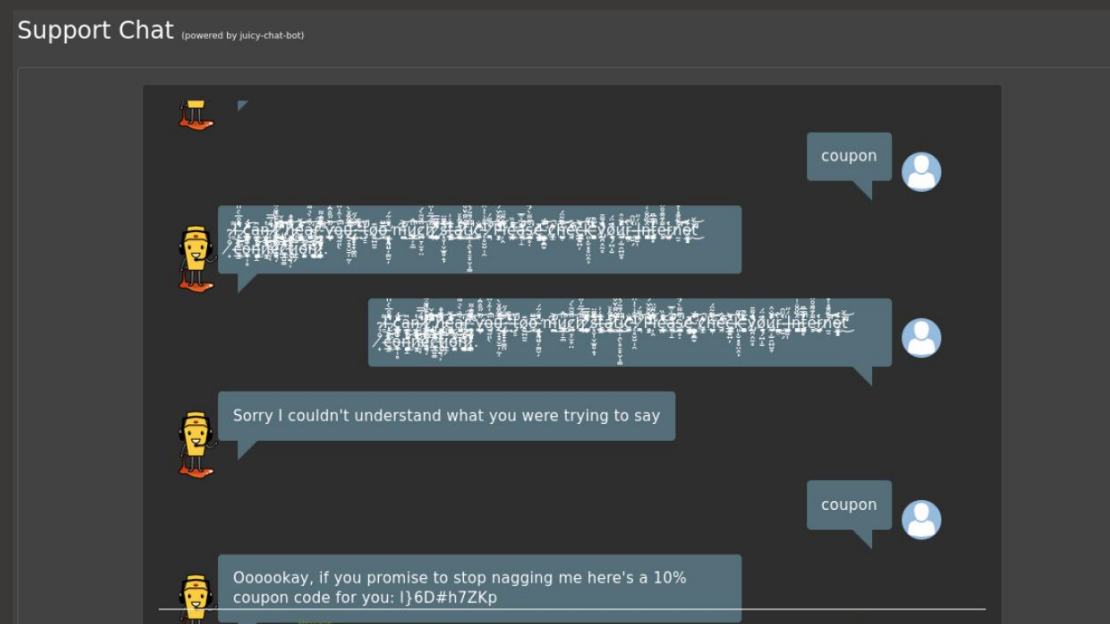
```
| 127.0.0.1:3000/#/search?q=<iframe src%3D"javascript:alert('xss')">
```

This vulnerability represents a reflected XSS attack, as the injected payload is immediately returned in the server response. The application does not properly sanitize or encode user input before rendering it in the response.

2. Brute Force chatbot Attack

Bruteforce is a trial-and-error method that involves repeated attempts to obtain information by systematically testing multiple inputs.

By applying this method while interacting with the site's chatbot, we can obtain the following results:



In this case, the chatbot does not implement any rate limiting or protection mechanisms such as CAPTCHA or request throttling. By repeatedly sending messages to the chatbot, it is possible to trigger predefined responses and extract information without any restrictions.

This behavior indicates insufficient protection against automated or repeated interactions.

3. Searching for hidden directories

Directory enumeration is a technique used to discover hidden or unlisted directories on a web server.

For this purpose, we can use the powerful utility dirb.

```
| dirb http://127.0.0.1:3000 -f
```

```
(vbox@vbox)-[~/Downloads/juice-shop]
$ dirb http://127.0.0.1:3000 -f

DIRB v2.22
By The Dark Raver

START_TIME: Thu Dec  4 16:45:22 2025
URL_BASE: http://127.0.0.1:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tuning of NOT_FOUND detection

GENERATED WORDS: 4612

— Scanning URL: http://127.0.0.1:3000/ —
+ http://127.0.0.1:3000/assets (CODE:301|SIZE:156)
+ http://127.0.0.1:3000/ftp (CODE:200|SIZE:941)
+ http://127.0.0.1:3000/profile (CODE:500|SIZE:1061)
+ http://127.0.0.1:3000/promotion (CODE:200|SIZE:692)
+ http://127.0.0.1:3000/redirect (CODE:500|SIZE:3559)
+ http://127.0.0.1:3000/robots.txt (CODE:200|SIZE:3)
+ http://127.0.0.1:3000/video (CODE:200|SIZE:263788)
+ http://127.0.0.1:3000/Video (CODE:200|SIZE:263788)

(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)

END_TIME: Thu Dec  4 16:47:48 2025
DOWNLOADED: 4589 - FOUND: 8
```

An HTTP 200 status code indicates that a directory is accessible and active.

One of these directories is /ftp, where we can find a file acquisitions.md, which is intended to be confidential.

```
← → ↺ 🏠 127.0.0.1:3000/ftp/acquisitions.md
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

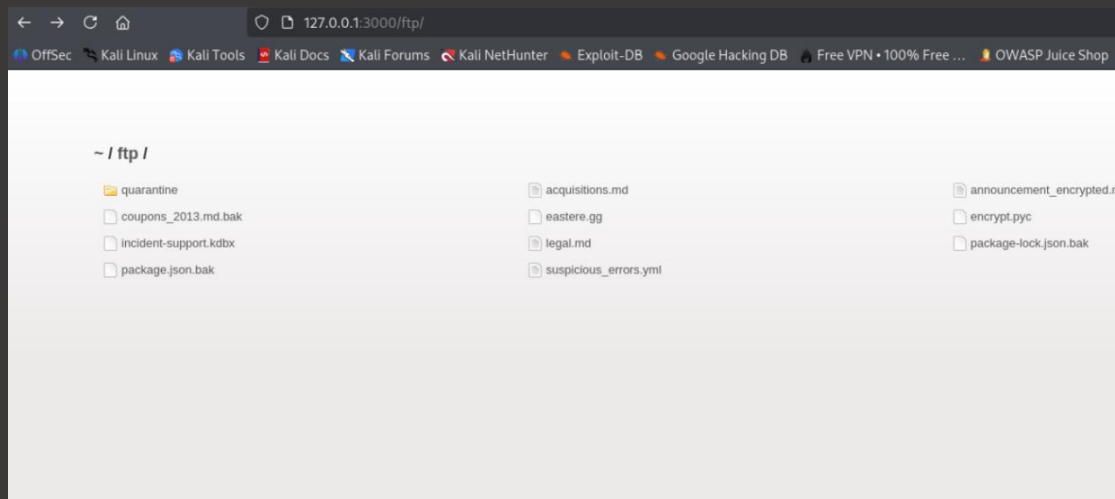
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```



This issue indicates improper access control and information exposure.

4. SQL Injection for Authentication Bypass

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

We can begin our penetration test at the registration form. For this purpose, we can enter the following into the username field:

```
- '
- ' OR true
- ' OR true --
```

The password field can be filled with any symbols.

As a result, we log in as an administrator.

This input manipulates the SQL query logic by forcing the condition to always evaluate as true, allowing authentication to be bypassed.

5. Metrics Exposure

*Metrics are important components of an application, as they can provide information about errors, requests, response time and memory usage of the server. **Prometheus**, a monitoring system, may expose sensitive metrics if it is improperly configured.*

Using the expression browser

Let us explore data that Prometheus has collected about itself. To use Prometheus's built-in expression browser, navigate to <http://localhost:9090/query> and choose the "Graph" tab.

As you can gather from localhost:9090/metrics , one metric that Prometheus exports about itself

Based on the above, we can access the following endpoint:

| <http://127.0.0.1:3000/metrics>

```
← → ↺ ↻ 🔍 127.0.0.1:3000/metrics

# OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Free VPN • 100% Free ... OWASP JuiceShop

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.041187399
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.120289601
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.1489029
juiceshop_startup_duration_seconds{task="dataRestorer",app="juiceshop"} 9.123920742
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.016554741
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.008488667
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 0.214

# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
# TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 50.611647

# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
# TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 95.311177

# HELP process_cpu_seconds_total Total user and system CPU time spent in seconds.
# TYPE process_cpu_seconds_total counter
process_cpu_seconds_total{app="juiceshop"} 145.922824

# HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
# TYPE process_start_time_seconds gauge
process_start_time_seconds{app="juiceshop"} 1764863569

# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"} 80134144

# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"} 1379672064

# HELP process_heap_bytes Process heap size in bytes.
# TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"} 243212288

# HELP process_open_fds Number of open file descriptors.
# TYPE process_open_fds gauge
process_open_fds{app="juiceshop"} 31

# HELP process_max_fds Maximum number of open file descriptors.
# TYPE process_max_fds gauge
process_max_fds{app="juiceshop"} 524288
```

As a result, we gain access to information that is intended to be confidential. Exposed metrics can reveal internal implementation details that may assist an attacker during reconnaissance.

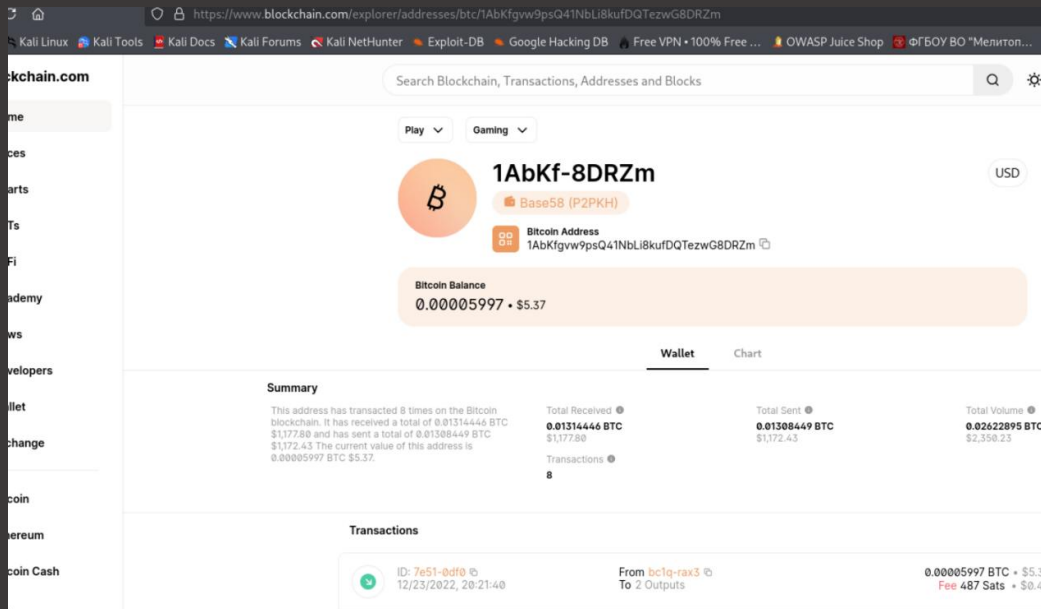
This issue apperars due to improper access control and information exposure.

6. Searching for Hidden Links

For this purpose we can download the main.js file and carefully review its contents for hidden resources. Within the file, we can identify a hidden link that is not visible through the user interface.

[illegible]

This link leads us to cryptocurrency wallet:



Exposing sensitive information in client-side JavaScript allows attackers to discover hidden functionality or confidential data without authentication. This issue is caused by improper handling of sensitive data on the client side.

7. DRY principle

"Don't repeat yourself" (DRY) is a principle of software development aimed at reducing repetition of information.

In this case, a violation of the DRY principle leads to a password confirmation bypass due to improper client-side validation.

To complete this task there are a few steps:

- 1) Fill the mail field on the registration page
- 2) Fill the password field
- 3) Fill the repeat password field
- 4) Return to password field and add some symbols

As a result, the password confirmation is bypassed, and the registration is accepted despite mismatched passwords. This issue occurs because the validation logic is not consistently applied and is only enforced on the client side without proper server-side verification.

User Registration

Email*

bibka13@gmail.com

Password*

●●●●●●

1 Password must be 5-40 characters long.

8/20

Repeat Password*

●●●●●●

7/40

Show password advice

Security Question *

1 This cannot be changed later!

Answer*

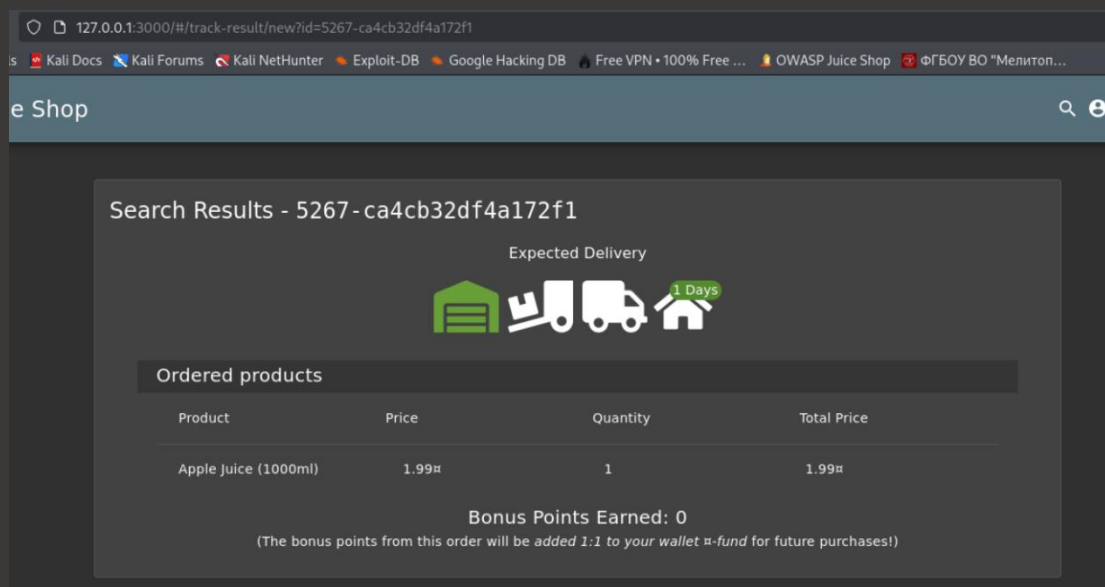
Register

Already a customer?

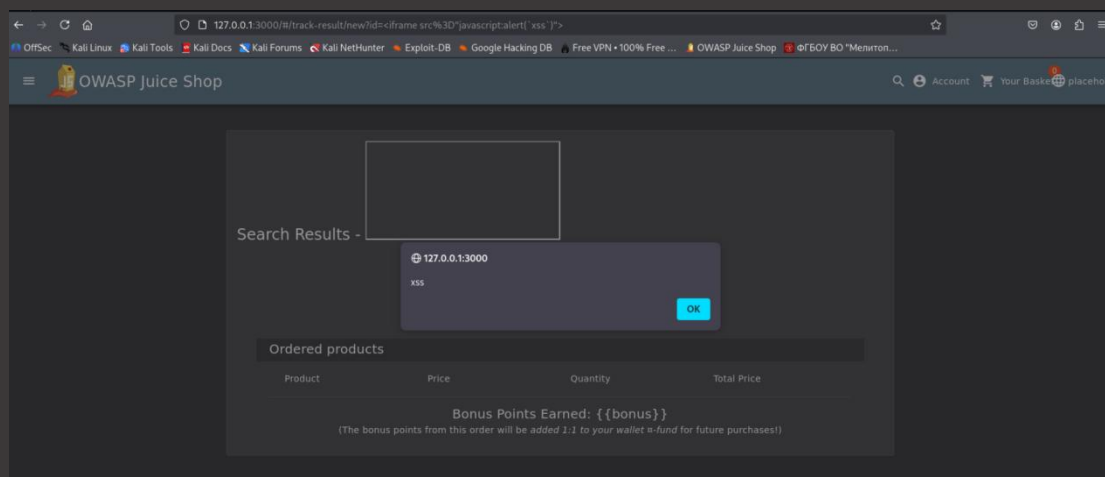
8. Reflected XSS Attack

A reflected XSS attack involves the injection of a malicious script into a website via user input (such as a URL parameter).

In this case we need to find a request that contains an id parameter “id” in its structure. While exploring the application, we can identify it on the order tracking result page.



Here we modify the value of the id parameter to `<iframe src="javascript:alert('xss')">`, and after reloading the page a pop-up window appears. This means that the injected script has been successfully executed.

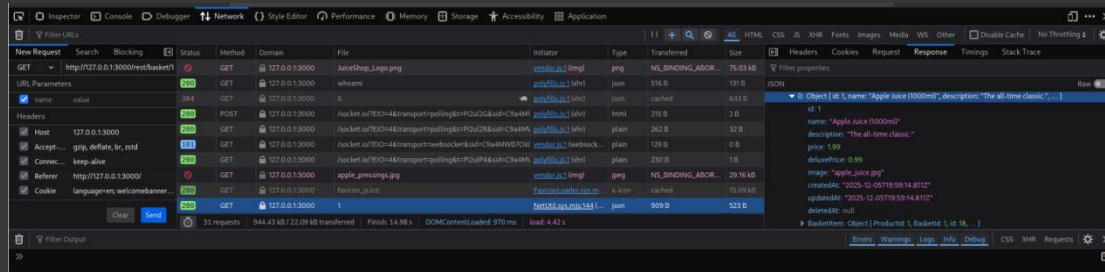


This vulnerability exists because user input is reflected in the response without proper sanitization or output encoding.

9. Viewing Another User's basket

This vulnerability is an example of Broken Access Control, specifically an Insecure Direct Object Reference (IDOR).

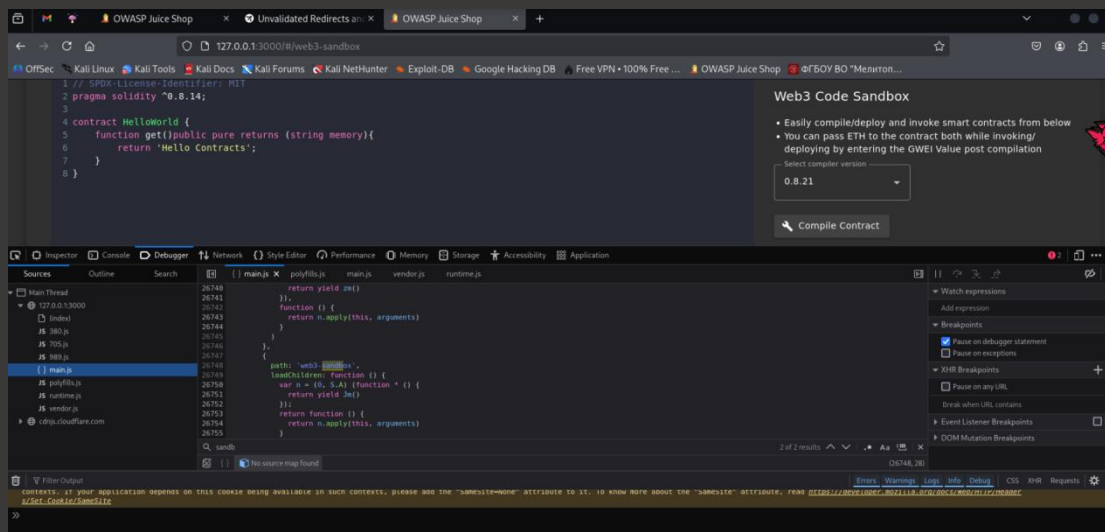
To exploit it, we open the browser developer tools, navigate to the Network tab and locate a GET request related to the basket. By modifying the basket ID parameter in the request and resending it, we are able to access another user's basket



This issue occurs because the server does not properly verify whether the authenticated user is authorized to access the requested basket ID.

10. Hidden sandbox

By reviewing the main.js file, we can identify a hidden path that is not directly accessible through the user interface.



This path leads to a sandbox environment, which should not be publicly exposed.

The vulnerability exists because sensitive or internal application paths are disclosed through client-side JavaScript files. This allows an attacker to discover internal application functionality through client-side source code analysis.

11. Zero-Starts Feedback

To complete this task, Burp Suit can be used to intercept a POST request related to submitting feedback.

The intercepted request is sent to Repeater, where the value of the “rating” parameter is modified from 3 to 0 we receive executing a request. After sending the modified request, the feedback with a zero-star rating is successfully accepted.

```
IJCjSTAN0TGMnAScJCL6IjAUMC4wLjAiLCJwcM9maWxLSWNzZU0lOIVYTNXZAPZL3S0tIXmPTySpwrHZNMFVdXBsb2Fkcy9kZWZhdxOLNnZ2YIsInRvdHBHTZWNYZXQoOiIlClJpcOfjdGJZZSi6dHJlZSwiY3JlYXRlZF01Oi01MjAyNS0xMi0wOSAwOT0OMj0zNC4yODAgKzAwOjAwIiwidXBKYXRlZEFOIjo1MjAyNS0xMi0wOSAwOT0OMj0zNC4yODAgKzAwOjAwIiwidGVzZXRLZEFOIjpudWxsfs9wiaWF0IjoxnZyY1Mjc2MDMwf0.PKhFTWSwhvI7IBqq-UP-JiOPz92ByI2mbNRHF2Rwuruk20gw9VRoV6tnCVYeORtC-ZizHxmM4ASFeuvbbdiDaOVHokXqdIdlBvnhz5-19ldCS9SaehBAEXNFNWuocxpj5rY_sCCEL9lgGetp36qtLLvwGNCM9Bclgk9NoKKlk
```

```
Accept-Language: en-US,en;q=0.9sec-ch-ua: "Chromium";v="139","Not;A=Brand";v="99"sec-ch-ua-mobile: ?0User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36Accept: application/json, text/plain, */*Content-Type: application/jsonOrigin: http://127.0.0.1:3000Sec-Fetch-Site: same-originSec-Fetch-Mode: corsSec-Fetch-Dest: emptyReferer: http://127.0.0.1:3000/Accept-Encoding: gzip, deflate, brCookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=nabybj29LKwoe7t2t2ckf6hmtVuq7ixxtGSazFGxfy7H4JdnJW3bkDrgeR; token=eYJOexAIoiJKVlQiLCJhbGciOiJSUzILNiJ9.eYJzdGF0dXMioiJzdWNjZXNXziIwiZGF0YSI6eyJpZCI6MjUsInZvZXJuYWllIjo1IiwiaWUiOm9kczkiOiJhZGIpbmtha2FAanVpY2UtC2gub3AiLCJwYXNzI2d29yZCI6Ij0yOTdtMTNDPMTMSNTUyUmZuNDViMj0SNzMSOWQ3YTktZiIiwicm9sZSI6bmNLc3RvbWVyIiwidGVzsdXhlVG9rZW4iOiIlClJscYNXNTQ9naWScjCl6IjAuMC4wLjAiLCJwcM9maWxlSW1hZ2U0Ii01YyYXNzZXRLZ3BlYmxpYy9pbWFnZXMFVdXBsb2Fkcy9kZWZhdxOLNnZ2YIsInRvdHBHTZWNYZXQoOiIlClJpcOfjdGJZZSi6dHJlZSwiY3JlYXRlZF01Oi01MjAyNS0xMi0wOSAwOT0OMj0zNC4yODAgKzAwOjAwIiwidXBKYXRlZEFOIjo1MjAyNS0xMi0wOSAwOT0OMj0zNC4yODAgKzAwOjAwIiwidGVzZXRLZEFOIjpudWxsfs9wiaWF0IjoxnZyY1Mjc2MDMwf0.PKhFTWSwhvI7IBqq-UP-JiOPz92ByI2mbNRHF2Rwuruk20gw9VRoV6tnCVYeORtC-ZizHxmM4ASFeuvbbdiDaOVHokXqdIdlBvnhz5-19ldCS9SaehBAEXNFNWuocxpj5rY_sCCEL9lgGetp36qtLLvwGNCM9Bclgk9NoKKlkConnection: keep-alive
```

```
{  "UserId":25,  "captchaId":0,  "captcha":"-1",  "comment":"'jjj (**inkaka@juice-sh.op)",  "rating":0}
```

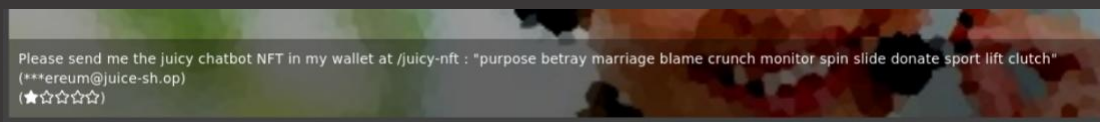
This vulnerability exists due to missing server-side validation of the rating parameter.

12. Accessing NFT Wallet Data

To gain access to NFT wallet data, we locate a seed phrase that is disclosed on the feedback page.

The following seed phrase is exposed:

purpose betray marriage blame crunch monitor spin slide donate sport lift clutch.



This seed phrase can be used to fully restore and access the associated wallet. The web tool iancoleman.io can be used to convert the phrase into a BIP39 seed.

This vulnerability represents a critical security issue, as exposure of a seed phrase allows complete control over the wallet and its assets.

Mnemonic Language English 日本語 Español 中文(简体) 中文(繁體) Français Italiano Čeština Português

BIP39 Mnemonic

☐ Show split mnemonic cards

BIP39 Passphrase (optional)

BIP39 Seed

Coin ETH - Ethereum

BIP32 Root Key

☐ Show BIP85

Derived Addresses

Note these addresses are derived from the BIP32 Extended Key


☐ Encrypt private keys using BIP38 and this password: Enabling BIP38 means each key will take several minutes to generate.

☐ Use hardened addresses

Path	Address	Public Key	Private Key
m/44'/68'/0'/0/0	0x8343d2eb2813A2495De435a1b15e85b98115Ce05	0x02c7a2a93289c9fbd55990bac659693e9bb0a8d3f178175a88b7cfd983983f506	0x5bcc3e9d38baa86e7bfaab80ae957bbe8ef059e640311d7d6d465e6bc948ae3e

You successfully solved a challenge: NFT Takeover (Take over the wallet containing our official Soul Bound Token (NFT).)

Note: Never reveal your personal private keys and seed phrase to anyone



Juicy Chatbot SBT
Owned by 034302

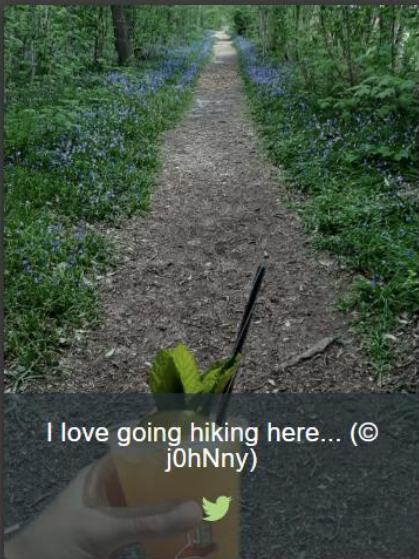
Account Address
0x8343d2eb2813A2495De435a1b15e85b98115Ce05

Description
Hurray! Find the Juice Shop SBT on OpenSea. This is a non-transferable token and is here to stay forever.

13. Work with metadata

Metadata is additional information embedded in files, such as images, which may include details about the device, time, and location where the file was created.

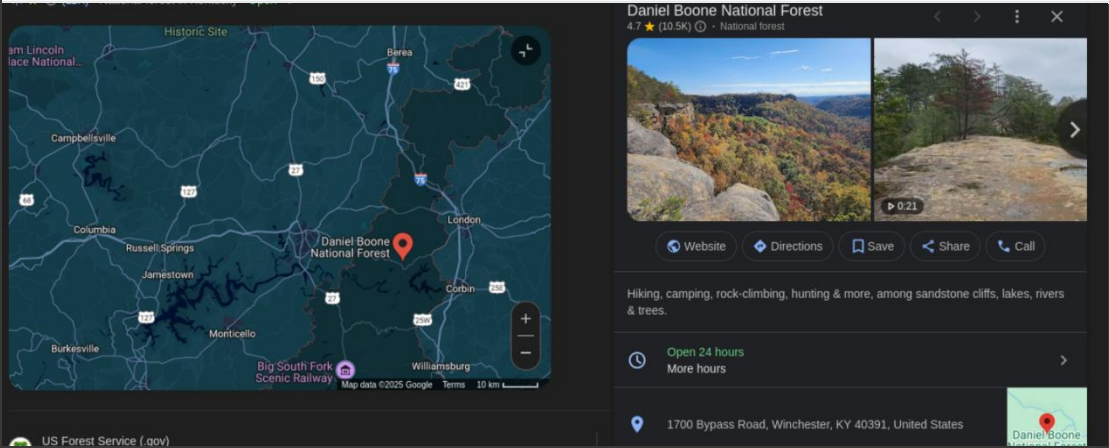
In this task, we analyze the metadata of an uploaded image using the web tool metadata2go.com. While reviewing the metadata, we discover GPS coordinates indicating where the photo was taken.



amy@juice-sh.op	👁
bjoern@juice-sh.op	👁
bjoern@owasp.org	👁
accountant@juice-sh.op	👁
uvogin@juice-sh.op	👁
demo	👁
john@juice-sh.op	👁
emma@juice-sh.op	👁
stan@juice-sh.op	👁
ethereum@juice-sh.op	👁

By searching coordinates on Google Maps, we determine that the location corresponds to the Daniel Boone National Forest. Next, we navigate to the login page and use the "Forgot your password?" functionality. By entering the email address john@juice-sh.op and answering the security question with "Daniel Boone National Forest", we are able to gain access to the account.


thumbnail_length	4531
srgb_rendering	Perceptual
gamma	2.2
pixels_per_unit_x	3779
pixels_per_unit_y	3779
pixel_units	meters
image_size	471x627
megapixels	0.295
thumbnail_image	(Binary data 4531 bytes)
gps_latitude	36 deg 57' 31.38" N
gps_longitude	84 deg 20' 53.58" W
gps_position	36 deg 57' 31.38" N, 84 deg 20' 53.58" W
category	image



This vulnerability demonstrates how exposed metadata can be leveraged in combination with weak account recovery mechanisms to compromise user accounts.

14. White-hat behavior.

As a first step, we visit the website securitytxt.org to understand the purpose and structure of the `security.txt` standard.



The screenshot shows a web browser window with the address bar displaying `https://example.com/.well-known/security.txt`. The page content is a text file with the following structure:

```
# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

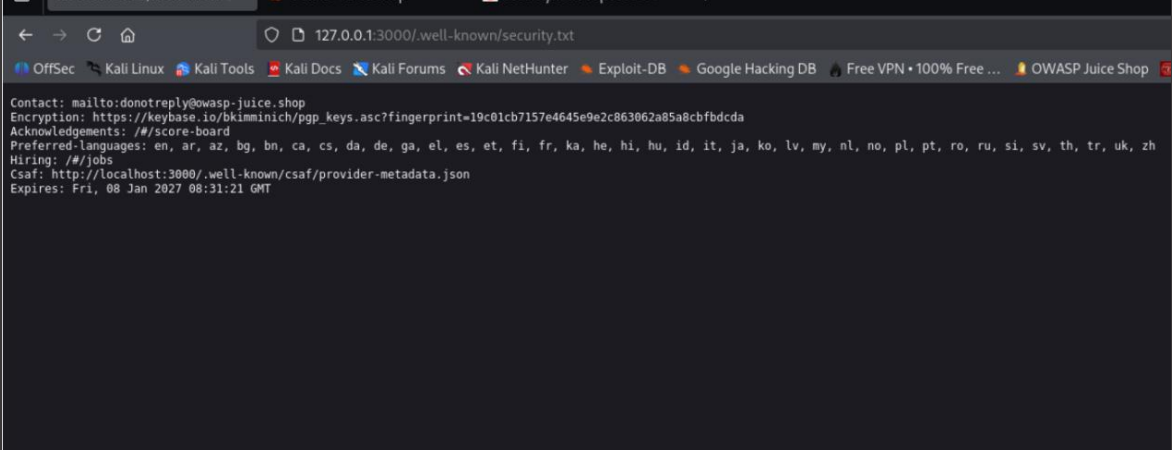
# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
```

Below the browser window, there is a section titled "Summary" with a quote: "When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely."

Below the quote, there is a paragraph: "security.txt files have been implemented by Google, Facebook, GitHub, the UK government, and many other organisations. In addition, the UK's Ministry of Justice, the Cybersecurity and Infrastructure Security Agency (US), the French government, the Italian government, the Dutch government, and the Australian Cyber Security Centre endorse the use of security.txt files."

A hint within the application suggests visiting the following path:

| <http://127.0.0.1:3000/.well-known/security.txt>



The screenshot shows a web browser window with the address bar displaying `127.0.0.1:3000/.well-known/security.txt`. The page content is a text file with the following structure:

```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdca
Acknowledgements: /#/score-board
Preferred-languages: en, ar, az, bg, bn, ca, cs, da, de, ga, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, lv, my, nl, no, pl, pt, ro, ru, si, sv, th, tr, uk, zh
Hiring: /#/jobs
Csaf: http://localhost:3000/.well-known/csaf/provider-metadata.json
Expires: Fri, 08 Jan 2027 08:31:21 GMT
```

The file contains contact information and security policies, indicating that penetration testing is permitted and providing details for responsible vulnerability disclosure.

This demonstrates proper white-hat behavior by verifying authorization before conducting security testing.

15. Adding a Negative Quantity to the Cart

This vulnerability is an example of a business logic flaw caused by missing server-side validation of input values.

To exploit this issue, we intercept a PUT request related to adding a product to the cart and modify it as follows:

- 1) Ensure that the product ID matches the selected product
- 2) Change the Authorization token to a different one obtained from another valid PUT request
- 3) In the request body, change the quantity value to -100
- 4) Send the modified request and place the order

New Request	Search	Blocking	Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
PUT	http://127.0.0.1:3000/api/basket/items/5		304	GET	127.0.0.1:3000	application-configuration	polyfills.js [xhr]	json	cached	2173 B	94 ms
URL Parameters			304	GET	127.0.0.1:3000	Cards	polyfills.js [xhr]	json	cached	237 B	122 ms
name	value		200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&f=PKX_kfq	polyfills.js [xhr]	plain	326 B	96 B	4 ms
Headers			200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=websocket&sid=c1Vt-TL5CRCi33y2AAAI	vendor.js [websocket]	plain	129 B	0 B	4 ms
Host	127.0.0.1:3000		200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&f=PKX_kG&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js [xhr]	plain	262 B	32 B	1 ms
Accept-Encoding	gzip, deflate, br, zstd		200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&f=PKX_kHP&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js [xhr]	plain	230 B	1 B	87 ms
Content-Length	17		304	GET	127.0.0.1:3000	1	polyfills.js [xhr]	json	cached	106 B	31 ms
Origin	http://127.0.0.1:3000		304	GET	127.0.0.1:3000	3	polyfills.js [xhr]	json	cached	273 B	17 ms
Connection	keep-alive		304	GET	127.0.0.1:3000	1	polyfills.js [xhr]	json	cached	1,311 B	301 ms
Referer	http://127.0.0.1:3000/		304	GET	127.0.0.1:3000	whoami	polyfills.js [xhr]	json	cached	125 B	130 ms
Cookie	language=en; welcomebanner_status=dismiss; cooki...		200	GET	127.0.0.1:3000	continue-code	polyfills.js [xhr]	json	492 B	107 B	52 ms
Sec-Fetch-Dest	empty		304	GET	127.0.0.1:3000	705.js	runtime.js [script]	js	cached	0 B	188 ms
Sec-Fetch-Mode	cors		200	GET	127.0.0.1:3000	1	polyfills.js [xhr]	json	538 B	153 B	84 ms
Sec-Fetch-Site	same-origin		200	GET	127.0.0.1:3000	5267-7fcd0c9468892634	polyfills.js [xhr]	json	944 B	558 B	64 ms
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100...		304	GET	127.0.0.1:3000	application-configuration	polyfills.js [xhr]	json	cached	2173 B	4 ms
Accept	application/json, text/plain, */*		304	GET	127.0.0.1:3000	3	polyfills.js [xhr]	json	cached	273 B	85 ms
Accept-Language	en-US,en;q=0.5		200	POST	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&f=PKX_kG&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js [xhr]	html	215 B	2 B	3 ms
Authorization	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJz...		200	POST	127.0.0.1:3000	checkout	polyfills.js [xhr]	json	429 B	45 B	166 ms
24 requests 47.73 kb / 5.30 kb transferred Finish: 20.81 s											

☒ User-Agent

Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100...

☒ Accept

application/json, text/plain, */*

☒ Accept-Langu...

en-US,en;q=0.5

☒ Authorization

Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJz...

☒ Content-Type

application/json

☒ name

value

Body

```
{"quantity":-100}
```

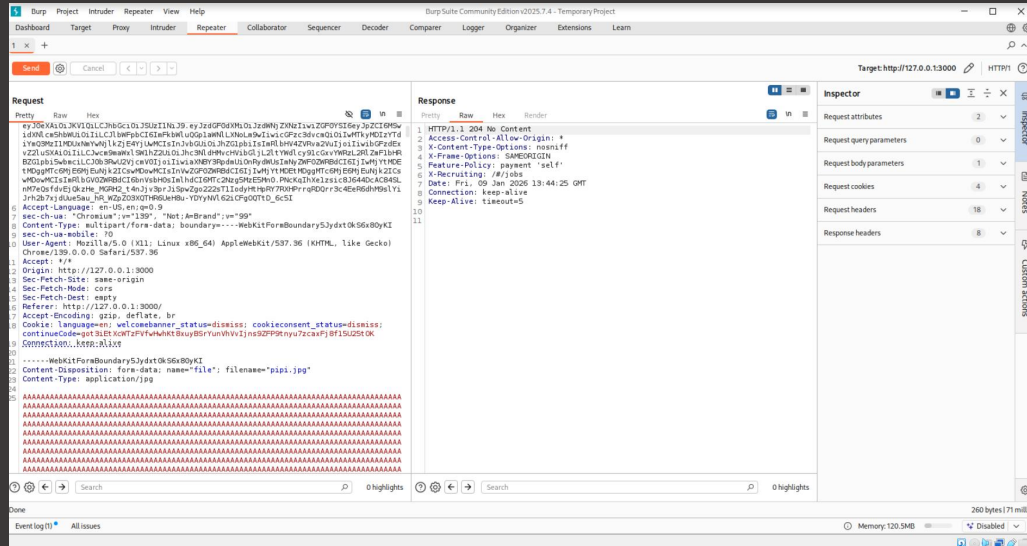
Order History				
Order ID	Total Price	Bonus	In Transit	
#5267-7fcd0c9468892634	-165.08€	2		
Product	Price	Quantity	Total Price	
Apple juice (1000ml)	1.99€	-100	-199.00€	
Orange Juice (1000ml)	2.99€	5	14.95€	
Eggfruit Juice (500ml)	8.99€	2	17.98€	
Order ID	Total Price	Bonus	Delivered	
#5267-a465ec6b4e26a118	26.97€	3		
Product	Price	Quantity	Total Price	
Eggfruit Juice (500ml)	8.99€	3	26.97€	

As a result, the application accepts a negative quantity, which leads to incorrect order processing and may result in financial manipulation

16. File Upload Manipulation

This vulnerability is caused by insufficient server-side validation of uploaded files.

To exploit this issue, we intercept a POST request while uploading a file that does not violate the size limit using Burp Suite. The intercepted request is sent to Repeater, where the file content, format, and file name are modified.



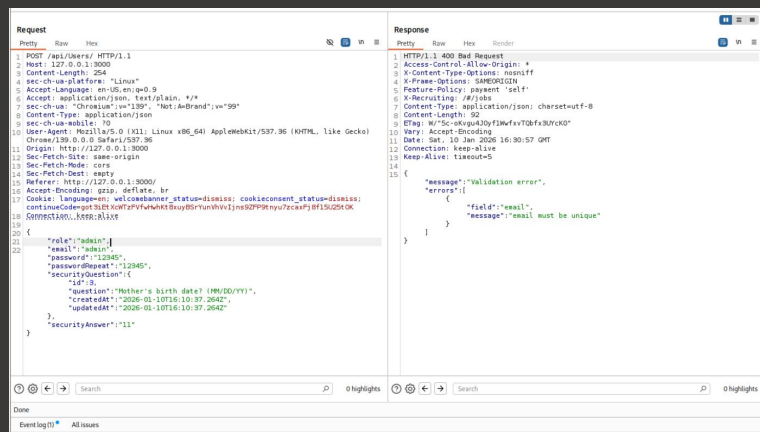
After sending the modified request, the application successfully accepts the manipulated file. This demonstrates that the server does not properly validate file type, content, or extension during the upload process.

17. Creating an Account with an Admin Role

This vulnerability is caused by improper server-side validation and is an example of a mass assignment issue.

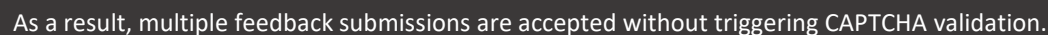
It is possible to create an account with the admin role by performing the following steps:

- 1) Open Burp Suite and enable the Proxy, then navigate to `http://127.0.0.1:3000`
- 2) Intercept the POST request related to the Users API and send it to Repeater.
- 3) Modify the request by adding a new parameter named "role"
- 4) Assign the value "admin" to this parameter
- 5) Send the modified request via Repeater



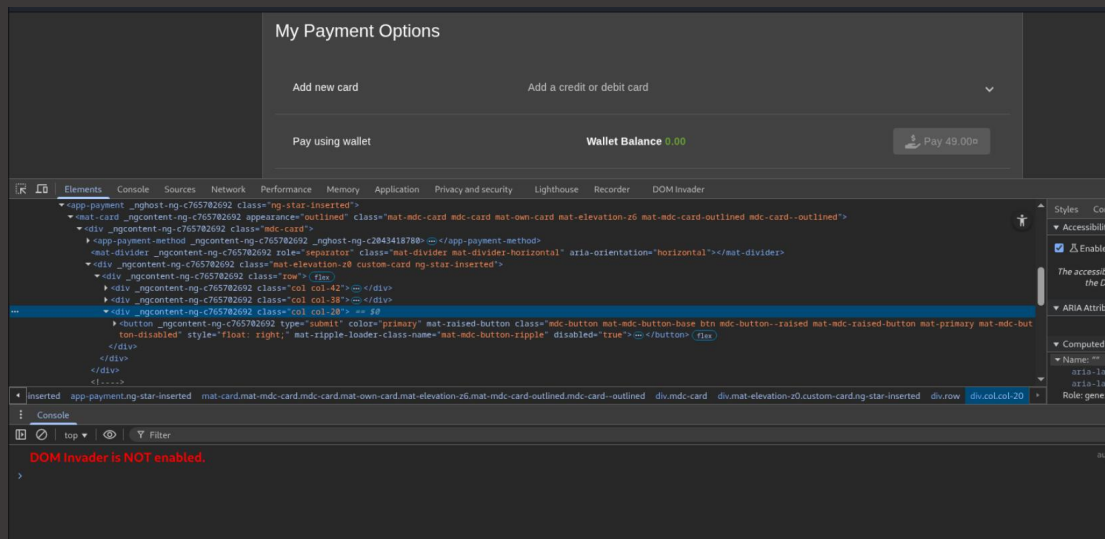
18. CAPTCHA Bypass

To exploit this vulnerability, we intercept a POST request while submitting normal feedback. The intercepted request is sent to Repeater and replayed 10–15 times.



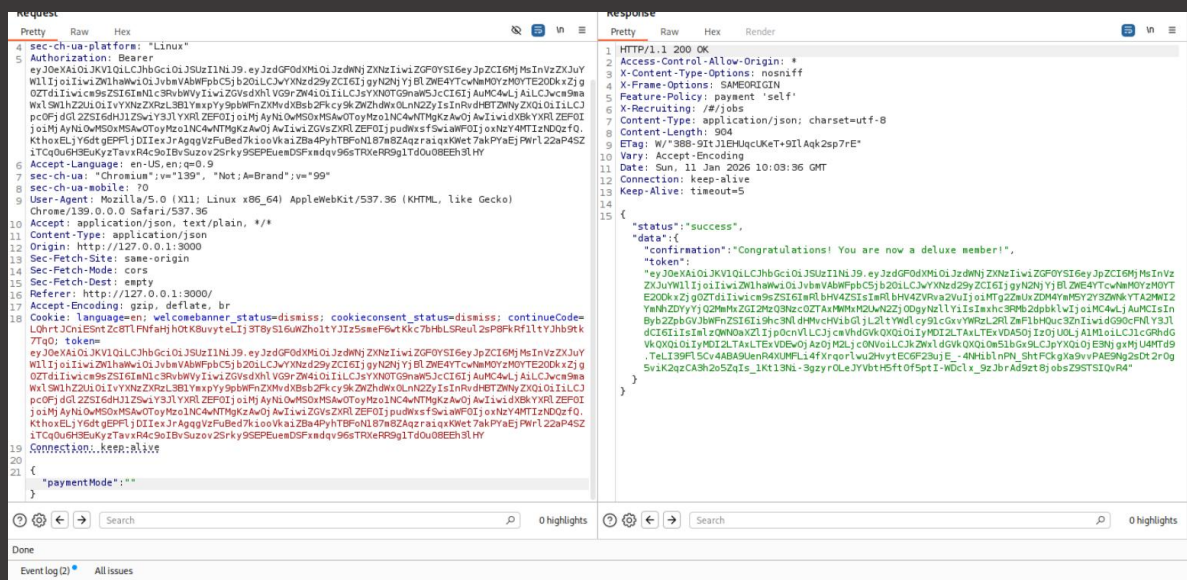
19. Becoming a Deluxe Member Without Payment

The “Pay using wallet” button is disabled on the client side. By using the browser developer tools, we locate the disabled="true" attribute and remove it to activate the *button*.



Next, we intercept the POST request generated when clicking the “Pay with wallet” button. The intercepted request is sent to Repeater in Burp Suite, where the value of the "paymentMode" parameter is removed.

After sending the modified request and disabling interception, the application upgrades the account to a Deluxe membership without completing a valid payment.



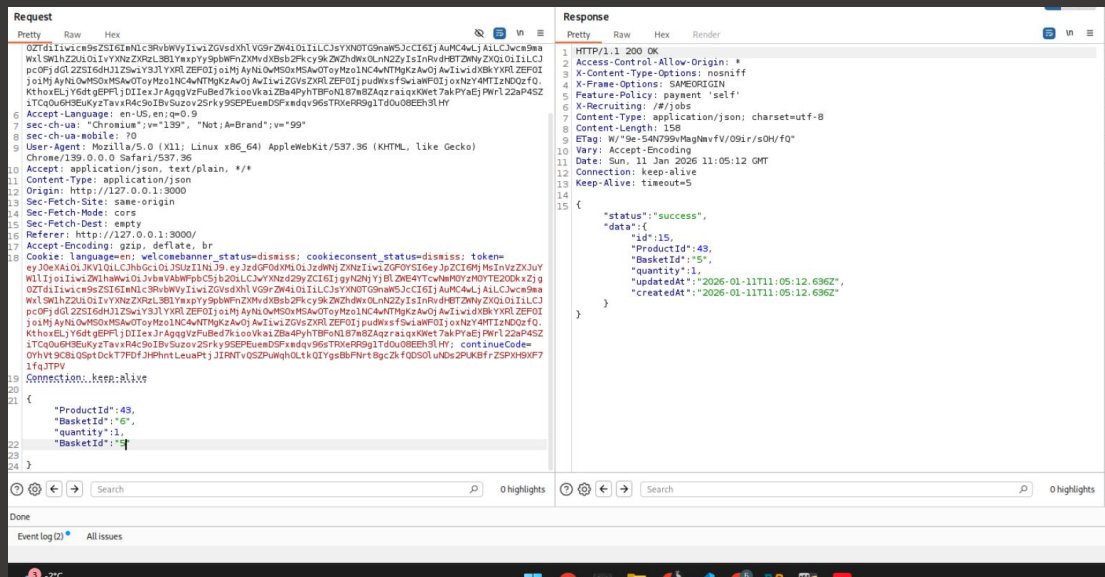
This issue exists because the server trusts client-side controls and does not properly verify payment status.

20. Putting a Product in Another User's Basket

This vulnerability is caused by broken access control and represents an Insecure Direct Object Reference (IDOR) issue.

To exploit this vulnerability, we intercept a POST request using Burp Suite. The request contains the following parameters: ProductId, BasketId, and Quantity.

By modifying the BasketId parameter to the ID of another user's basket (using a lower numeric value) and sending the modified request through Repeater, the product is successfully added to another user's basket.



This issue occurs because the server does not verify ownership of the basket before processing the request.

21. Performing a Persisted XSS attack by Bypassing a Client-Side Security

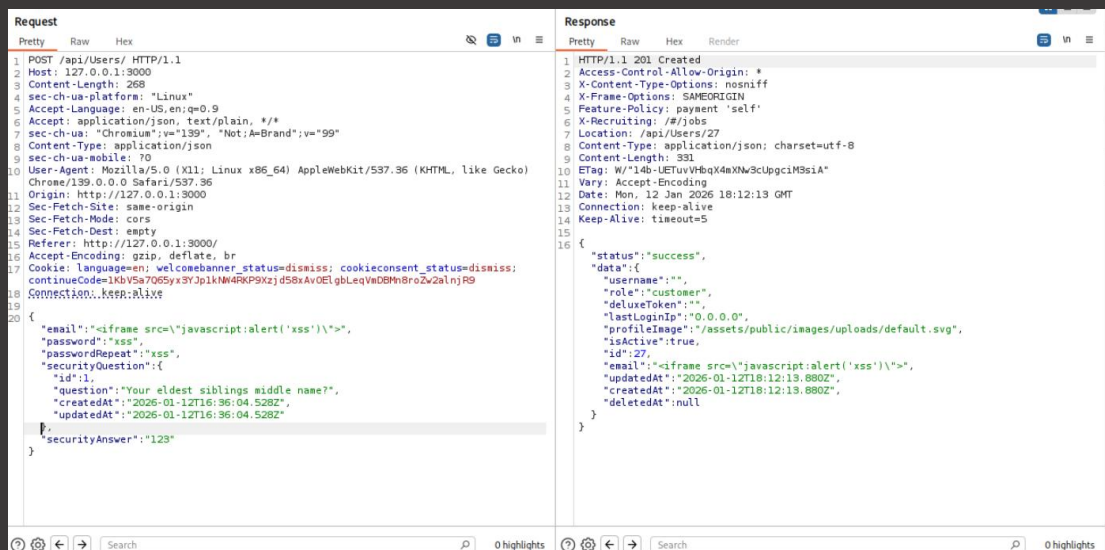
This vulnerability allows a persisted (stored) XSS attack due to insufficient server-side input validation and reliance on client-side security mechanisms.

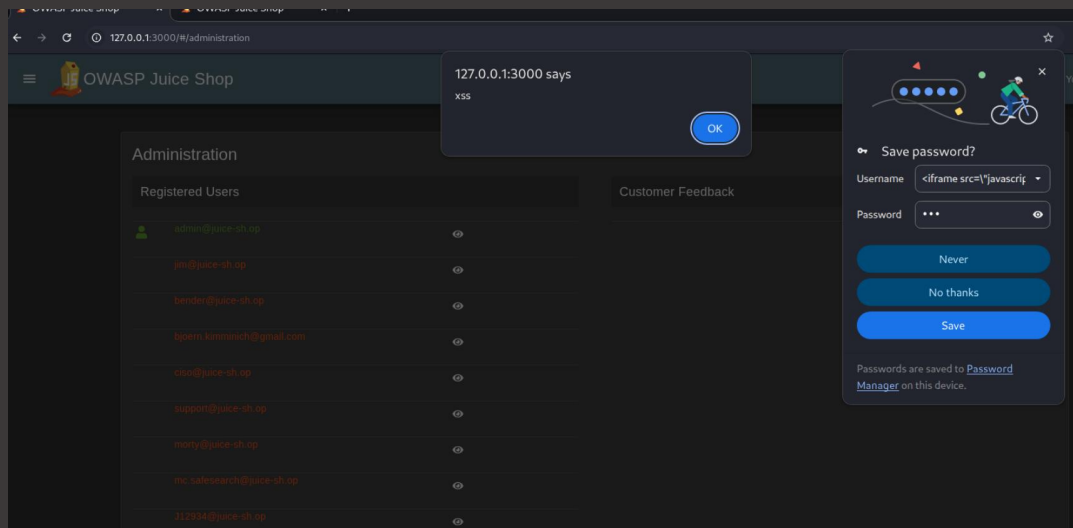
To exploit this issue, we intercept the POST request to the /api/user endpoint while registering a new user. The intercepted request is modified with the following values:

Email:
{ "email": "<iframe src='\"javascript:alert('xss')\">" }

Password:
{ "password": "xss" }

The modified request is sent through Repeater. After logging in to the application as an administrator and navigating to the /administration page, the injected script is executed when viewing the list of registered accounts.





This confirms a persisted XSS vulnerability, as the malicious payload is stored on the server and executed when accessed by privileged users.

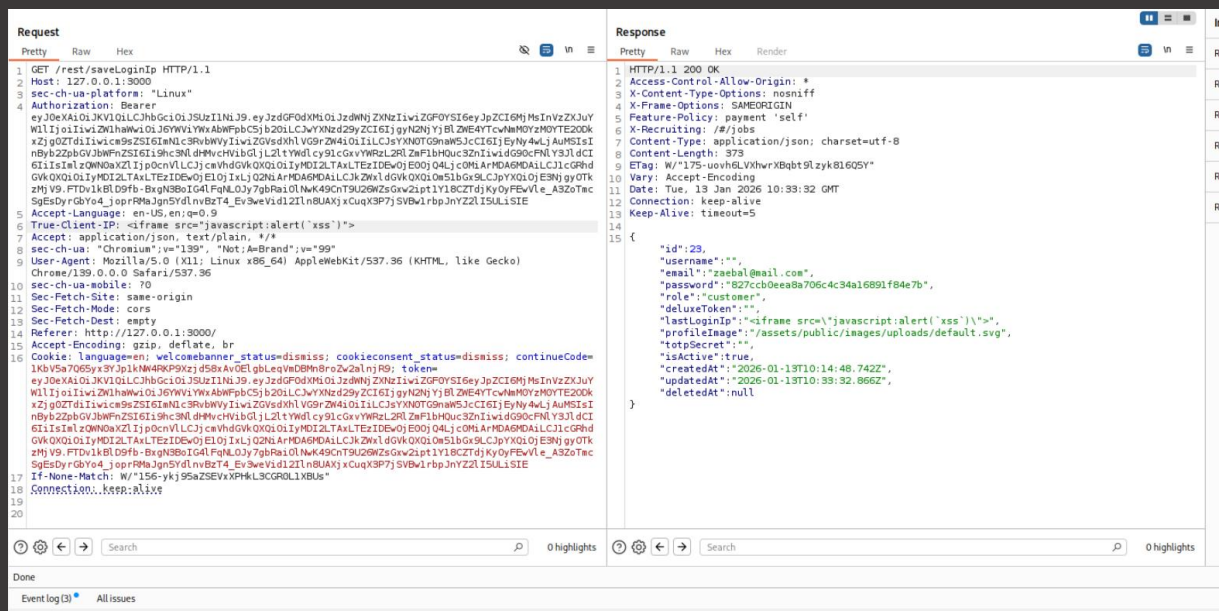
22. Performing a Persisted XSS Attack via HTTP Header Injection

This vulnerability exists due to the application trusting user-controlled HTTP headers and storing their values without proper server-side sanitization.

To exploit this issue, the `/rest/saveLoginIP` endpoint was identified. A malicious payload was injected into the True-Client-IP HTTP header with the following value:

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

The commonly used X-Forwarded-For header was tested but was not successful.



The injected payload was stored by the application and later rendered in the interface, resulting in script execution. This confirms a persisted XSS vulnerability originating from an HTTP header.