
*root@localhost:~$ echo "b477l3 0f l337"*

# BATTLE_OF_1337

## CTF 2022

# BATTLE OF 1337 OFFICIAL WRITEUP

*Writeup By : thomaswayne*

# TABLE OF CONTENT

# RANTAIANBLOK


**STEPS OF REPLICATION**

- install quasar using NPM I -G @QUASAR/CLI, we will also need ethers NPM I ETHERS
- initatiate a new project by running NPM INIT QUASAR

```
~/Dev
└ npm init quasar


 .d88888b.
d88P" "Y88b
888     888
888     888 888  888  8888b.  .d8888b   8888b.  888d888
888     888 888  888     "88b 88K          "88b 888P"
888 Y8b 888 888  888 .d888888 "Y8888b. .d888888 888
Y88b.Y8b88P Y88b 888 888  888      X88 888  888 888
 "Y888888"   "Y88888 "Y888888  88888P' "Y888888 888
       Y8b

✓ What would you like to build? › App with Quasar CLI, let's go!
✓ Project folder: … blokrantaian
✓ Pick Quasar version: › Quasar v2 (Vue 3 | latest and greatest)
✓ Pick script type: › Javascript
✓ Pick Quasar App CLI variant: › Quasar App CLI with Webpack
✓ Package name: … blokrantaian
✓ Project product name: (must start with letter if building mobile apps) … Quasar App
✓ Project description: … A Quasar Project
✓ Author: … s3ns3 <s3ns3xy@yahoo.com>
✓ Pick your CSS preprocessor: › Sass with SCSS syntax
✓ Check the features needed for your project: › ESLint
```

- place the ABI file in any folder that you wish, in my case i placed it under the /UTILS folder. i have also format the json using HTTPS://JSONFORMATTER.CURIOUSCONCEPT.COM/#

```
" Press ? for help
.. (up a dir)
/home/vecna/Dev/rantaianblok/
▸ [ ]node_modules/
▸ [ ]public/
▾ [ ]src/
  ▸ [ ]assets/
  ▸ [ ]boot/
  ▸ [ ]components/
  ▸ [ ]css/
  ▸ [ ]layouts/
  ▸ [ ]pages/
  ▸ [ ]router/
  ▾ [ ]utils/
      {} rantai.json
    App.vue
    index.template.html
  babel.config.js
  jsconfig.json
  package-lock.json
  package.json
  quasar.config.js
  README.md
```

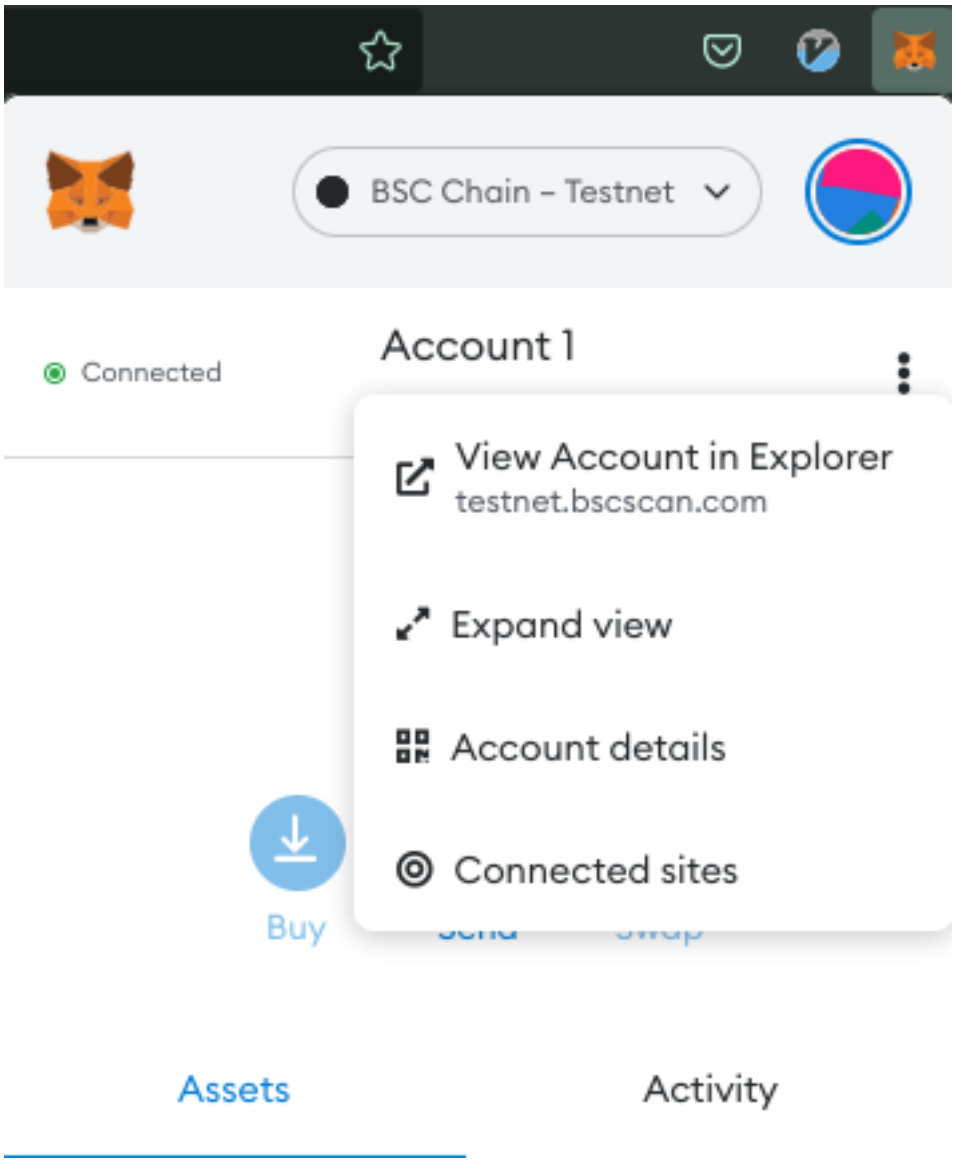
```
{
    "abi":[
        {
            "inputs":[

            ],
            "stateMutability":"nonpayable",
            "type":"constructor"
        },
        {
            "inputs":[

            ],
            "name":"flag",
            "outputs":[
                {
                    "internalType":"string",
                    "name":"",
                    "type":"string"
                }
            ],
            "stateMutability":"view",
            "type":"function"
        }
    ]
}
```

- below are the source code for **/SRC/PAGES/INDEXPAGE.VUE**. we will need to make asynchronous call to the **FLAG()** function as it will return a promise.

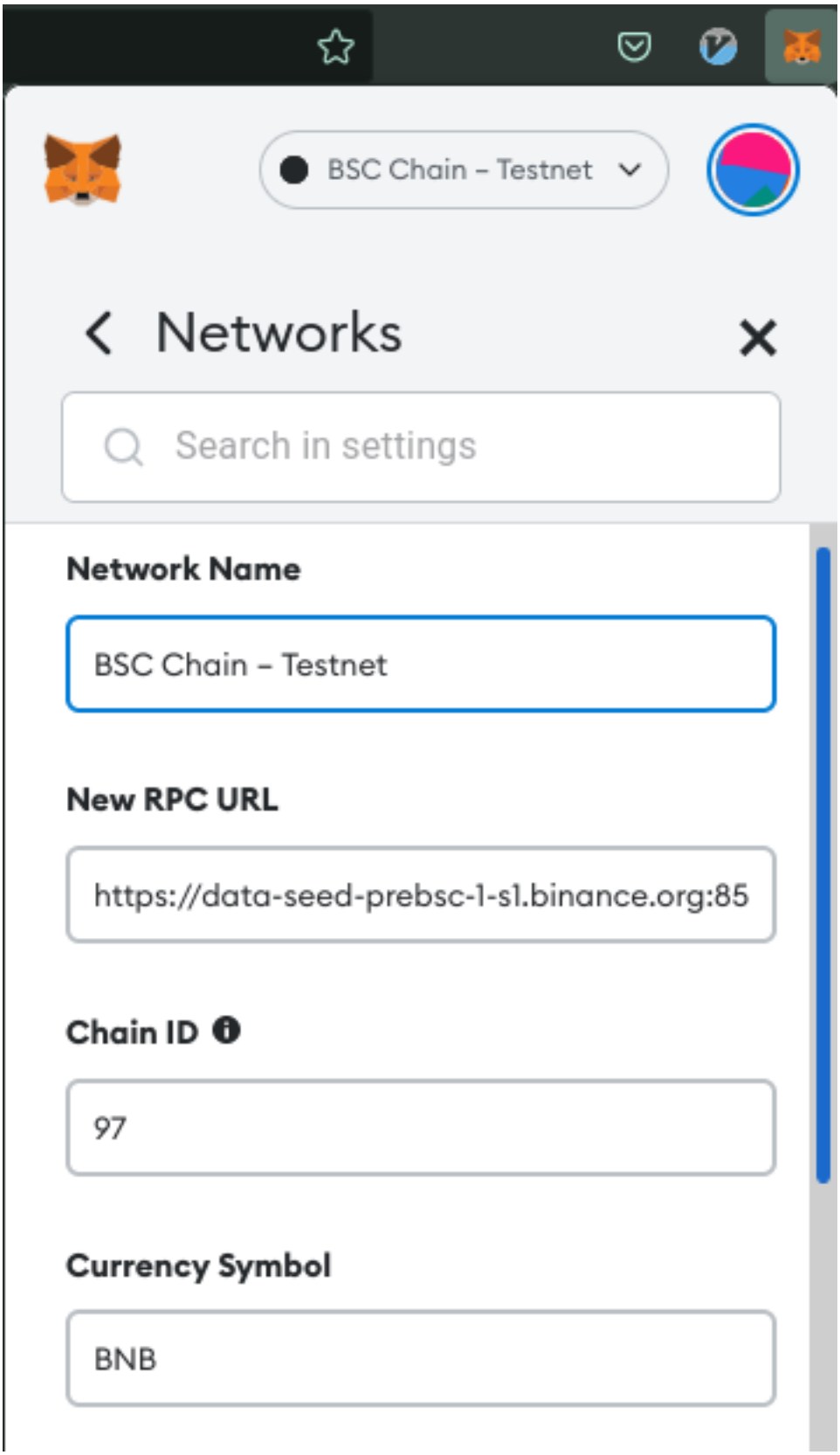
```
" Press ? for help

.. (up a dir)
/home/vecna/Dev/rantaianblok/
▶ [  ]node_modules/
▶ [  ]public/
▼ [  ]src/
  ▶ [  ]assets/
  ▶ [  ]boot/
  ▶ [  ]components/
  ▶ [  ]css/
  ▶ [  ]layouts/
  ▼ [  ]pages/
      ErrorNotFound.vue
      IndexPage.vue
  ▶ [  ]router/
  ▼ [  ]utils/
      rantai.json
    App.vue
    index.template.html
  babel.config.js
  jsconfig.json
  package-lock.json
  package.json
  quasar.config.js
  README.md
/home/vecna/Dev/rantaianblok
```

```vue
<template>
  <q-page class="flex flex-center">
    <div class="column">
      <q-btn @click='getFlag' class="col" color="primary" label="Flag pls" />
      <p class="col">{{ flag }} </p>
    </div>
  </q-page>
</template>

<script>
import { defineComponent } from 'vue'
import { ethers } from 'ethers'
import abi from '../utils/rantai.json'

const contractAddress = '0xC669100117c2e8b0492bD2f03a9a64B459776e62'
const contractABI = abi.abi


export default defineComponent({
  name: 'IndexPage',

  data() {
    let contract = null;
    let flag = null;
    return {
      contract, flag
    }
  },

  created() {
    this.checkIfWalletIsThere()
  },

  methods: {
   checkIfWalletIsThere() {
      window.addEventListener('load', () => {
        const { ethereum } = window
        if (!ethereum) {
          console.log('No metamask')
          return
        }
        console.log('We have an ethereum object!!', ethereum)
      })
    },

    createContract() {
      const { ethereum } = window

      const provider = new ethers.providers.Web3Provider(ethereum)
      const signer = provider.getSigner()
      this.contract = new ethers.Contract(contractAddress, contractABI, signer)
      return this.contract
    },

    async getFlag() {
        let r = this.createContract();
        this.flag = await r.flag();
        console.log('flag', this.flag)
    },
  },
})
src/pages/IndexPage.vue
```

- run the apllication with **QUASAR DEV**
- on the browser, metamask will be needed for us to connect into the BSC test network, upon installed and register account on metamask, click the **CONNECTED SITES** like image below and click connect to **LOCALHOST:8080**




- connecting to the test network by adding a new network in metamask setting like so.


BSC Chain – Testnet
Networks
Search in settings
Network Name
BSC Chain – Testnet
New RPC URL
https://data-seed-prebsc-1-s1.binance.org:85
Chain ID
97
Currency Symbol
BNB

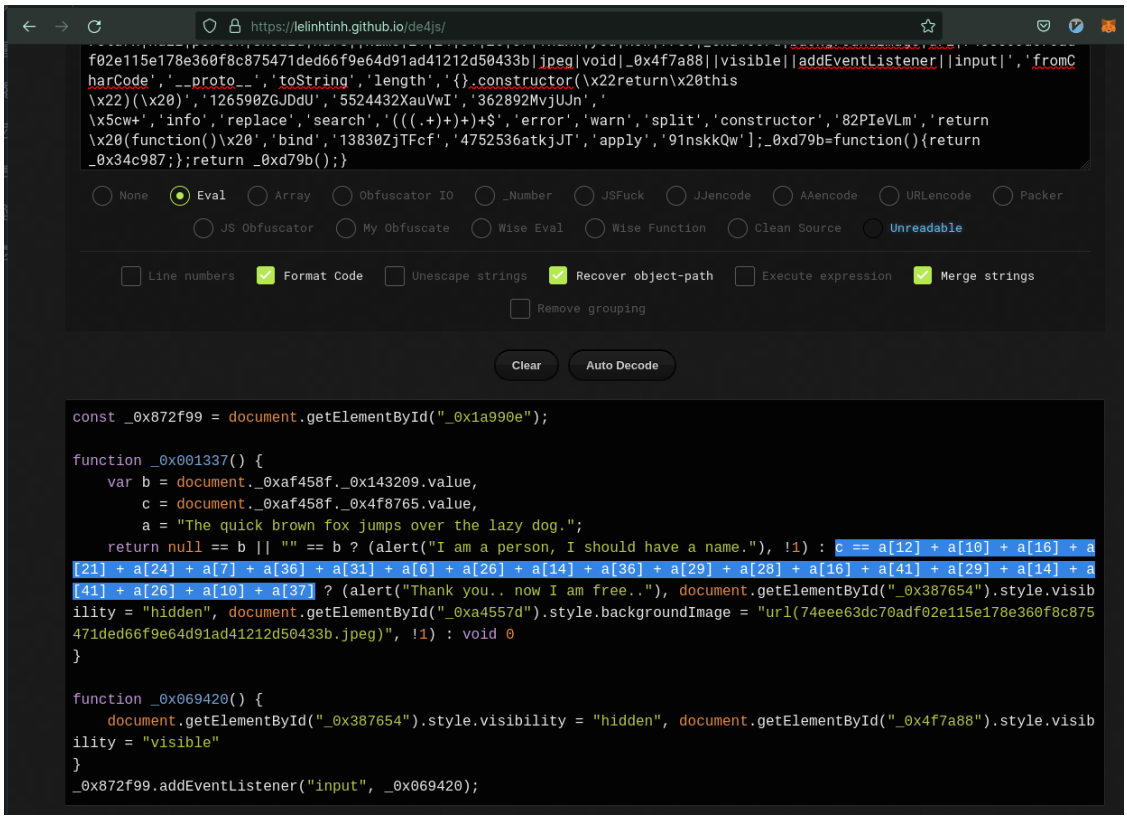
- if all works as intended, we should get our flag from the address by calling its public **FLAG()** function.


- a good resource to learn more about web3 for free -> **HTTPS://BUILDSPACE.SO**

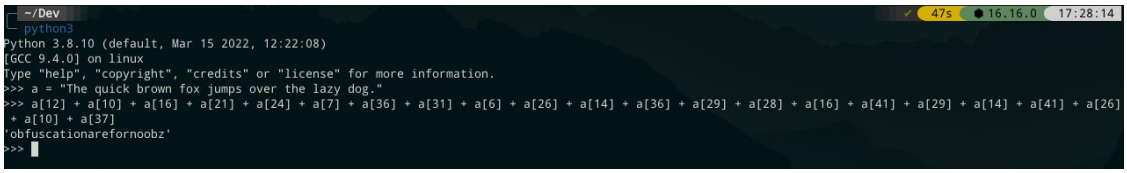
# AND EKCELI


**STEPS OF REPLICATION**

- input the password -> **DOWN HERE**
- inspect the element and go into the **DEBUGGER** tab. take note of the troll face as there is only one long function that doesn't have troll face below it.
- copy the function and throw it into de4js **HTTPS://LELINHTINH.GITHUB.IO/DE4JS/**



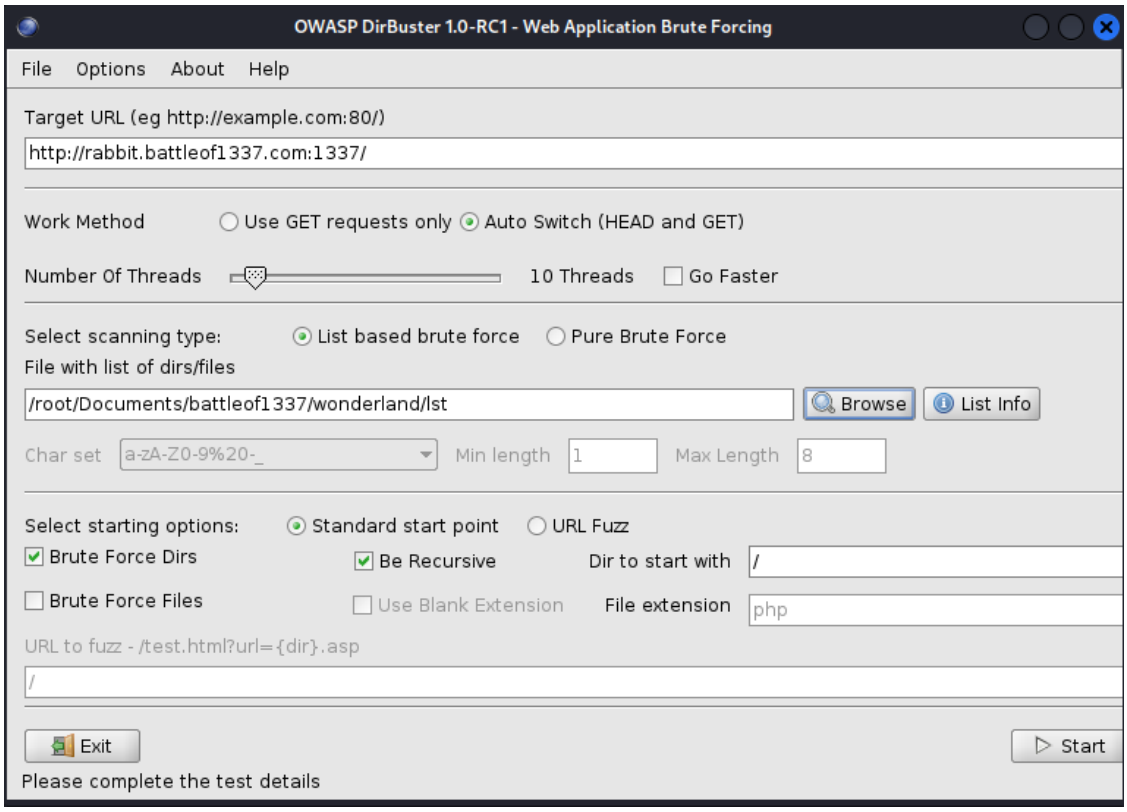

- retrieve the flag like the image below



# ALICEINWONDERLAND


**STEPS OF REPLICATION**

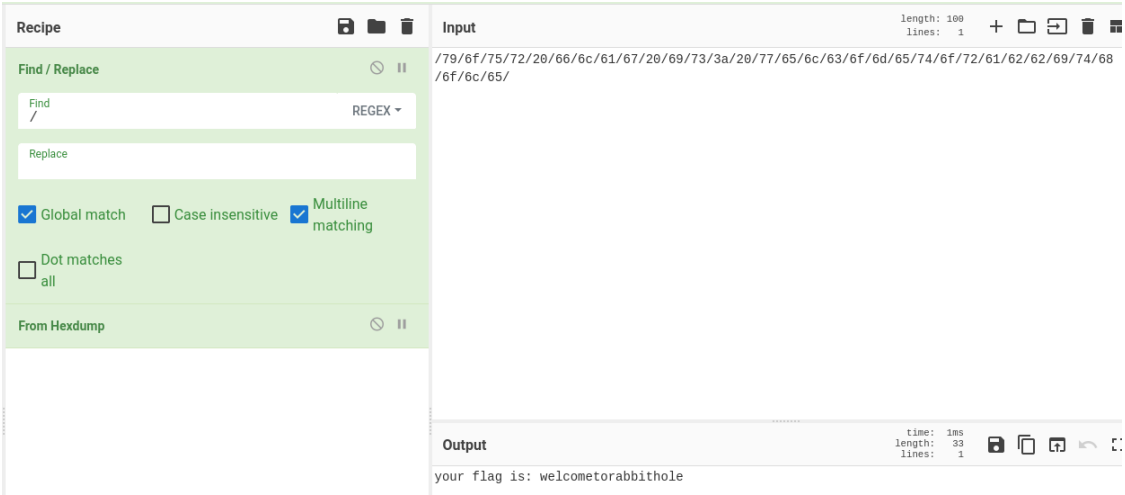
- head over to /ROBOTS.TXT and copy all of them and put it in a wordlist
- i use DIRBUSTER to bruteforce the directory as FFUF and GOBUSTER didn't work for me (not sure why)



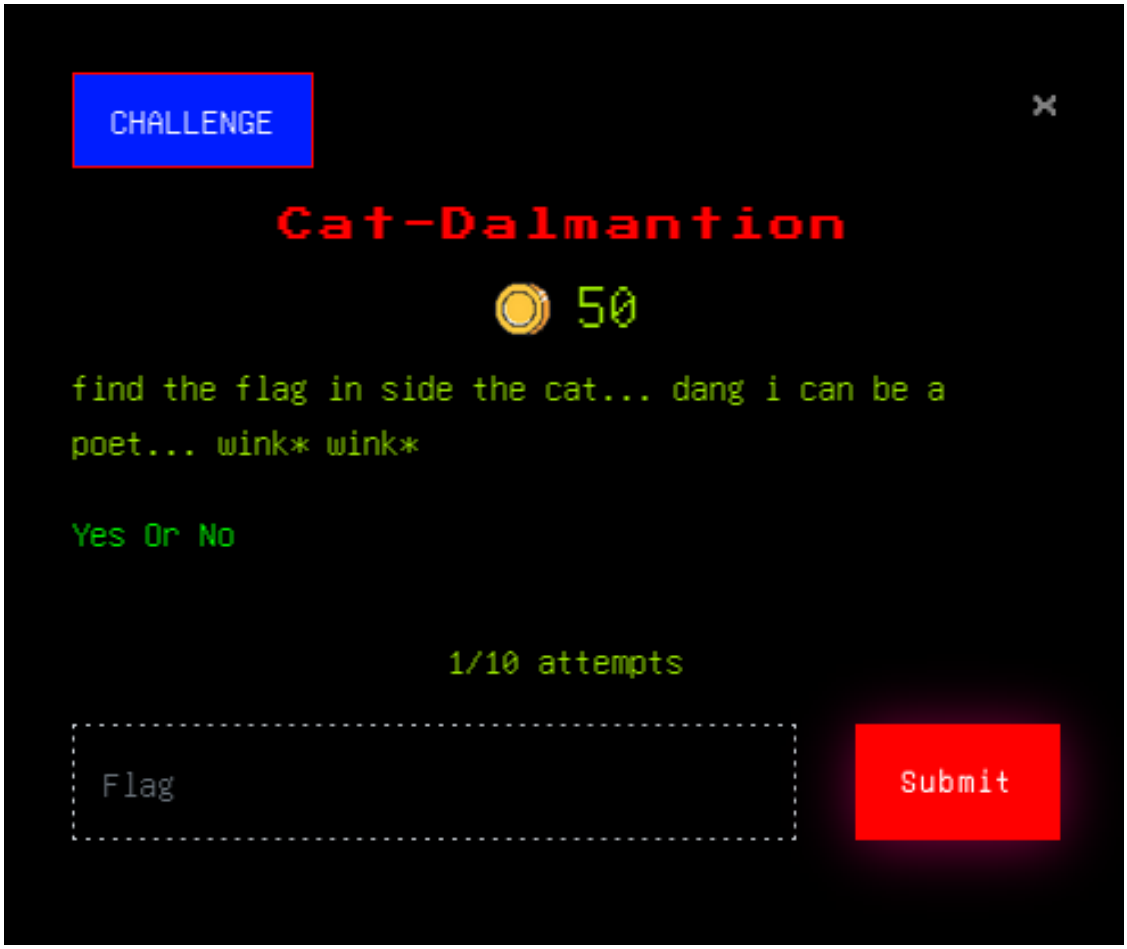

- we will need to follow a **403 FORBIDDEN** response

```
Dir found: /79/6f/ - 403
Dir found: /79/6f/75/ - 403
Dir found: /79/6f/75/72/ - 403
Dir found: /79/6f/75/72/20/ - 403
Dir found: /79/6f/75/72/20/66/ - 403
Dir found: /79/6f/75/72/20/66/6c/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/74/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/74/68/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/74/68/6f/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/74/68/6f/6c/ - 403
Dir found: /79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/61/62/62/69/74/68/6f/6c/65/ - 200
DirBuster Stopped
```

- the achieved final url looks like this **HTTP://RABBIT.BATTLEOF1337.COM:1337/79/6F/75/72/20/66/6C/61/67/20/69/73/3A/20/77/65/6C/63/6F/6D/65/74/6F/72/61/62/62/69/74/68/6F/6C/65/**
- head over to cyberchef and replace / into nothing then convert it **FROM HEXDUMP** and we got our flag

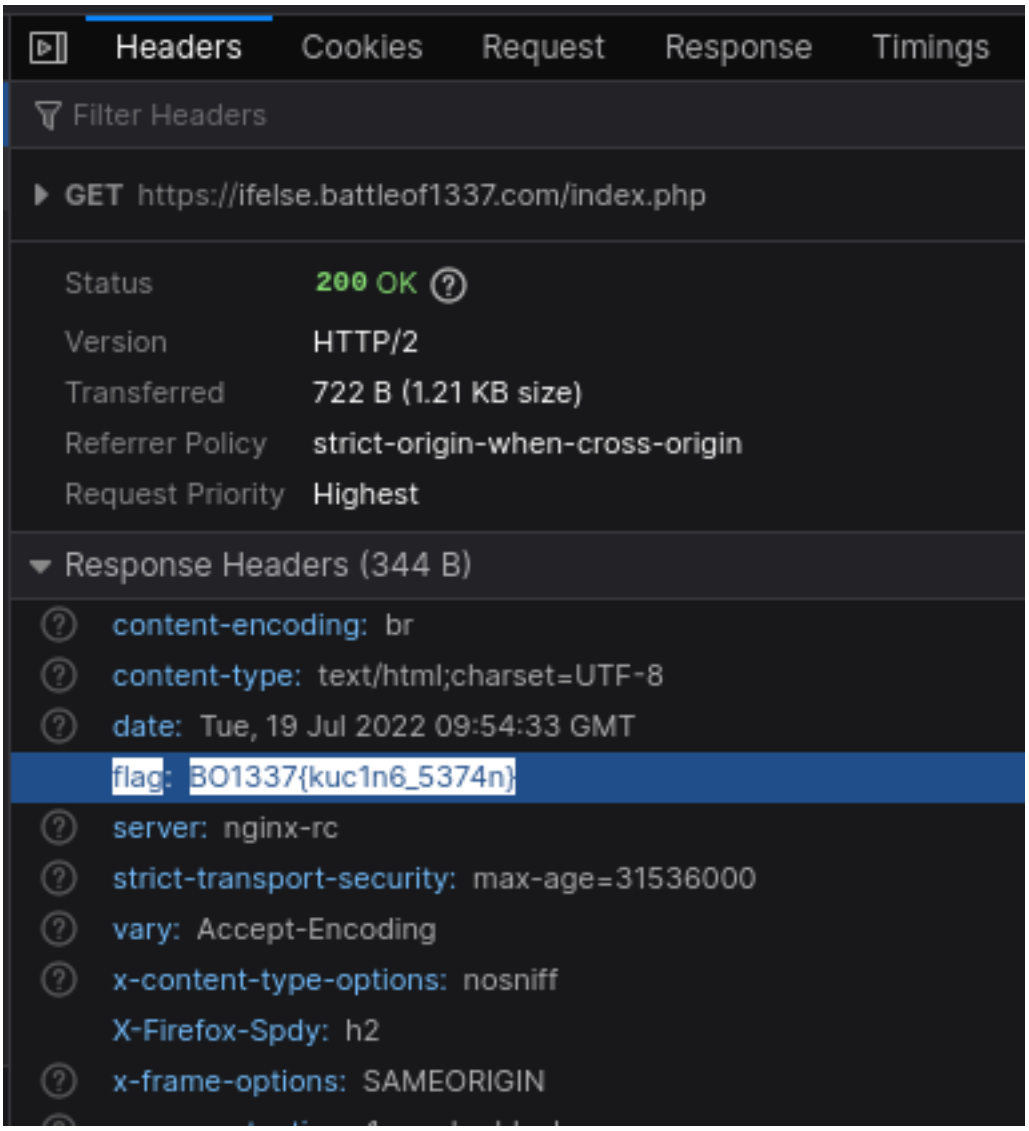


# CAT-DALMANTION




**STEPS OF REPLICATION**

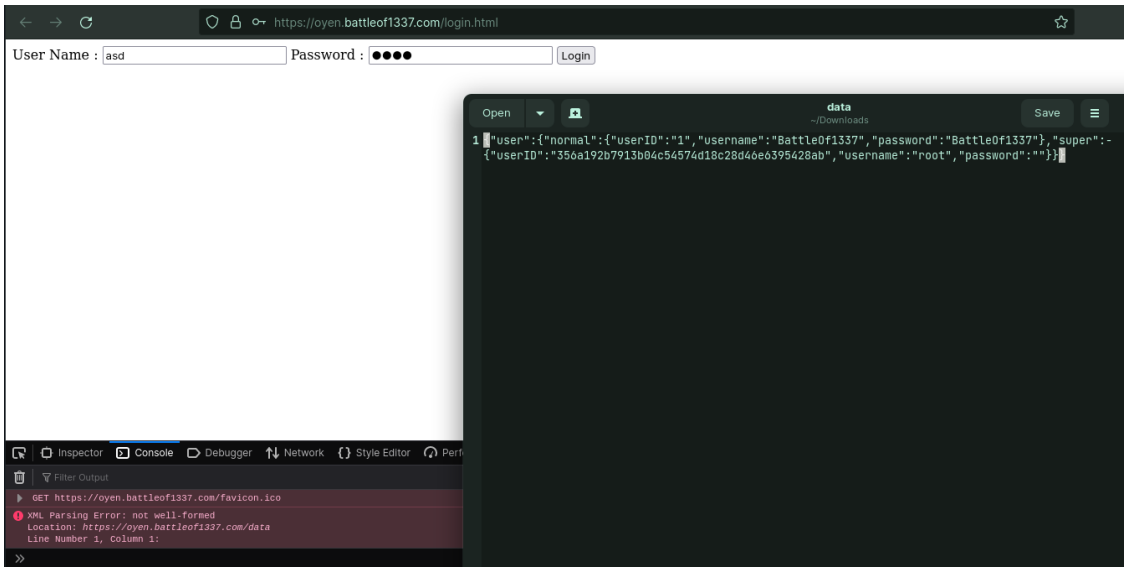
- we click click both button while viewing NETWORK tab in the inspect element will reveal the flag inside the response headers.


Headers
Cookies
Request
Response
Timings
Filter Headers
GET https://ifelse.battleof1337.com/index.php
Status 200 OK
Version HTTP/2
Transferred 722 B (1.21 KB size)
Referrer Policy strict-origin-when-cross-origin
Request Priority Highest
Response Headers (344 B)
content-encoding: br
content-type: text/html;charset=UTF-8
date: Tue, 19 Jul 2022 09:54:33 GMT
flag: BO1337{kuc1n6_5374n}
server: nginx-rc
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-frame-options: SAMEORIGIN

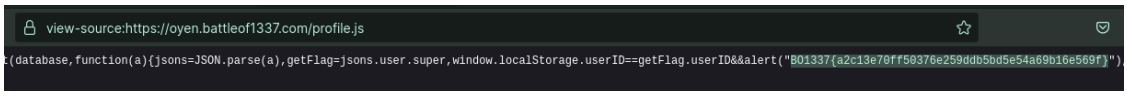
# BREAK THE STORAGE


**STEPS OF REPLICATION**

- there are a XML parsing error in the CONSOLE tab, visiting the url that will download us a file which turns out to be the credentials for us to login.




- upon successful login, viewing the source code reveal a JS file which contains the flag



# REDPOINT


**STEPS OF REPLICATION**

- this challenge shows us the flag which is the SCREWDRIVER

# HEIHAWRU


**STEPS OF REPLICATION**

- the encoded text from downloaded file is **ROT13** crypto with 6 rotation, hence by using cyberchef we will retrieved the decoded text like below image

```
Assalamualaikum, dari jeneral
RAP, rythm and poetry
Terjemahannya ritma atas puisi
Jurucakap institusi puisi
Berjasa pada semua macam pensil 2B
Otak kanan tekan tubi pena jadi deltoid
Lagu minum protein rap suntik steroid
Dua kati creatine aku android
Datang sesekali impak asteroid (boom)
Aku kejam kuhilang kau rindu
Lepas tampar mau cium satu minggu
Jangan begitu jangan mengada
Macam mana boleh rindu Mawi kan ada kan?
(Assalamualaikum)
Realitinya ini 083
Bintang realiti kujadikan sarapan
Makan lima mangkuk tanya, mana sarapanku?
Makan lima mangkuk lagi, mana sarapanku?
Aku lapar, ya mana musuh terkini?
Aku bakar terbalikkan di pasar macam mussolini
Mana kundalini? tak kunjung tiba
Sakti jadi hiba tapi fokus
Chakra berputar-putar kejar titik lokus
Tafakur, asmara, semua posisi lotus
Yup, best of both worlds I'm the dopest
Look into the mirror, yup yup you the closest
I flip language like sandwich
Either side same phat shit like goddamn it
And if you got a problem with me being malay dude
Lets take it back to 1511
Ya, ya 1511
Jom bertikam lidah dengan hamba dalam aku
Aku pantang kalah, bangun bila jatuh
Kalau patah sayap bertongkatkan paruh (shhh)
Ku punya teman yang punya teman
Yang boleh buat engkau hilang teman
Jadi dari buat lawan, baik buat kawan
Dari bagi jari, baik angkat tangan
Sepuluh jari ke atas macam kena tangkap
Kalau ingkar kupotong tujuh jadi pengakap
Ikan duri, gelama, senohong, siakap
Rapper penipu pembohong semua ku pap pap
Bukan terhandal, bukan 7erkuat
Cuma terhandal dalam apa yang ku buat
Jadi bila general berucap, sampai darah gusi
Tolong ceraikan buntut dari kerusi
Bangun
Assalamualaikum, dari jeneral
RAP, rythm and poetry
Terjemahannya ritma atas puisi
Jurucakap institusi puisi
Berjasa pada semua macam pensil 2B
Otak kanan tekan tubi pena jadi deltoid
Lagu minum protein rap suntik steroid
Dua kati creatine aku android
Datang sesekali impak asteroid (boom)
Aku kejam kuhilang kau rindu
Lepas tampar mau cium satu minggu
Jangan begitu jangan mengada
Macam mana boleh rindu Mawi kan ada kan?
(Assalamualaikum)
```

- in the downloaded file, there are some code for us whereas the code is used to find the location of characters of the flag

**5:6:2 6:1:1 31:3:1 15:3:3 15:3:3 43:4:1 27:2:1 32:3:1 33:1:1 41:3:1 38:3:4 24:2:2 10:5:4 41:5:3 45:6:3 35:1:1 15:3:3 1:3:3 36:2:2 34:1:1 45:2:3 21:2:2 17:1:2 11:4:2**

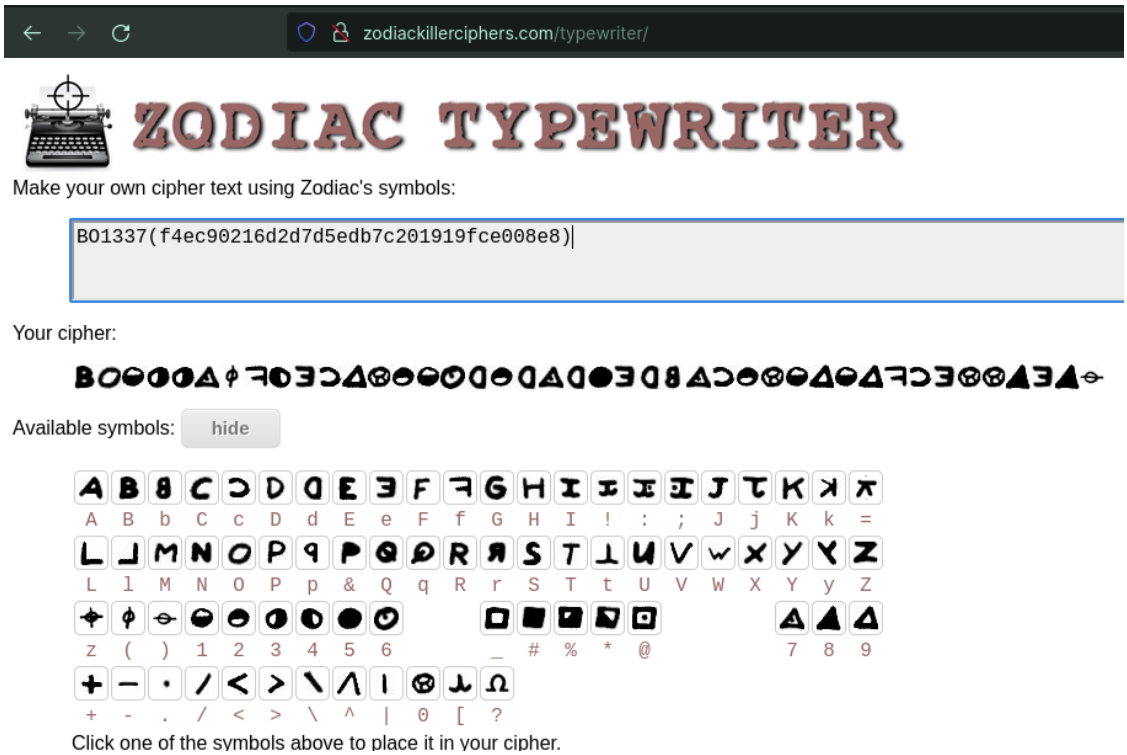
**COPY**

- decoding it manually revealed the flag - > **BO1337FLAGISDARK3NOKLUAI**

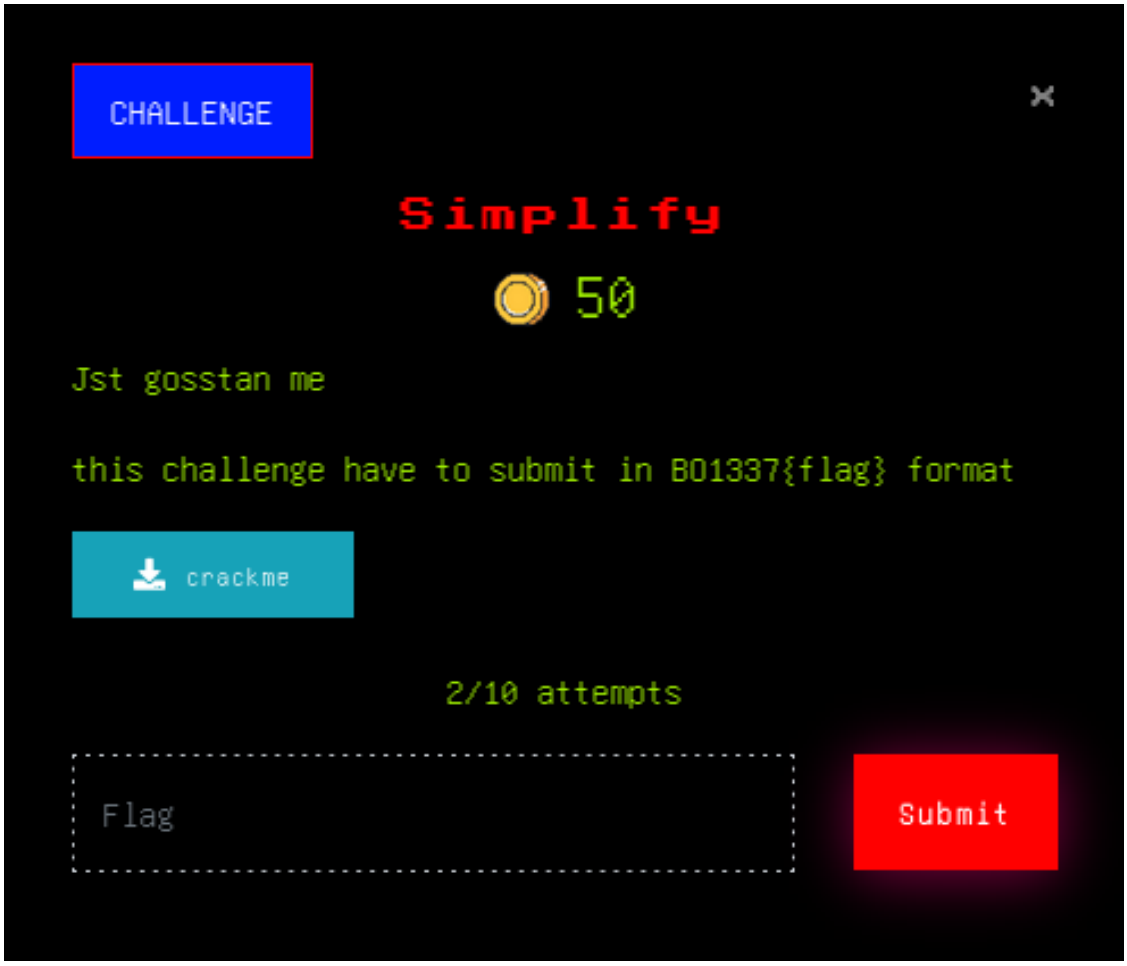
# SHENG XIAO


**STEPS OF REPLICATION**

- using an online tool to decode the code HTTP://ZODIACKILLERCIPHERS.COM/TYPEWRITER/


zodiackillerciphers.com/typewriter/
ZODIAC TYPEWRITER
Make your own cipher text using Zodiac's symbols:
BO1337(f4ec90216d2d7d5edb7c201919fce008e8)
Your cipher:
Available symbols:
hide
A B b C c D d E e F f G H I ! : ; J j K k =
L l M N O P p & Q q R r S T t U V W X Y y Z
z ( ) 1 2 3 4 5 6 _ # % * @ 7 8 9
+ - . / < > \ ^ | 0 [ ?
Click one of the symbols above to place it in your cipher.

# SIMPLIFY




**STEPS OF REPLICATION**

- upload the executable on **HTTPS://DOGBOLT.ORG**
- using hexrays reveal an interesting function

Hex-Rays

7.7.0.220218

```
150   unsigned int v4; // [rsp+18h] [rbp-18h] BYREF
151   unsigned int v5; // [rsp+1Ch] [rbp-14h] BYREF
152   unsigned int v6; // [rsp+20h] [rbp-10h] BYREF
153   unsigned int v7; // [rsp+24h] [rbp-Ch] BYREF
154   unsigned __int64 v8; // [rsp+28h] [rbp-8h]
155
156   v8 = __readfsqword(0x28u);
157   printf("Enter code: ");
158   __isoc99_scanf("%i-%i-%i-%i", &v4, &v5, &v6, &v7);
159   if ( 3 * v7 + v4 == 18044 && 3 * v6 * v5 == 5174190 && v4 == 1010 && v7 + 49363 * v6 == 63683948 )
160     printf("Correct code! The flag is %i-%i-%i-%i\n", v4, v5, v6, v7);
161   else
162     puts("Wrong code..");
163   return 0;
164 }
165 // 10B0: using guessed type __int64 __isoc99_scanf(const char *, ...);
166
167 //----- (00000000000012A0) ----------------------------------------------------
```

- all we have to do left is to solve the mathematics equation

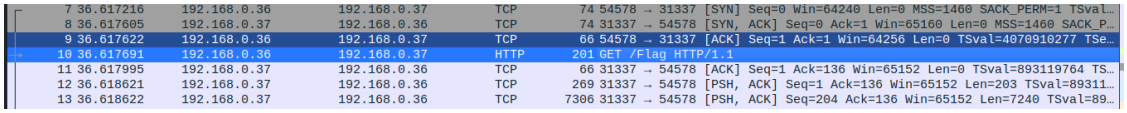
**v4 = 1010**
**v5 = 1337**
**v6 = 1290**
**v7 = 5678**
**COPY**

- input the code into the executable and we get our flag

# SEMERAH PADI

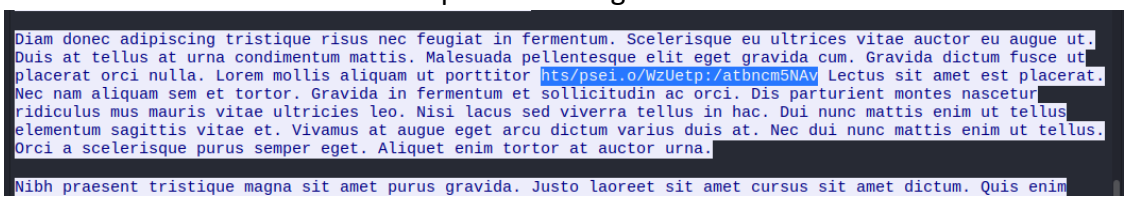

**STEPS OF REPLICATION**

- upon opening the **.PCAP** file, we see a request to **/FLAG**



| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | 36.617216 | 192.168.0.36 | 192.168.0.37 | TCP | 74 | 54578 → 31337 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval… |
| 8 | 36.617605 | 192.168.0.37 | 192.168.0.36 | TCP | 74 | 31337 → 54578 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_P… |
| 9 | 36.617622 | 192.168.0.36 | 192.168.0.37 | TCP | 66 | 54578 → 31337 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4070910277 TSe… |
| 10 | 36.617691 | 192.168.0.36 | 192.168.0.37 | HTTP | 201 | GET /flag HTTP/1.1 |
| 11 | 36.617995 | 192.168.0.37 | 192.168.0.36 | TCP | 66 | 31337 → 54578 [ACK] Seq=1 Ack=136 Win=65152 Len=0 TSval=893119764 TS… |
| 12 | 36.618621 | 192.168.0.37 | 192.168.0.36 | TCP | 269 | 31337 → 54578 [PSH, ACK] Seq=1 Ack=136 Win=65152 Len=203 TSval=89311… |
| 13 | 36.618622 | 192.168.0.37 | 192.168.0.36 | TCP | 7306 | 31337 → 54578 [PSH, ACK] Seq=204 Ack=136 Win=65152 Len=7240 TSval=89… |

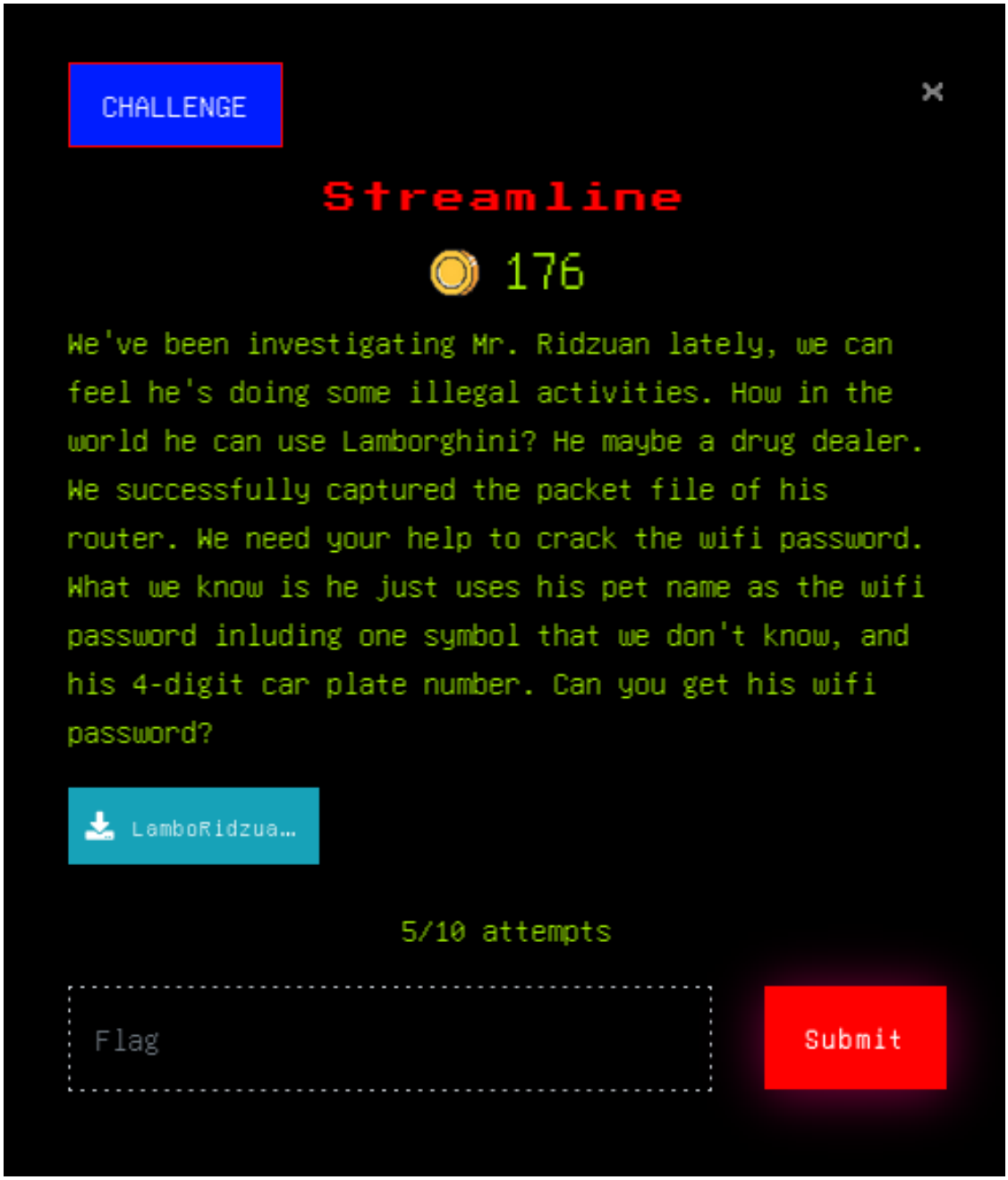
- follow the packets using **HTTP STREAM**, and we got a long ascii text, if we take a really really close look we can find somewhat peculiar string inside it.



```
Diam donec adipiscing tristique risus nec feugiat in fermentum. Scelerisque eu ultrices vitae auctor eu augue ut.
Duis at tellus at urna condimentum mattis. Malesuada pellentesque elit eget gravida cum. Gravida dictum fusce ut
placerat orci nulla. Lorem mollis aliquam ut porttitor hts/psei.o/WzUetp:/atbncm5NAv Lectus sit amet est placerat.
Nec nam aliquam sem et tortor. Gravida in fermentum et sollicitudin ac orci. Dis parturient montes nascetur
ridiculus mus mauris vitae ultricies leo. Nisi lacus sed viverra tellus in hac. Dui nunc mattis enim ut tellus
elementum sagittis vitae et. Vivamus at augue eget arcu dictum varius duis at. Nec dui nunc mattis enim ut tellus.
Orci a scelerisque purus semper eget. Aliquet enim tortor at auctor urna.

Nibh praesent tristique magna sit amet purus gravida. Justo laoreet sit amet cursus sit amet dictum. Quis enim
```

- i figured this is an url by the way it was scrambled and its characters. the way we can decode this is by reading the characters from front then back. we will get a pastebin link **HTTPS://PASTEBIN.COM/5WNZAUVE** which gives us two audio file
- i use several tools online to view its spectogram, but the one that working is **HTTPS://WWW.SONICVISUALISER.ORG/** and we got the flag.

# STREAMLINE




**STEPS OF REPLICATION**

- using STEGHIDE to reveal its hidden file inside the image

```
┌──(root㉿kali)-[~/Downloads]
└─# steghide extract -sf LamboRidzuan.jpg
Enter passphrase:
wrote extracted data to "handshake.cap".

┌──(root㉿kali)-[~/Downloads]
└─#
```

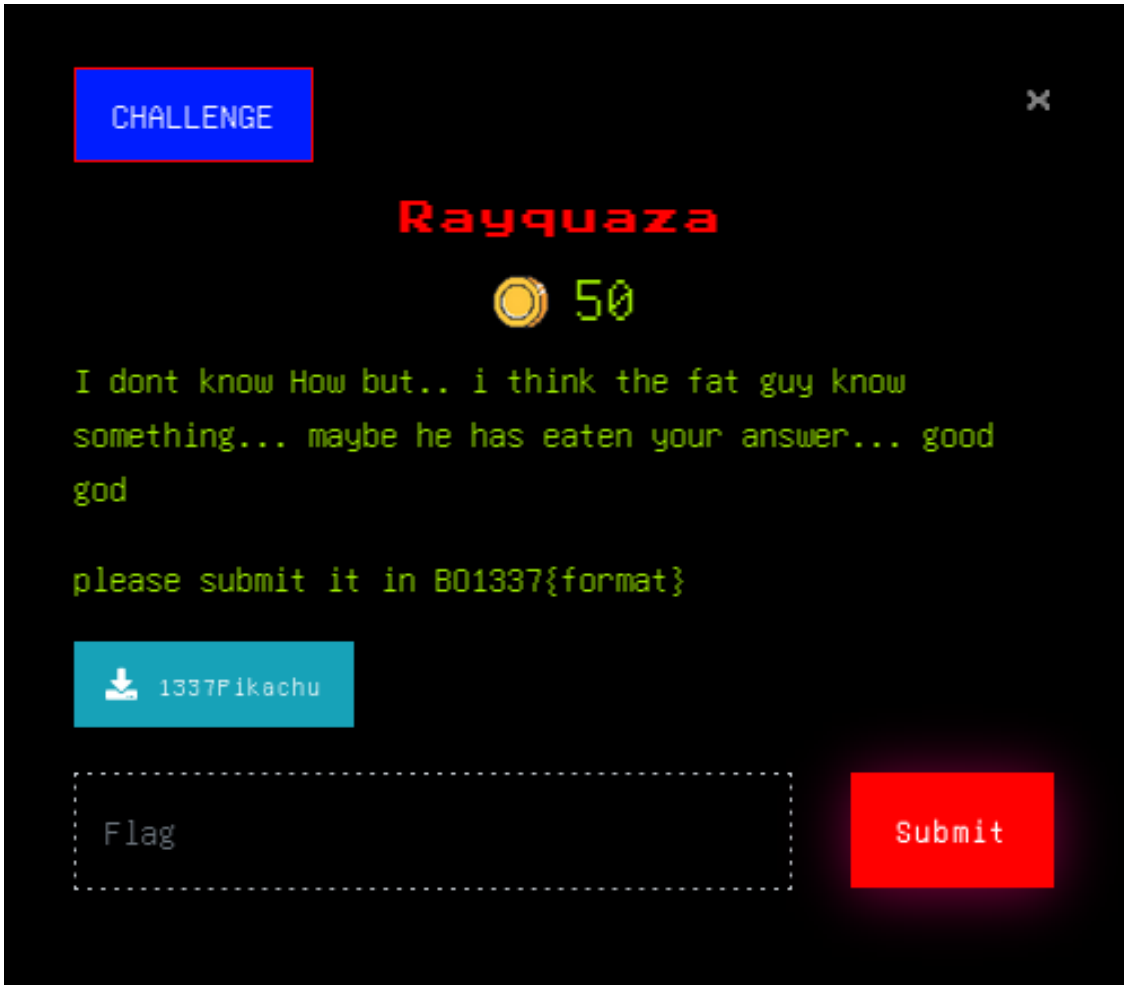
- based on the challenge description, we will need to crack the the handshake captured using the info given. seeing an orange cat and there's one challenge called oyen, we can safely assume that the name of the cat is oyen. hence we can generate a wordlist like image below using **CRUNCH**

```
┌──(root㉿kali)-[~/Downloads]
└─# crunch 9 9 -t oyen^%%%% > pls.txt
Crunch will now generate the following amount of data: 3300000 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330000

┌──(root㉿kali)-[~/Downloads]
└─#
```

- we can next crack the **.CAP** file using **AIRCRACK-NG**

```
                              Aircrack-ng 1.6

      [00:00:03] 20520/330000 keys tested (6152.09 k/s)

      Time left: 50 seconds                                      6.22%

                          KEY FOUND! [ oyen@9367 ]


      Master Key     : E7 F0 93 EC 46 85 39 40 10 90 31 B3 62 CE E0 13
                       77 9E A4 F8 A5 07 00 F8 33 4B 1F 7A 22 BA D5 57

      Transient Key  : 0B 56 BD 4D AF AD 2B 8D 4E A8 CF EC 26 3E C3 5D
                       AC CC 49 8D D3 AD CC AB 73 B9 15 02 3B 90 1F 10
                       6A 1D BB 51 41 84 B3 5D EA D0 94 C4 B3 77 4B 62
                       71 E1 D6 5F 88 B8 D6 F8 57 D4 4F DF D4 A9 BF 98

      EAPOL HMAC     : 8B D0 54 60 09 84 7E 11 0A 17 83 CA 4A 7D 1B 11


┌──(root㉿kali)-[~/Downloads]
└─# aircrack-ng handshake.cap -w pls.txt
```

# RAYQUAZA



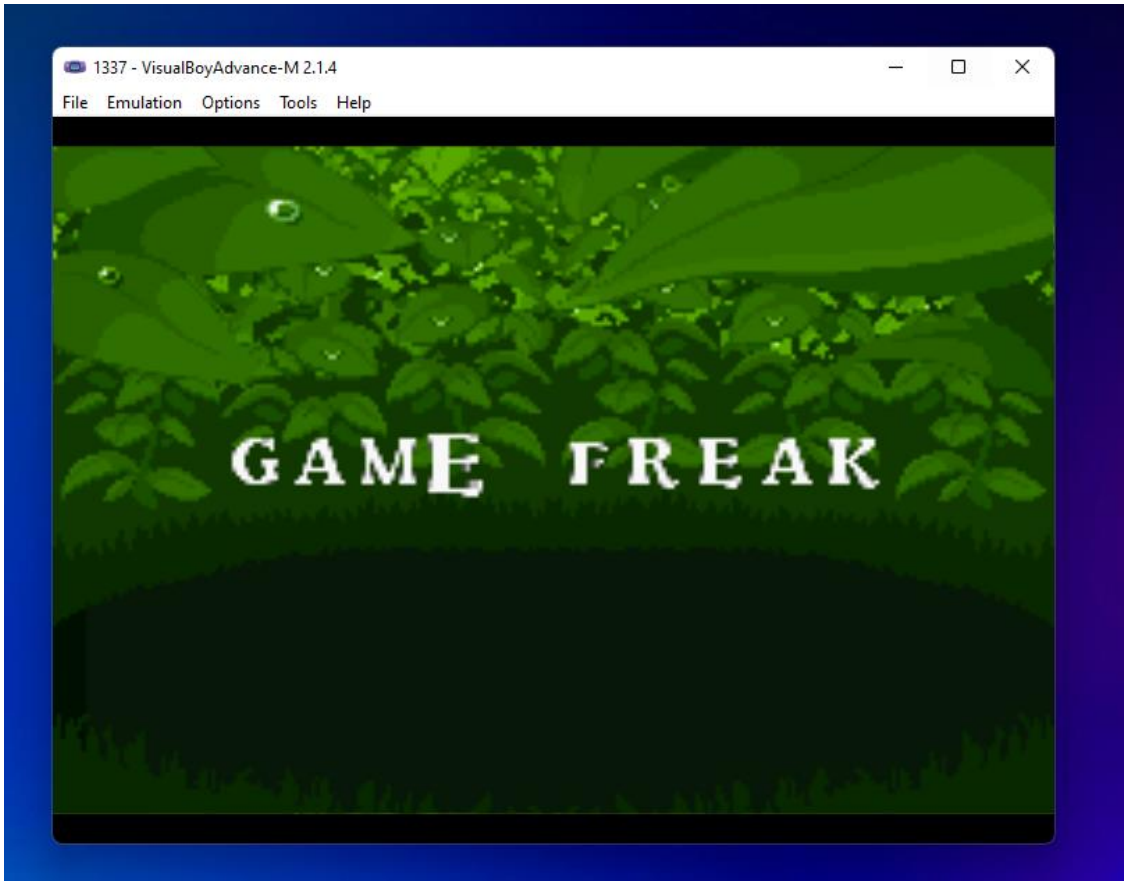

**STEPS OF REPLICATION**

- we can run FILE to the executable and take note of what its filetype is

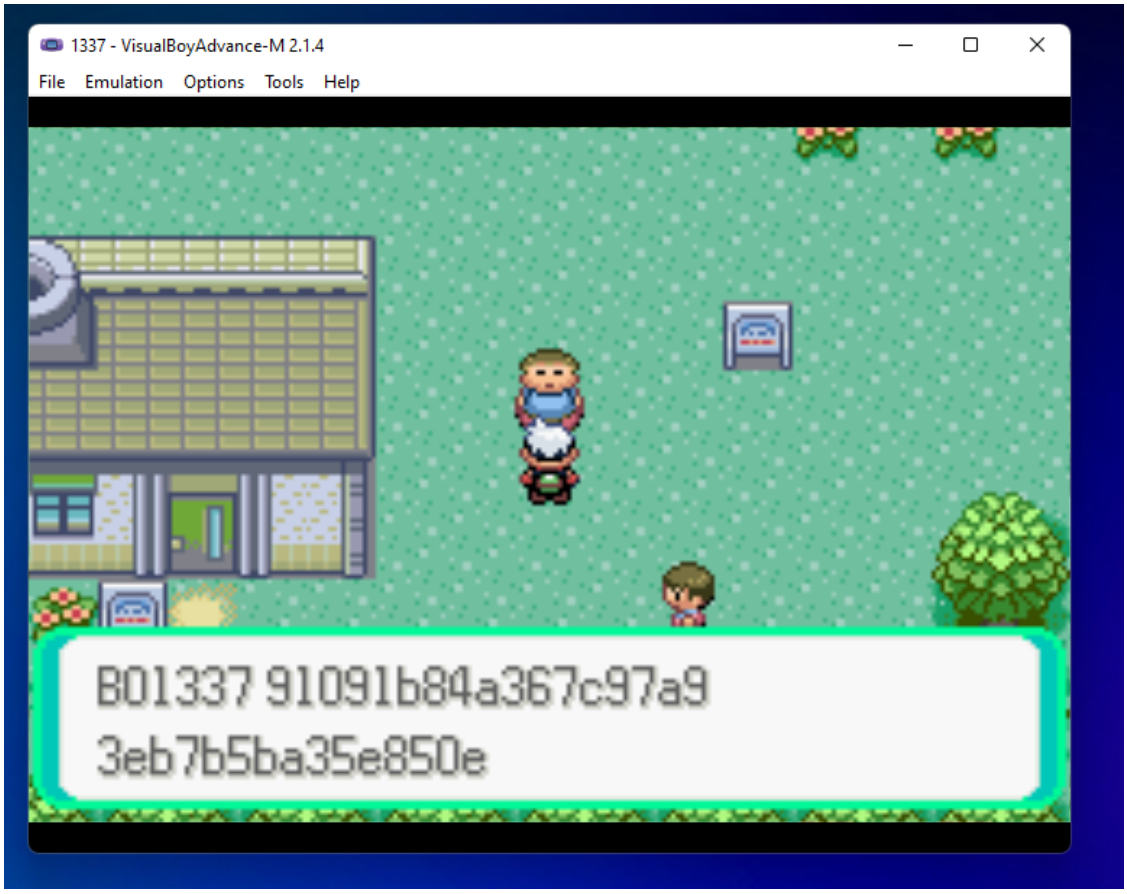
```
┌──(root㉿kali)-[~/Downloads]
└─# file 1337Pikachu
1337Pikachu: Game Boy Advance ROM image: "POKEMON EMER" (BPEE01, Rev.00)

┌──(root㉿kali)-[~/Downloads]
└─#
```

- googling Game Boy Advance's extension gives us .GBA which we can rename the file to.
- i use an emulator from github that has a release for windows, so i then next transferred the .GBA file into my windows vm. HTTPS://GITHUB.COM/VISUALBOYADVANCE-

### M/VISUALBOYADVANCE-M/RELEASES



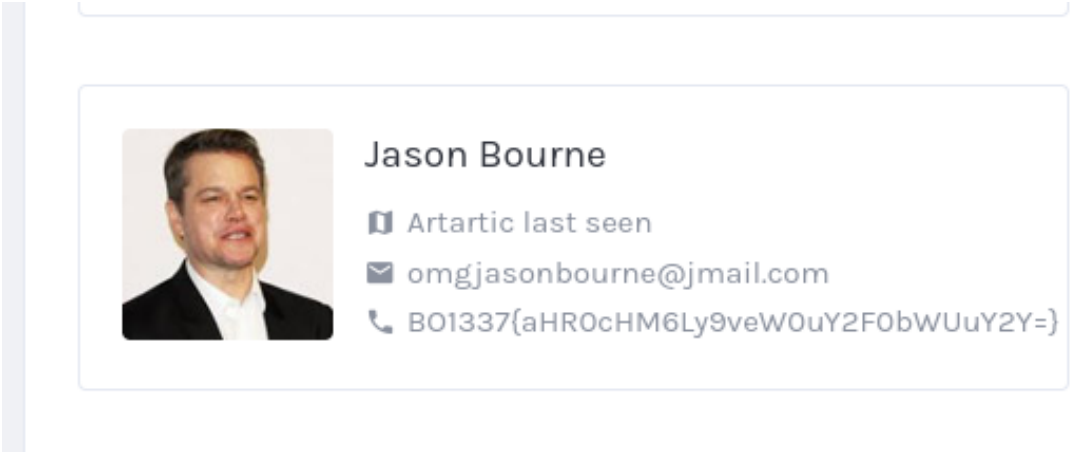
- we can get the flag by talking to a neighbour



# BACK TO THE FUTURE


**STEPS OF REPLICATION**

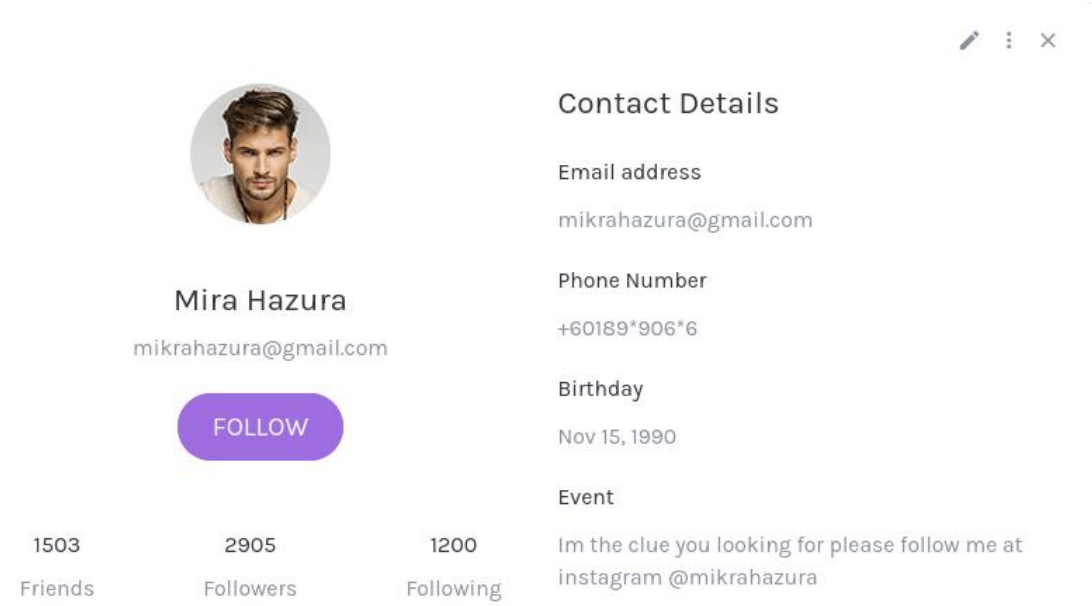
- by using the wayback machine, we can find the flag
  **HTTPS://WEB.ARCHIVE.ORG/WEB/20220704083124/HTTPS://B2F.BATTLEOF1337.COM/**



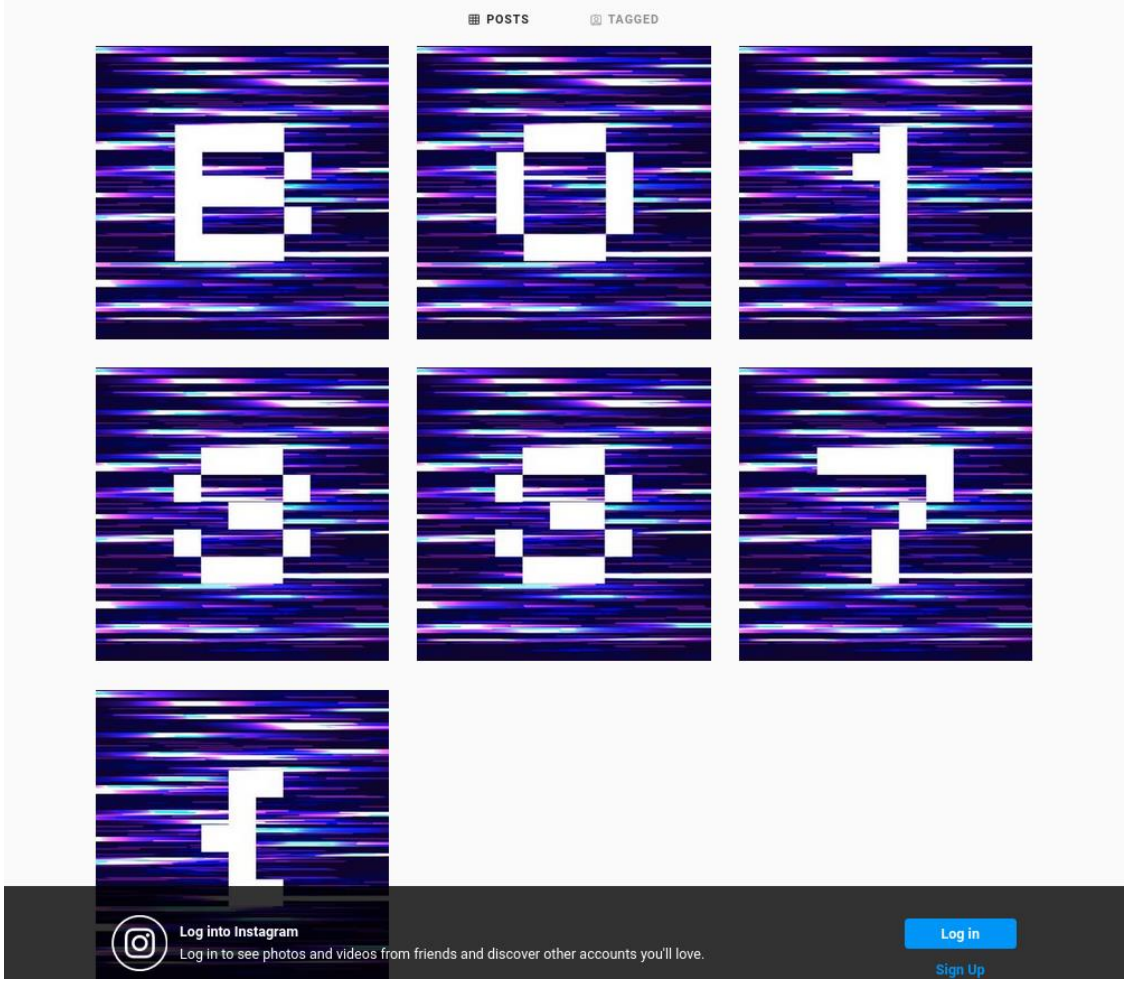
# 1GRAM


**STEPS OF REPLICATION**

- by clicking any one of the card, we get a hint to visit someone's Instagram




- in the user profile, we can see few images that reveals part of the flag.

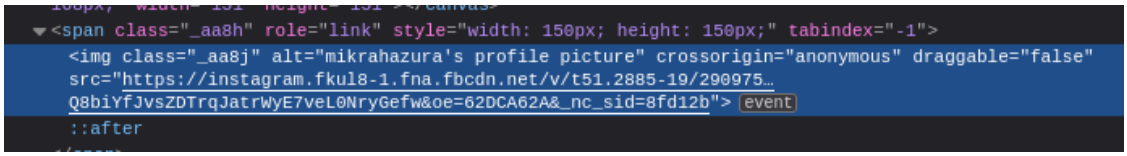


- in one of those images, there are few people tagged, hence by viewing each one of them, we can retrieve the full flag -> **BO1337{S74LK_4P4_7U?}**

# SNAP


**STEPS OF REPLICATION**

- on each of profiles that we retrieved the flag from previous challenge, notice that the user profile picture is somewhat related to each other. by inspecting the element and get the url path of the image, we can arrange the full image.



- all that's left is to arrange the image, so we can get the idea where it is the location. i use canva to arrange the images.

- the image that we are looking at is the station of Imbi hence the flag is -> **BO1337{IMBI}**