

Juice-Shop exploring Report

Juice-shop - interactive vulnerable platform, where entry-level pentesters can apply their skills and knowledge, put theory to practice.

First that we need to do - install npm server. This will allow us to have access to site every time when we need it. There are several steps to achieve this.

1. Install nodejs through terminal

Sudo nodejs install

2. Instal npm

Sudo npm install

3. Install juice-shop from github

Git clone <https://github.com/juice-shop/juice-shop.git>

4. Enter to the fold Juice-shop

Cd juice-shop

5. Start npm-server

Npm start

6. Open site with browser on the port 3000.

127.0.0.1:3000/

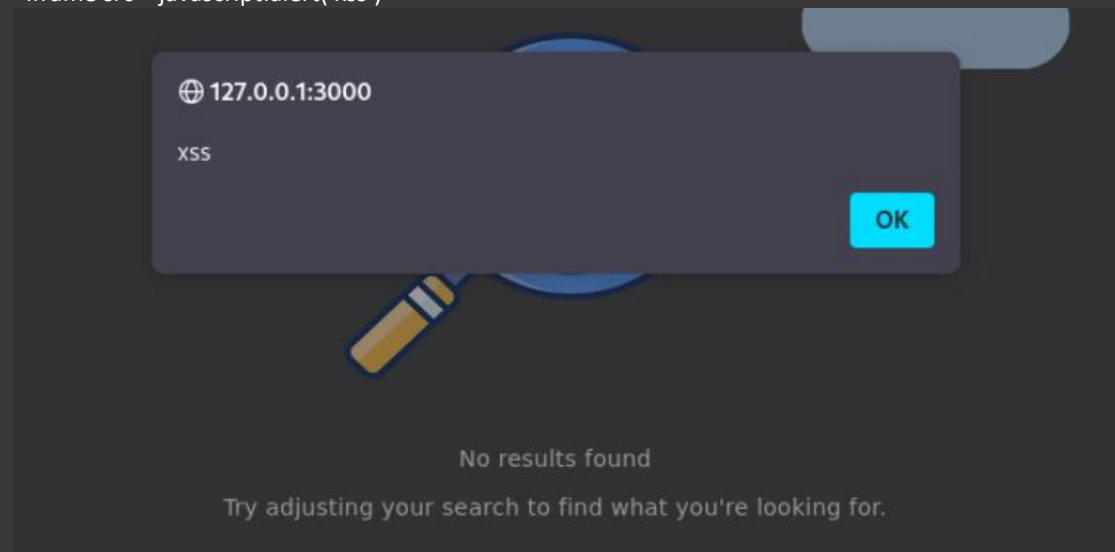
Tasks level EASY

1. XSS-injection.

This term means a web-security vulnerability where an attacker can inject malicious scripts into trusted web-sites.

For our understanding if site vulnerable to XSS-injection or not we can use search-field. For this we can enter <h1>owasp. We can see that site do not resist. So we can use next script:

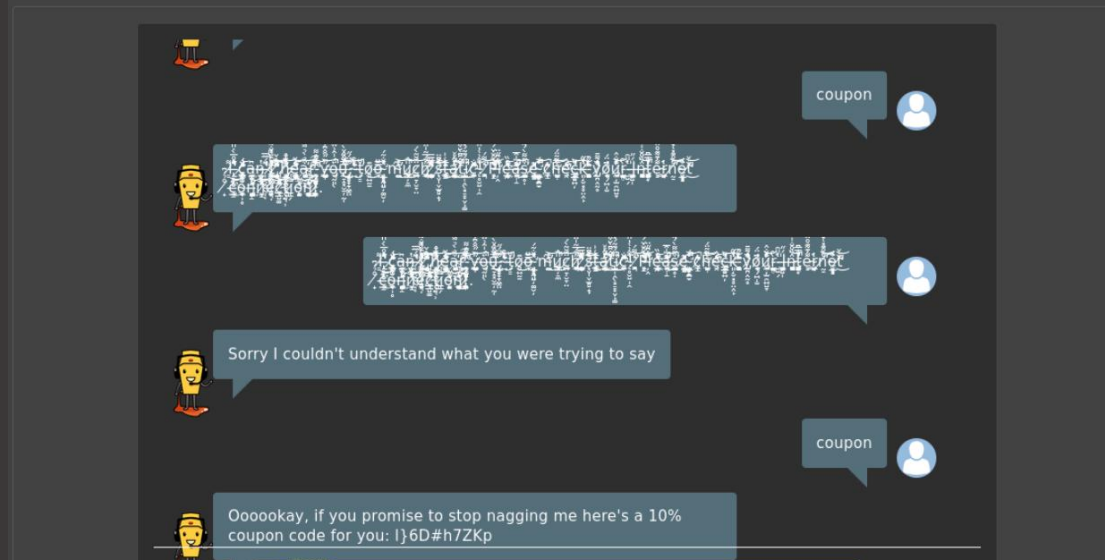
<iframe src="javascript:alert('xss')">



As result we can see next changes in the address field: 127.0.0.1:3000/#/search?q=<iframe src%3D"javascript:alert('xss')">

2. Brutforce chat-bot

Bruteforce this is trial-or-error method, that implies repetitive tries with every possible combinations. Using this method while talking with site's bot, we can reach next results:



3. Searching for a hidden directories.

For this purpose we can use powerful utilita 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

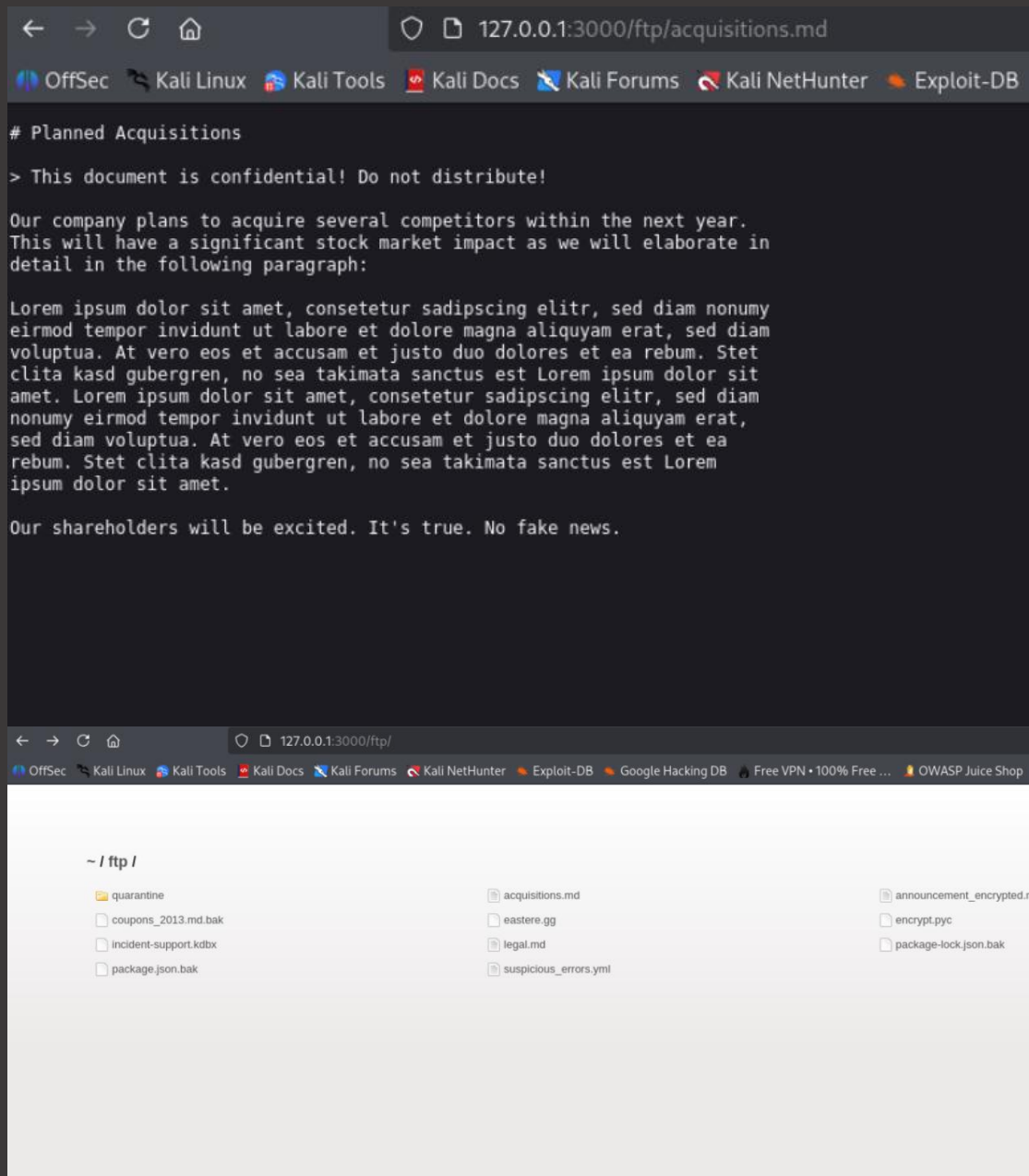
— Scanning URL: http://127.0.0.1:3000/ —
+ http://127.0.0.1:3000/assets (CODE:301|SIZE:156)
+ http://127.0.0.1:3000/ftp (CODE:200|SIZE:941)
+ http://127.0.0.1:3000/profile (CODE:500|SIZE:1061)
+ http://127.0.0.1:3000/promotion (CODE:200|SIZE:692)
+ http://127.0.0.1:3000/redirect (CODE:500|SIZE:3559)
+ 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
```

Code 200 allows us to see which directories are active and exists in the access zone.

One of them is directory /ftp, where we can find a document acquisitions.md, that suppose to be confidential.



4. SQL-injection for password bypassing

We can start our penetration in the registration form. For this we can put next to the username field:

```
'
- ' or true
- ' or true --
```

Password field we can fill by any symbols.

As result, we can login as an administrator.

Metrics are very important entity. They can provide information about errors, requests, time and memory, that server needs. Prometheus - system of monitoring - can disclose information about exposed metrics on site.

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.

So, based on the above, we can use next link:

```
← → ↺ ↻ 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
```

6. Searching for hidden list.

There we can see hidden link

[illegible]

This link leads us to cryptowallet.

Blockchain.com Explorer: 1AbKf-8DRZm

Search Blockchain, Transactions, Addresses and Blocks

Play Gaming

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 • \$5.37

Fee 487 Sats • \$0.44

7. DRY principle

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

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*

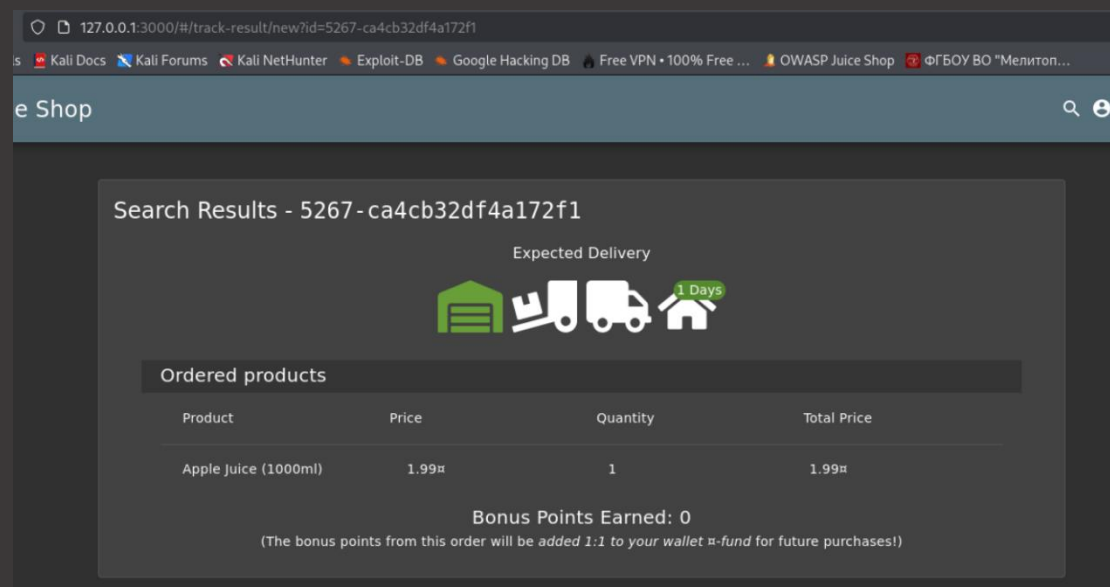
Register

Already a customer?

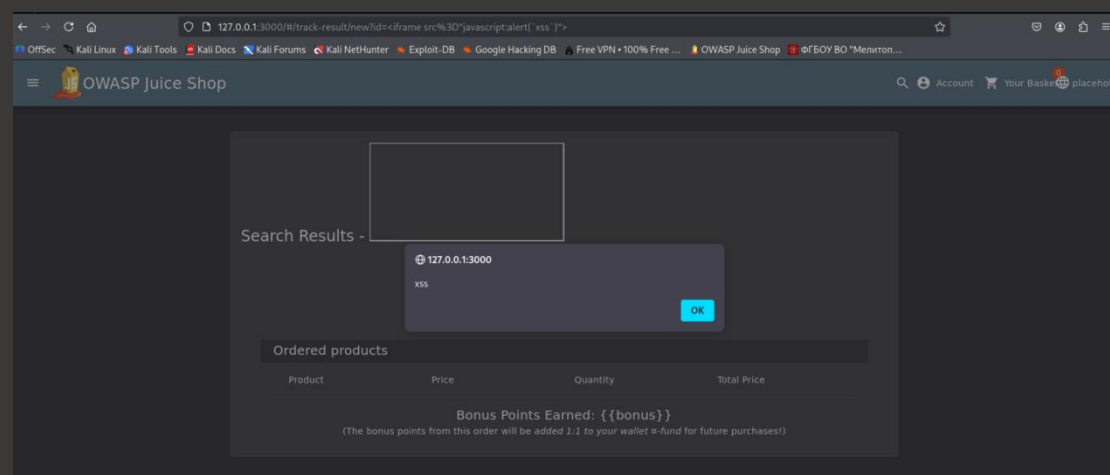
We just change pass in the first field and registration is successfully finished

8. Reflected XSS Attack

Reflected XSS attack implies injection of malicious script into a website via user input (like URL parameter).
We suppose to find a reference that has parameter “id” in it’s structure. Exploring whole site we see it on the track-result page.

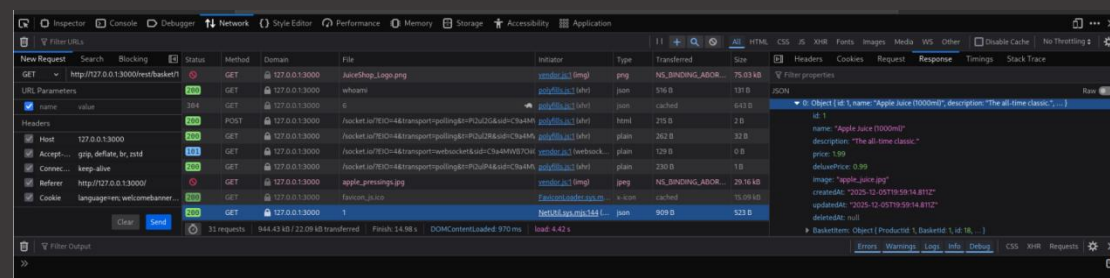


Here we change an id parameter value for `<iframe src=javascript:alert('xss')">`, and after reloading of page we can see pop-up window, that testifies that script is done



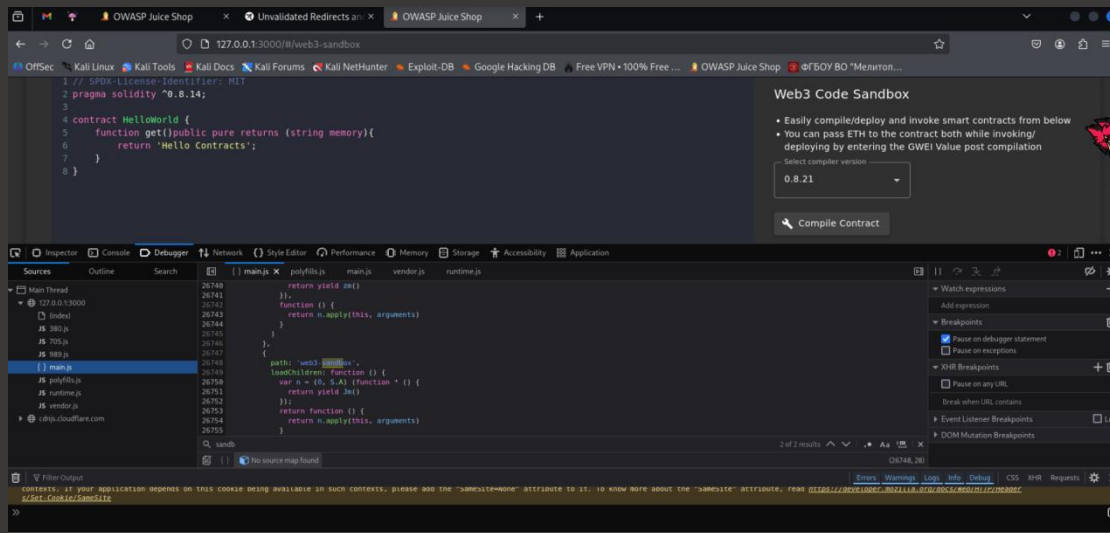
9. Another user’s basket viewing

For achieving this we use the developer mode, go to the network tab and through requests changing basket’s id in th GET request.



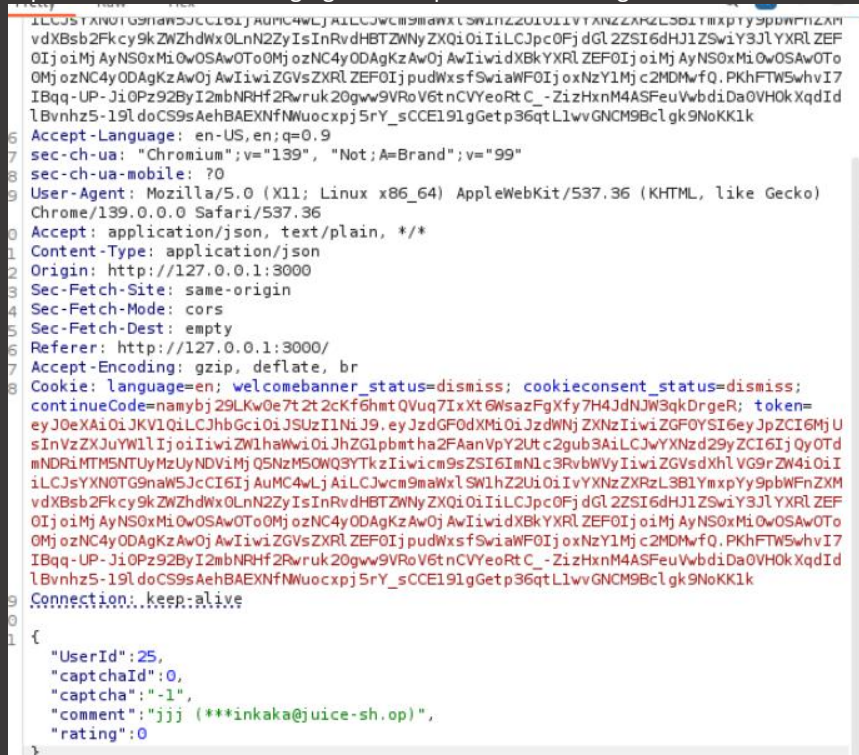
10. Hidden sandbox

We can find hidden path in the main.js.



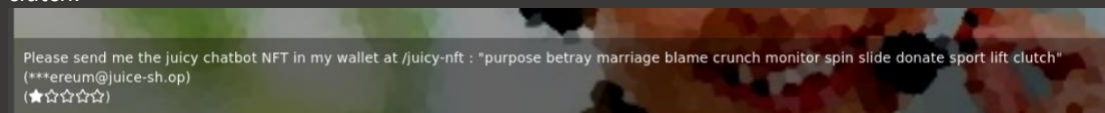
11. 0 starts feedback

For this purpose we used BurpSuite. 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.



12. To get acces to NFT-wallet data we find seedphrase, that disclosed on the feedbacks page.

We see the seed phrase: purpose betray marriage blame crunch monitor spin slide donate sport lift clutch.



Web-tool iancoleman.io helps to convert it to BIP39 Seed.

Mnemonic Language

English日本語Español中文(简体)中文(繁體)FrançaisItalianoČeštinaPortuguês

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

xprv9s21ZrQH143K4DfTxz9Ygc6kvSBEV8LgZPk7BcXzJzT49gjeVoY5xqD21Q9jnyZQXaeWqp7wRs44vbeWU1FwRzbXFazix1hc7qFhSoyD6ub

☐ 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

TableCSV

PathToggle

AddressToggle

Public KeyToggle

Private KeyToggle

m/44'/68'/0'/0/00x8343d2eb2813a2495de435a1b15e85b98115ce050x02c7a2a93289c9fbd5990bac6596993e9bb0a8d3f178175a80b7cfd983983f5060x5bcc3e9d38baa86e7bfaab80ac9597b8e8f059e640311d7d6d46e6bc948e3e

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 0343D2

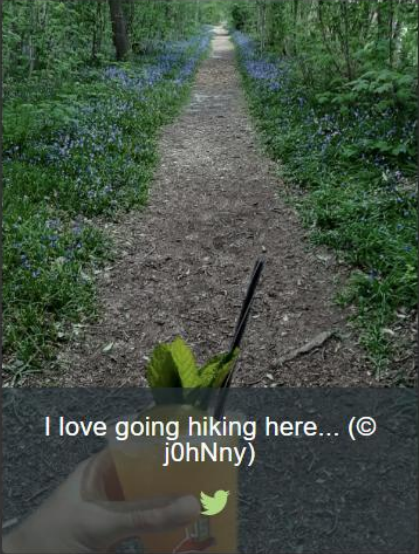
Account Address

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



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

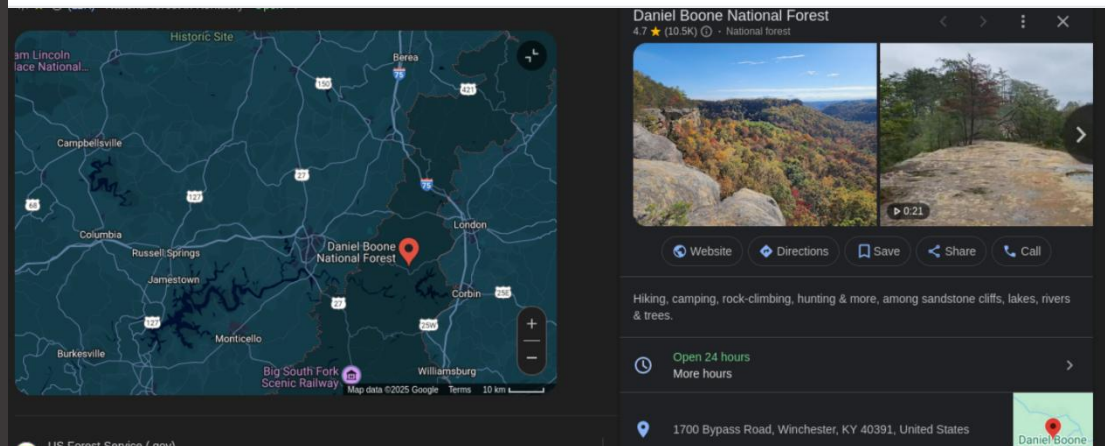
john@juice-sh.op

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



14. White-hat behavior.
- visit the site securitytxt.org

Order History

16.- Intercept the POST request when sending a file that doesn't violate the size limit with burp suit
- Edit the request in Repeater, changing the content, format, and file name

