root@localhost:~$ echo “b477l3 0f l337”

BATTLE_OF_1337

CTF 2022

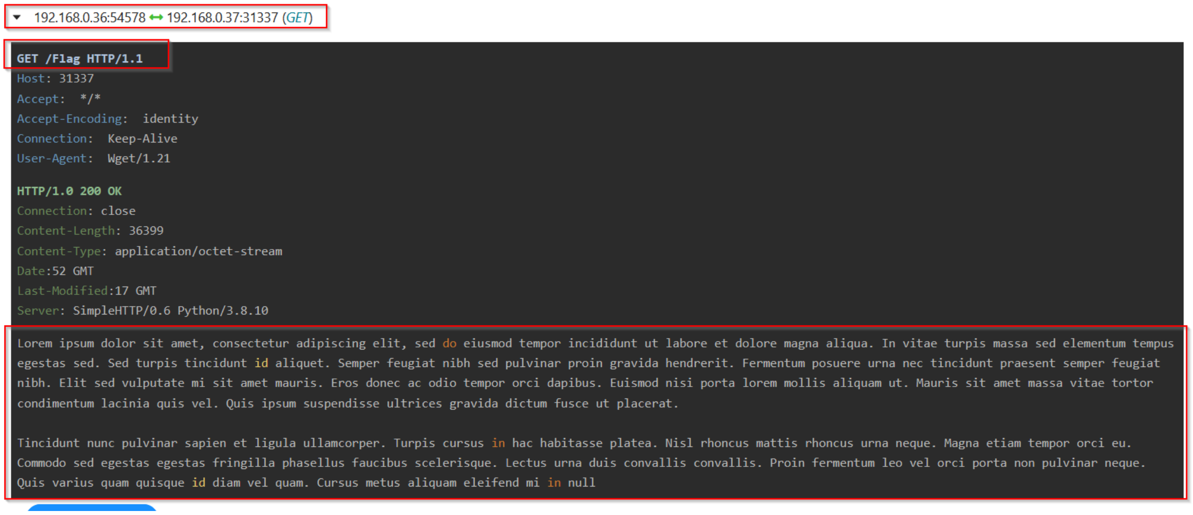
BATTLE OF 1337 OFFICIAL WRITEUP

Writeup By : 0xShu

TABLE OF CONTENT

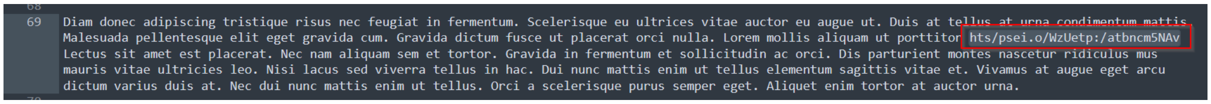
NET

SEMERAH PADI



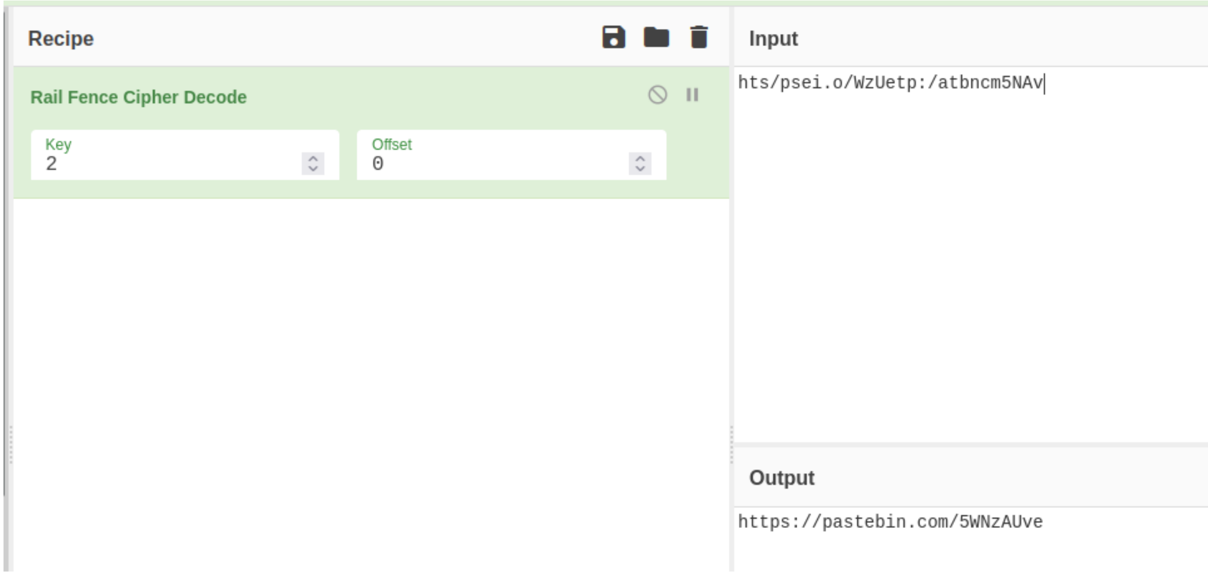
```
192.168.0.36:54578 ↔ 192.168.0.37:31337 (GET)

GET /Flag HTTP/1.1
Host: 31337
Accept:  */*
Accept-Encoding:  identity
Connection:  Keep-Alive
User-Agent:  Wget/1.21

HTTP/1.0 200 OK
Connection: close
Content-Length: 36399
Content-Type: application/octet-stream
Date:52 GMT
Last-Modified:17 GMT
Server: SimpleHTTP/0.6 Python/3.8.10

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. In vitae turpis massa sed elementum tempus
egestas sed. Sed turpis tincidunt id aliquet. Semper feugiat nibh sed pulvinar proin gravida hendrerit. Fermentum posuere urna nec tincidunt praesent semper feugiat
nibh. Elit sed vulputate mi sit amet mauris. Eros donec ac odio tempor orci dapibus. Euismod nisi porta lorem mollis aliquam ut. Mauris sit amet massa vitae tortor
condimentum lacinia quis vel. Quis ipsum suspendisse ultrices gravida dictum fusce ut placerat.

Tincidunt nunc pulvinar sapien et ligula ullamcorper. Turpis cursus in hac habitasse platea. Nisl rhoncus mattis rhoncus urna neque. Magna etiam tempor orci eu.
Commodo sed egestas egestas fringilla phasellus faucibus scelerisque. Lectus urna duis convallis convallis. Proin fermentum leo vel orci porta non pulvinar neque.
Quis varius quam quisque id diam vel quam. Cursus metus aliquam eleifend mi in null
```

Given .pcap file and using online tools to analysis and found some encrypted message.



```
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.
```

Deep down dive and notice that might possibility is URL.



Rail Fence Cipher Decode

Key 2

Offset 0

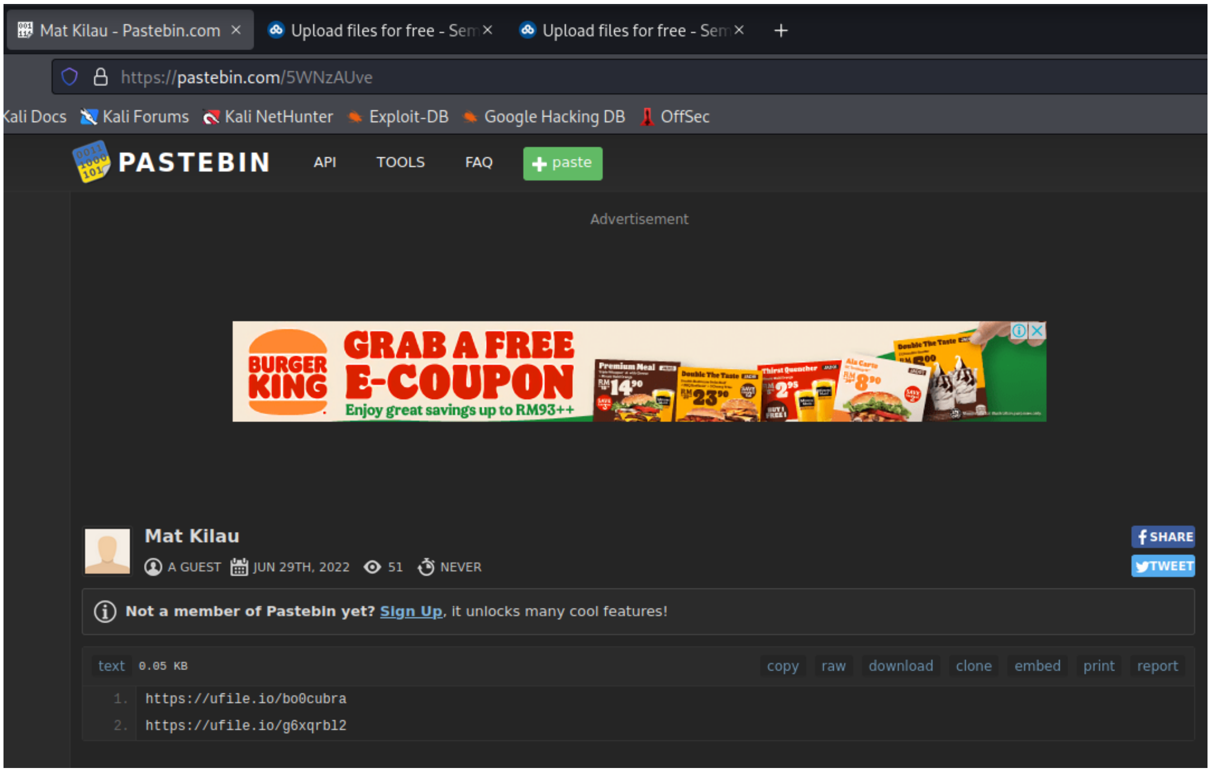
Input

```
hts/psei.o/WzUetp:/atbncm5NAv
```

Output

```
https://pastebin.com/5WNzAUve
```

As we know the encrypted type of message is Rail Fence Cipher by playing `Key` and show URL.



Mat Kilau

A GUEST JUN 29TH, 2022 51 NEVER

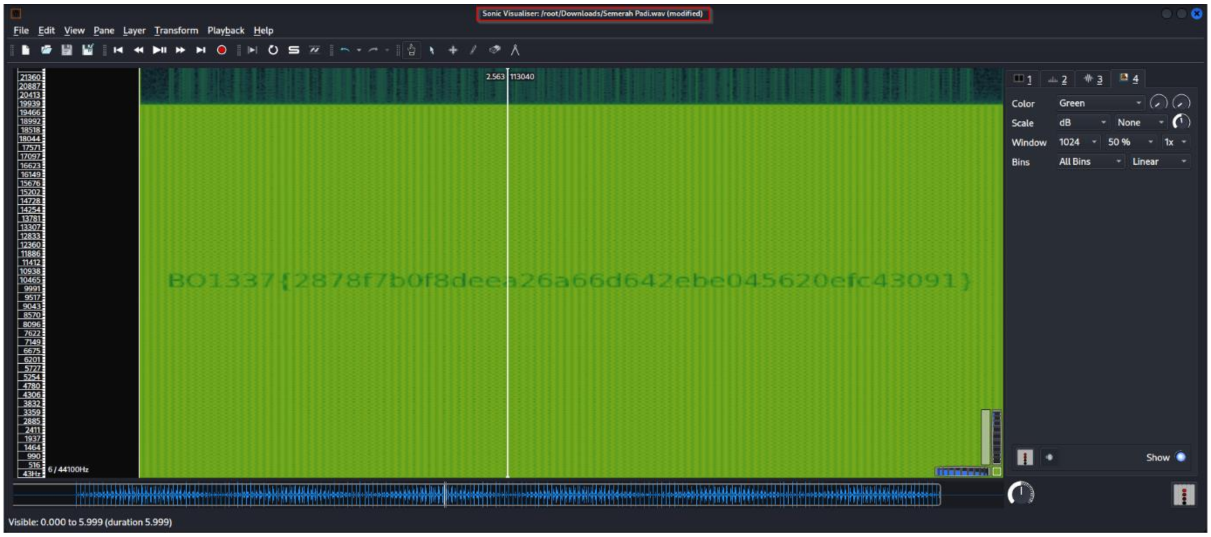
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.05 KB

```
https://ufile.io/bo0cubra
https://ufile.io/g6xqrbl2
```

Showed there 2 links. By selecting 2nd option link because of guessing name challenge.

https://ufile.io/g6xqrbl2



BO1337{2878f7b0f8deea26a66d642ebe045620efc43091}

Color Green

Scale dB None

Window 1024 50 % 1x

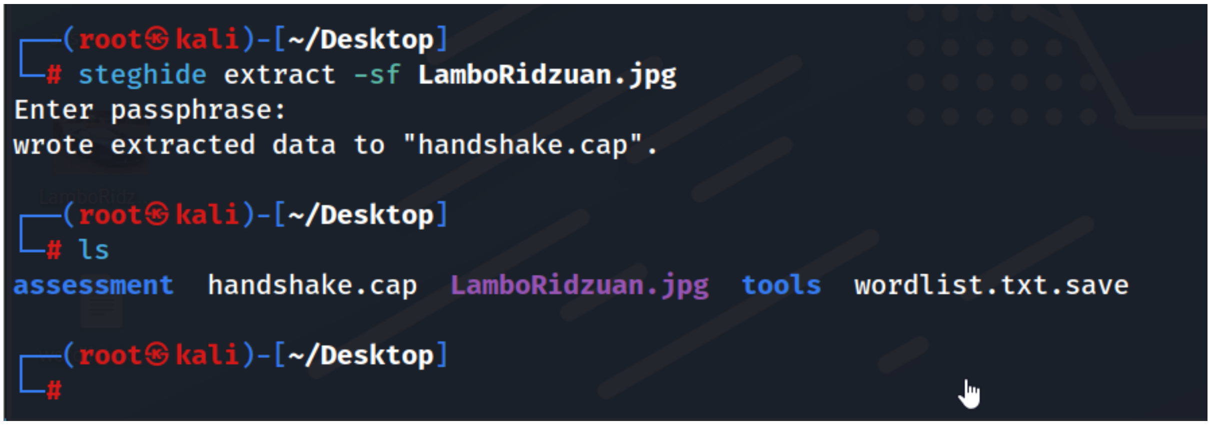
Bins All Bins Linear

Visible: 0.000 to 5.999 (duration 5.999)

Is showed .wav video and add spectrograms will show flag.

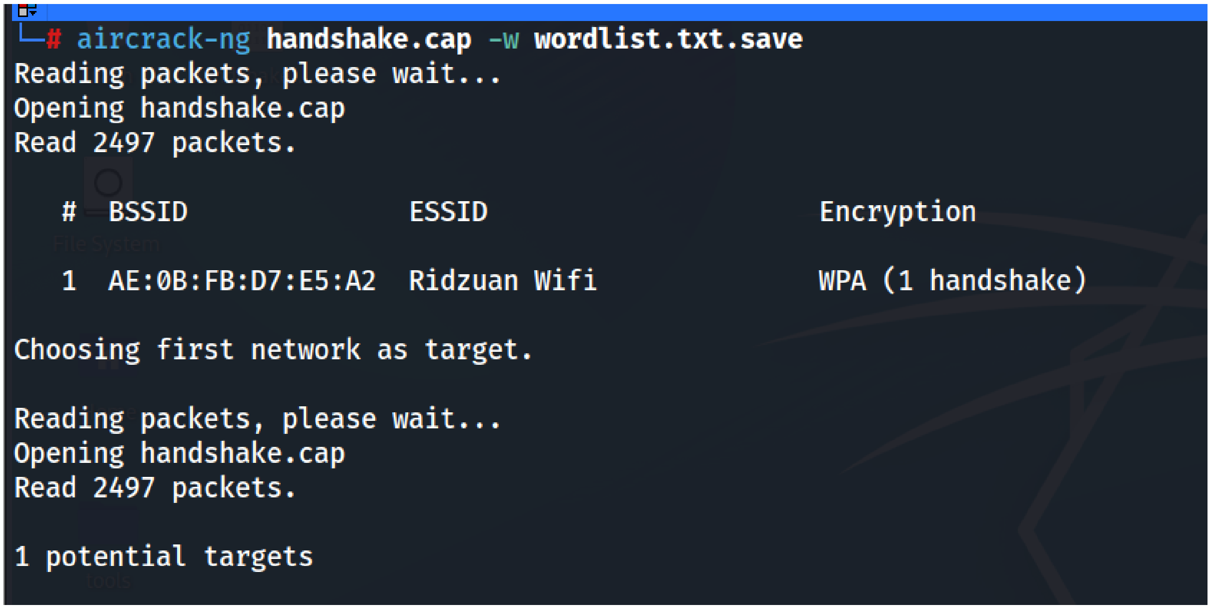
FLAG = BO1337{2878f7b0f8deea26a66d642ebe045620efc43091}

STREAMLINE



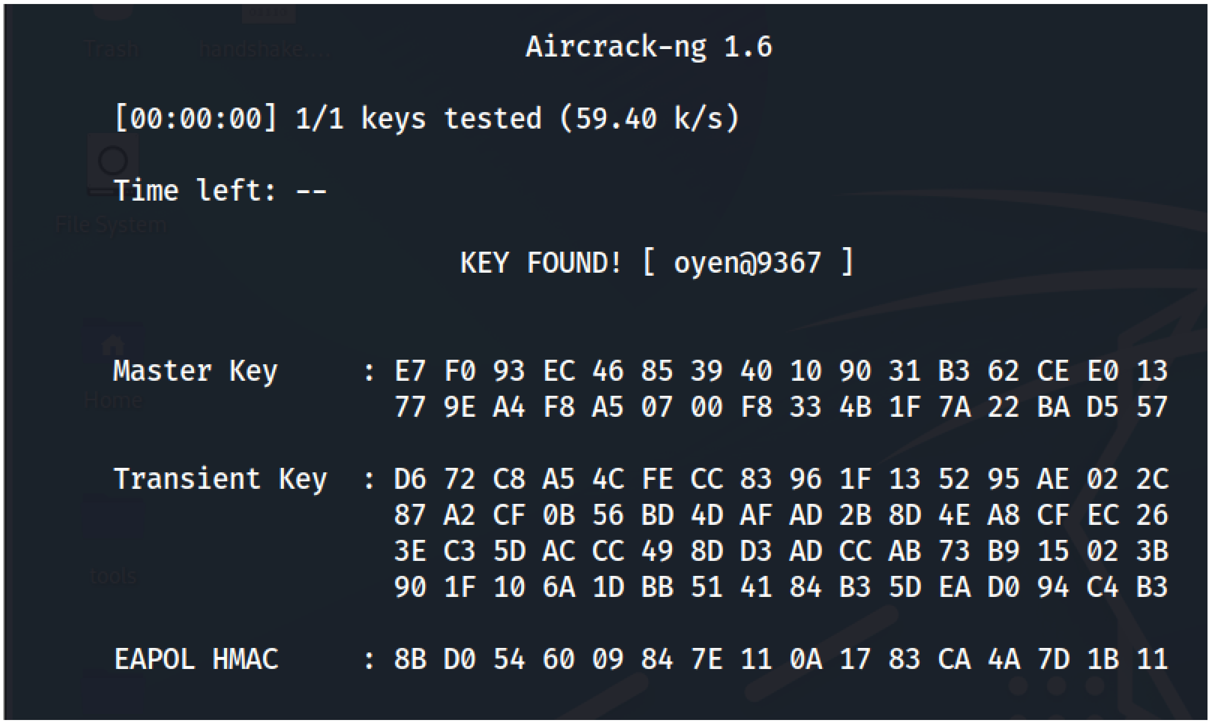
```
┌──(root㉿kali)-[~/Desktop]
└─# steghide extract -sf LamboRidzuan.jpg
Enter passphrase:
wrote extracted data to "handshake.cap".

┌──(root㉿kali)-[~/Desktop]
└─# ls
assessment  handshake.cap  LamboRidzuan.jpg  tools  wordlist.txt.save

┌──(root㉿kali)-[~/Desktop]
└─#
```

Given an image that contain .jpg file. However, from question itself asked for password Wifi. Wild guess is extract hidden file inside that image by using steghide.



```
└─# aircrack-ng handshake.cap -w wordlist.txt.save
Reading packets, please wait...
Opening handshake.cap
Read 2497 packets.

   #  BSSID              ESSID                     Encryption

   1  AE:0B:FB:D7:E5:A2  Ridzuan Wifi              WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening handshake.cap
Read 2497 packets.

1 potential targets
```

Is contain .cap file and showed that we need crack in order to obtain password of Wifi. However, with given hint what might possible password is oyen and 1 special character. We could create custom wordlist based on that requirement by using cruch tool.

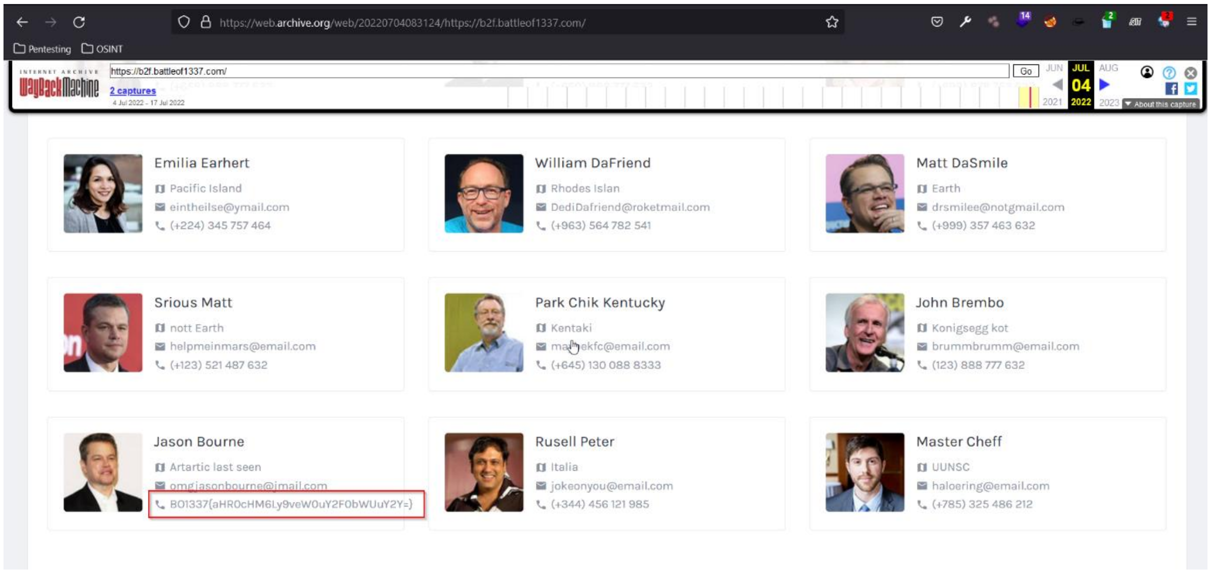


```
                                 Aircrack-ng 1.6

      [00:00:00] 1/1 keys tested (59.40 k/s)

      Time left: --

                             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  : D6 72 C8 A5 4C FE CC 83 96 1F 13 52 95 AE 02 2C
                       87 A2 CF 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

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

Flag = BO1337{oyen@9367}

OSINT

BACK TO THE FUTURE



https://web.archive.org/web/20220704083124/https://b2f.battleof1337.com/

Pentesting OSINT

https://b2f.battleof1337.com/ Go

2 captures

4 Jul 2022 - 17 Jul 2022

JUN JUL AUG

04

2021 2022 2023

About this capture

Emilia Earhert
Pacific Island
eintheilse@ymail.com
(+224) 345 757 464

William DaFriend
Rhodes Islan
DediDafriend@roketmail.com
(+963) 564 782 541

Matt DaSmile
Earth
drsmilee@notgmail.com
(+999) 357 463 632

Srious Matt
nott Earth
helpmeinmars@email.com
(+123) 521 487 632

Park Chik Kentucky
Kentaki
ma[illegible]ekfc@email.com
(+645) 130 088 8333

John Brembo
Konigsegg kot
brummbrumm@email.com
(123) 888 777 632

Jason Bourne
Artartic last seen
omgjasonbourne@jmail.com
BO1337(aHR0cHM6Ly9veW0uY2F0bWUuY2Y=)

Rusell Peter
Italia
jokeonyou@email.com
(+344) 456 121 985

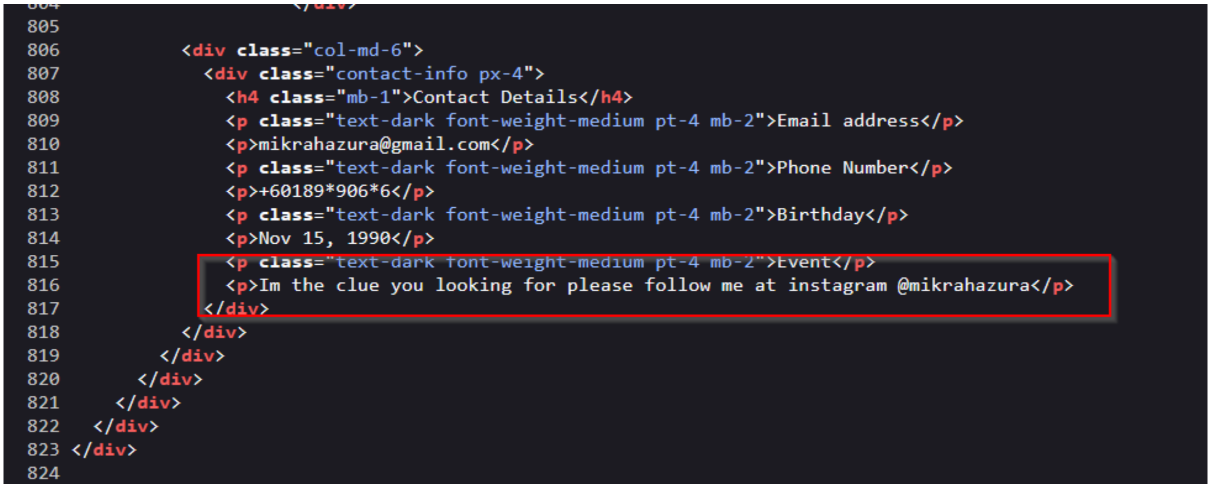
Master Cheff
UUNSC
haloering@email.com
(+785) 325 486 212

HTTPS://WEB.ARCHIVE.ORG/WEB/20220704083124/HTTPS://B2F.BATTLEOF1337.COM/

From title itself giving hint to use wayback.

Flag : BO1337{aHR0cHM6Ly9veW0uY2F0bWUuY2Y=}

1GRAM



```
                    </div>

          <div class="col-md-6">
            <div class="contact-info px-4">
              <h4 class="mb-1">Contact Details</h4>
              <p class="text-dark font-weight-medium pt-4 mb-2">Email address</p>
              <p>mikrahazura@gmail.com</p>
              <p class="text-dark font-weight-medium pt-4 mb-2">Phone Number</p>
              <p>+60189*906*6</p>
              <p class="text-dark font-weight-medium pt-4 mb-2">Birthday</p>
              <p>Nov 15, 1990</p>
              <p class="text-dark font-weight-medium pt-4 mb-2">Event</p>
              <p>Im the clue you looking for please follow me at instagram @mikrahazura</p>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</div>
```

By using view page source, we could notice there Instagram account inside there. By, following tag is reveal the flag.

HTTPS://WWW.INSTAGRAM.COM/MIKRAHAZURA/

HTTPS://WWW.INSTAGRAM.COM/SHARIZALIYAD/

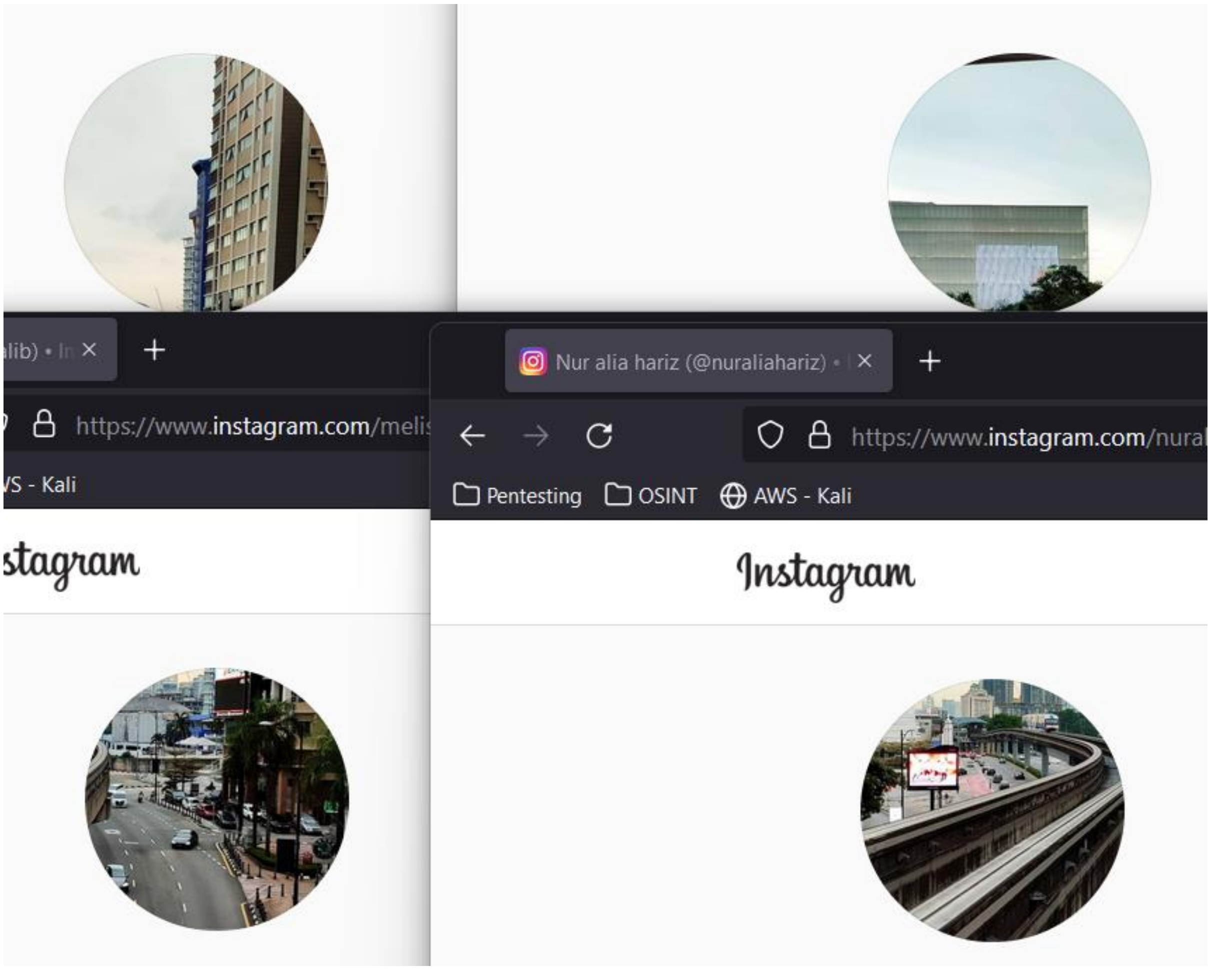
HTTPS://WWW.INSTAGRAM.COM/MELISAHALIB/

HTTPS://WWW.INSTAGRAM.COM/NURALIAHARIZ/

Flag : BO1337{S74LK_4P4_7U?}

SNAP

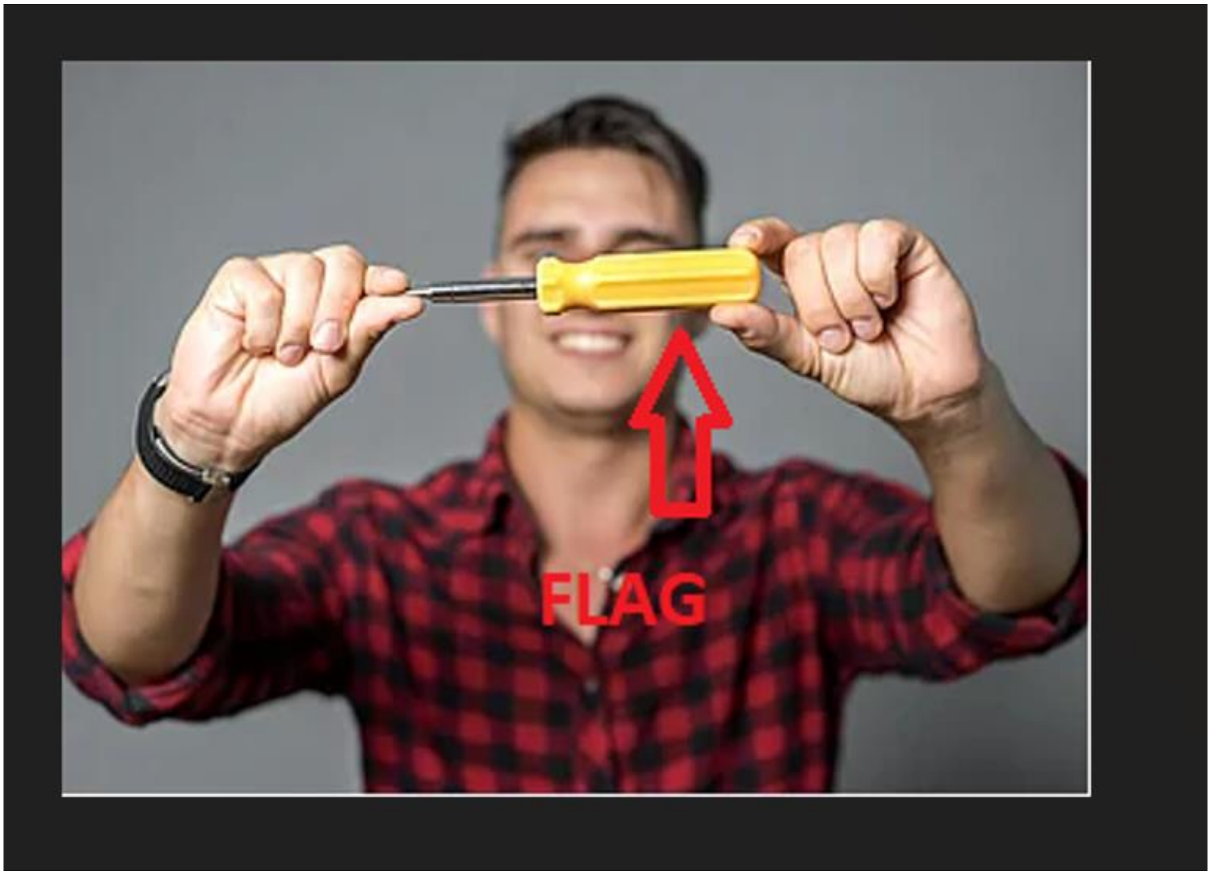
Based on Profile Picture, is really obviously near with BERJAYA TIME SQUARE


alib) • In ×
+
https://www.instagram.com/melis
/S - Kali
stagram
Nur alia hariz (@nuraliahariz) • I ×
+
https://www.instagram.com/nural
Pentesting
OSINT
AWS - Kali
Instagram

Therefore, the answer is BO1337{Imbi}

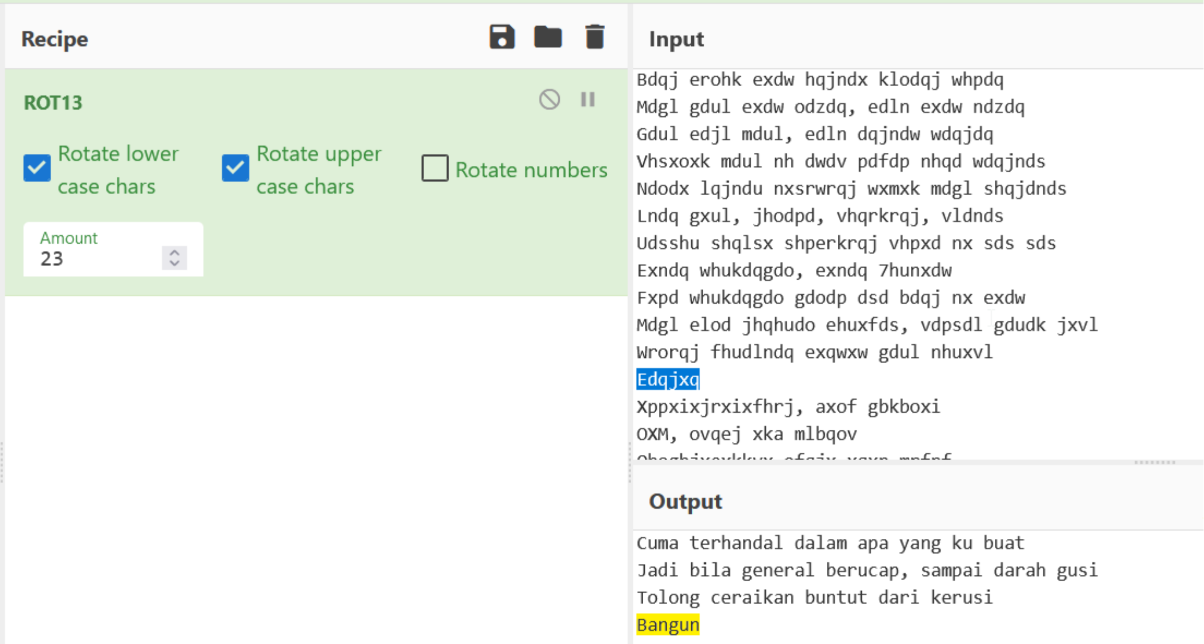
MISC

REDPOINT



Flag : BO1337{screwdriver}

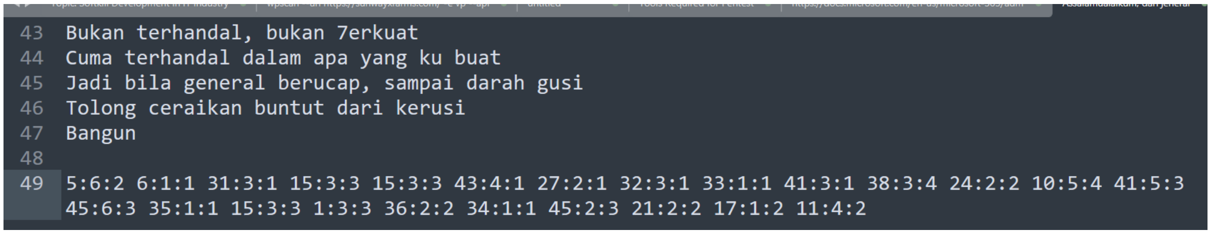
HEIHAWRU



```
Bdqj erohk exdw hqjndx klodqj whpdq
Mdgl gdul exdw odzdq, edln exdw ndzdq
Gdul edjl mdul, edln dqjndw wdqjdq
Vhsxoxk mdul nh dwdv pdfdp nhqd wdqjnds
Ndodx lqjndu nxsrwrqj wxmxk mdgl shqjdnds
Lndq gxul, jhodpd, vhqrkrqj, vldnds
Udsshu shqlsx shperkrqj vhpxd nx sds sds
Exndq whukdqgdo, exndq 7hunxdw
Fxpd whukdqgdo gdodp dsd bdqj nx exdw
Mdgl elod jhqhudo ehuxfds, vdpsdl gdudk jxvl
Wrorqj fhudlndq exqwxw gdul nhuxvl
Edqjxq
Xppxixjrxixfhrj, axof gbkboxi
OXM, ovqej xka mlbqov
```

```
Cuma terhandal dalam apa yang ku buat
Jadi bila general berucap, sampai darah gusi
Tolong ceraikan buntut dari kerusi
Bangun
```

Look like lyric from Assalamualaikum Malique.

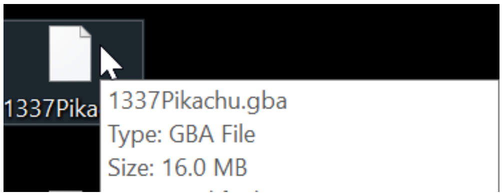


```
43  Bukan terhandal, bukan 7erkuat
44  Cuma terhandal dalam apa yang ku buat
45  Jadi bila general berucap, sampai darah gusi
46  Tolong ceraikan buntut dari kerusi
47  Bangun
48
49  5:6:2 6:1:1 31:3:1 15:3:3 15:3:3 43:4:1 27:2:1 32:3:1 33:1:1 41:3:1 38:3:4 24:2:2 10:5:4 41:5:3
    45:6:3 35:1:1 15:3:3 1:3:3 36:2:2 34:1:1 45:2:3 21:2:2 17:1:2 11:4:2
```

With given another guidance same like **And Ekceli** web challenge. Manually track a:b:c format. Mean first is the line, second is the sentence. and third is the alphabet.

BO1337{flAgisdarK3noKluai}

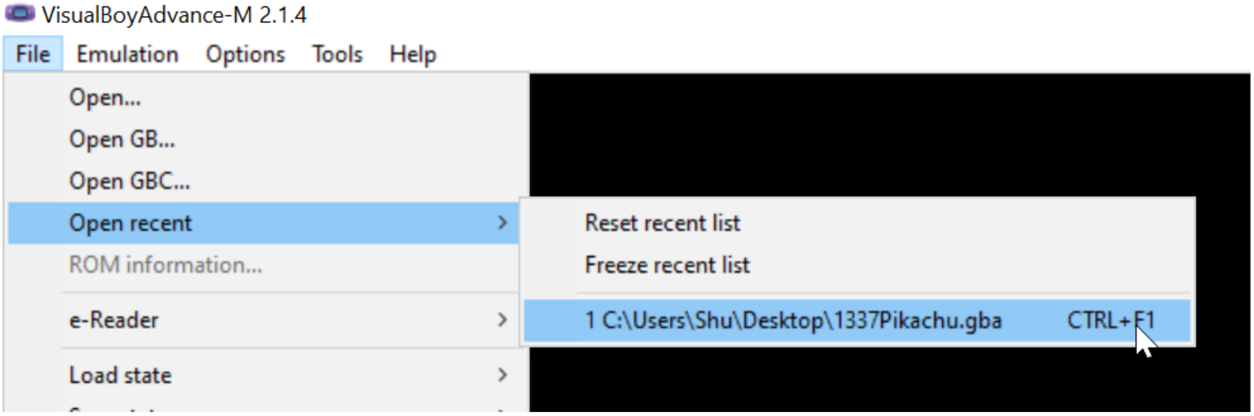
RAYQUAZA



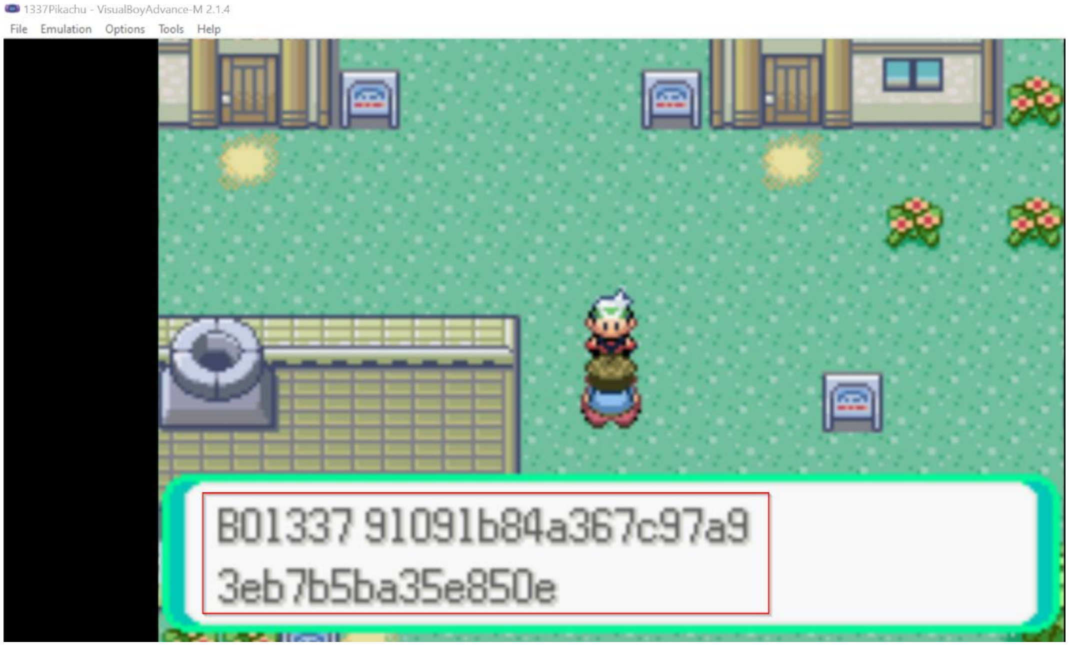
1337Pika

1337Pikachu.gba
Type: GBA File
Size: 16.0 MB

By simple "file" command is showed .gba file and rename it to 1337Pikachu.gba.



As we know, we need simulator in order to run the game.



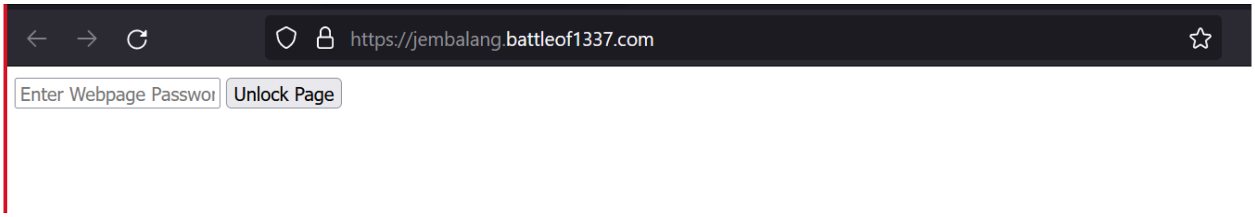
B01337 91091b84a367c97a9
3eb7b5ba35e850e

By simply talk to fat guy and it will show the flag.

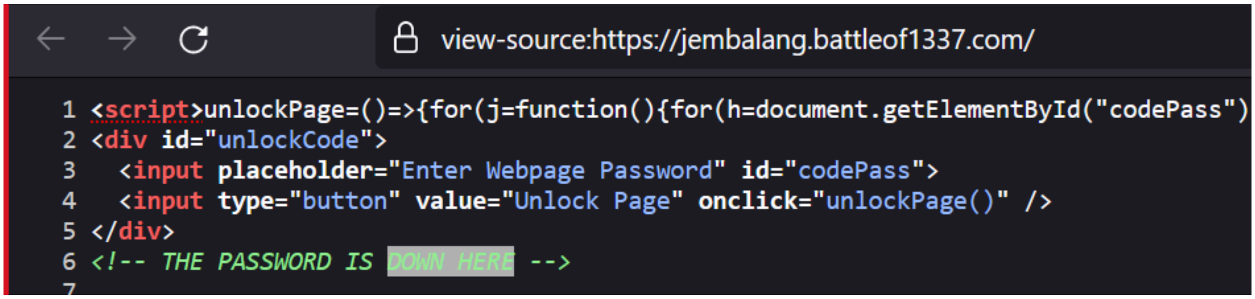
Flag = BO1337{91091b84a367c97a93eb7b5ba35e850e}

WEB

AND EKCELI

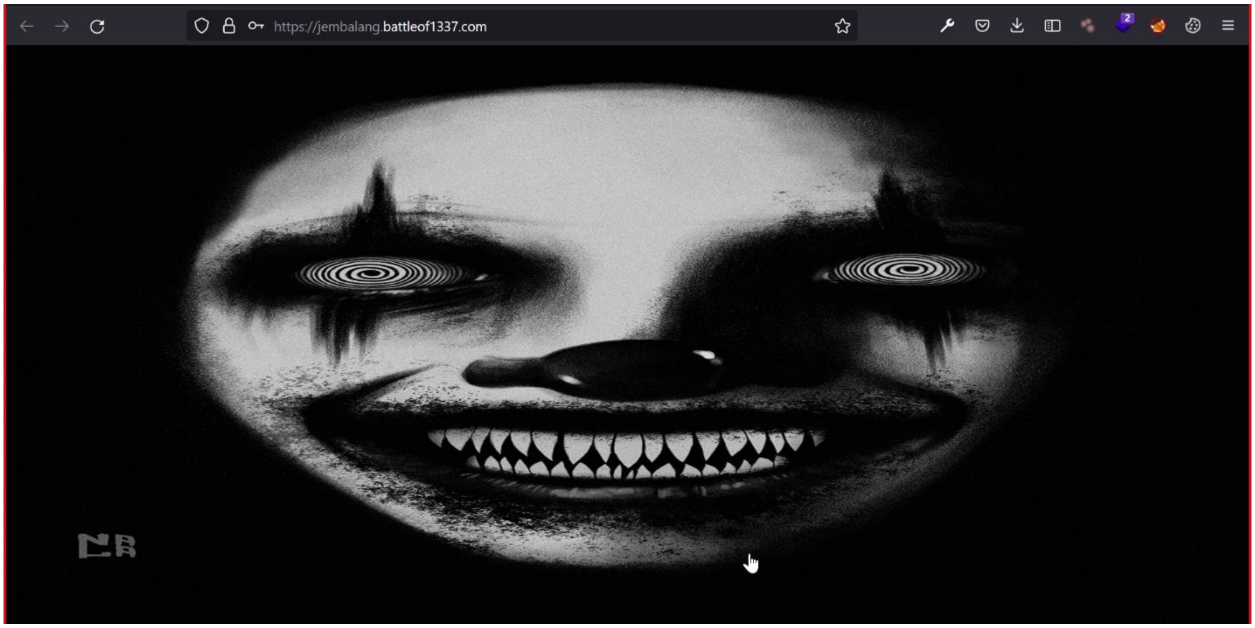


In order to procced next stage, we need a password. But wild guess by view page source.

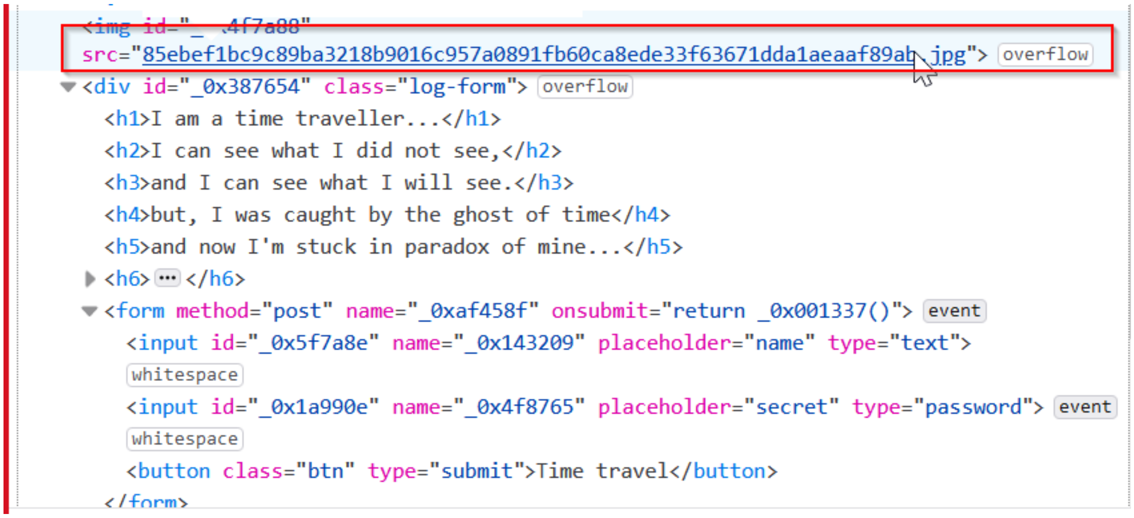


```
<script>unlockPage=()=>{for(j=function(){for(h=document.getElementById("codePass")
<div id="unlockCode">
  <input placeholder="Enter Webpage Password" id="codePass">
  <input type="button" value="Unlock Page" onclick="unlockPage()" />
</div>
<!-- THE PASSWORD IS DOWN HERE -->
```

Is showed the password is DOWN HERE.

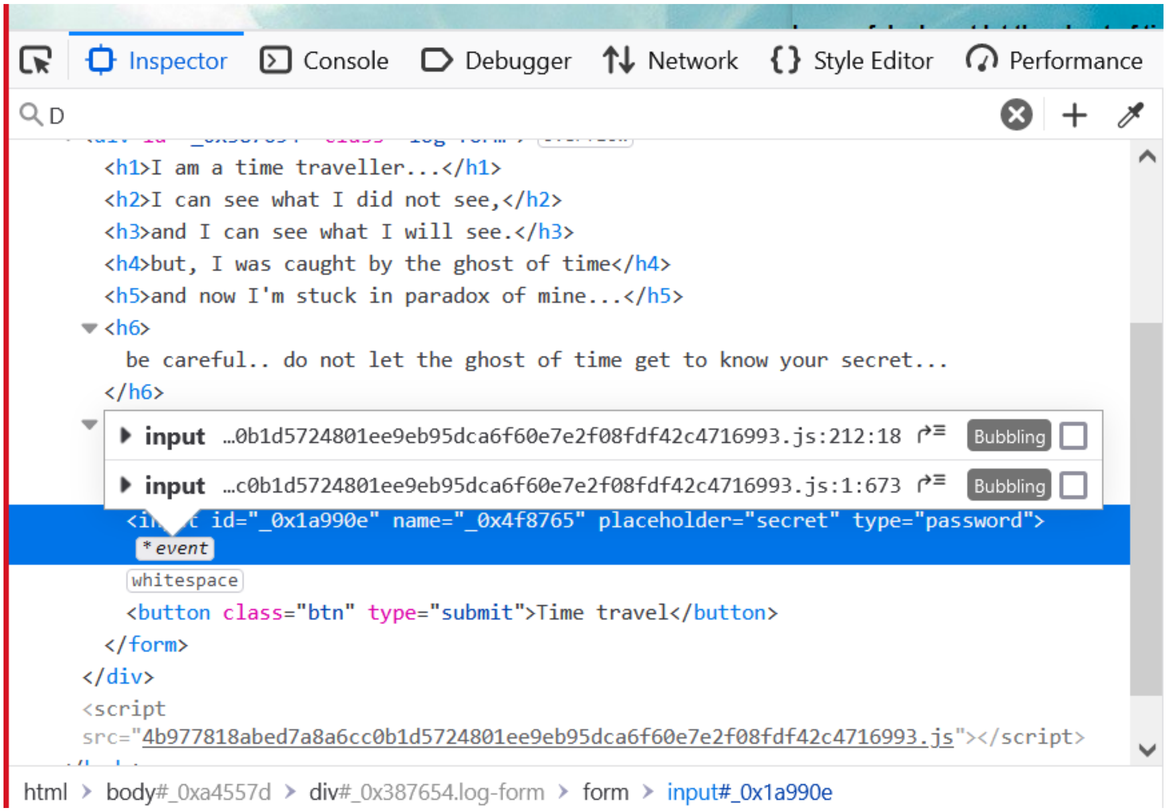


Based on several test and showed this image triggered automatically. In order, to procced next we need to disable the event.



```
<img id="_ 4f7a88"
src="85ebef1bc9c89ba3218b9016c957a0891fb60ca8ede33f63671dda1aeaaf89ab.jpg"> overflow
▼<div id="_0x387654" class="log-form"> overflow
   <h1>I am a time traveller...</h1>
   <h2>I can see what I did not see,</h2>
   <h3>and I can see what I will see.</h3>
   <h4>but, I was caught by the ghost of time</h4>
   <h5>and now I'm stuck in paradox of mine...</h5>
  ▶<h6>⋯</h6>
  ▼<form method="post" name="_0xaf458f" onsubmit="return _0x001337()"> event
     <input id="_0x5f7a8e" name="_0x143209" placeholder="name" type="text">
     whitespace
     <input id="_0x1a990e" name="_0x4f8765" placeholder="secret" type="password"> event
     whitespace
     <button class="btn" type="submit">Time travel</button>
   </form>
```

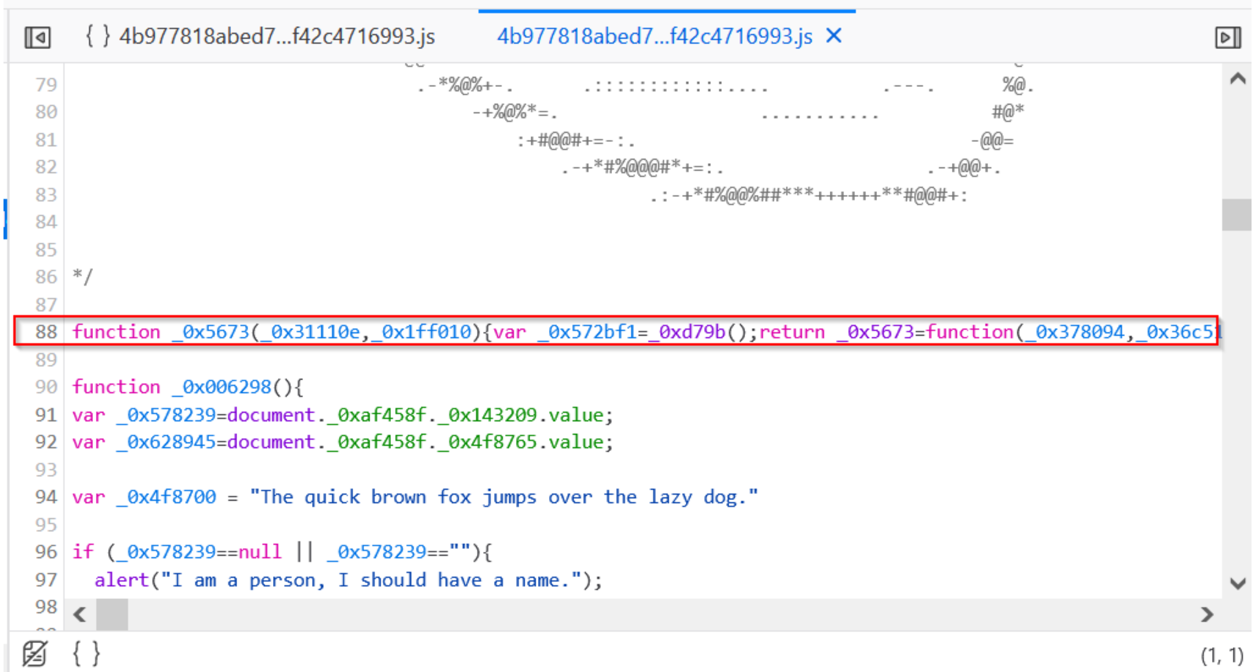
We know the event will occur in this.



```
   <h1>I am a time traveller...</h1>
   <h2>I can see what I did not see,</h2>
   <h3>and I can see what I will see.</h3>
   <h4>but, I was caught by the ghost of time</h4>
   <h5>and now I'm stuck in paradox of mine...</h5>
  ▼<h6>
     be careful.. do not let the ghost of time get to know your secret...
   </h6>
  ▼ ▶ input …0b1d5724801ee9eb95dca6f60e7e2f08fdf42c4716993.js:212:18  Bubbling ☐
    ▶ input …c0b1d5724801ee9eb95dca6f60e7e2f08fdf42c4716993.js:1:673  Bubbling ☐
     <input id="_0x1a990e" name="_0x4f8765" placeholder="secret" type="password">
     * event
     whitespace
     <button class="btn" type="submit">Time travel</button>
   </form>
 </div>
 <script
 src="4b977818abed7a8a6cc0b1d5724801ee9eb95dca6f60e7e2f08fdf42c4716993.js"></script>
```

html > body#_0xa4557d > div#_0x387654.log-form > form > input#_0x1a990e

In order to disable by untick it.

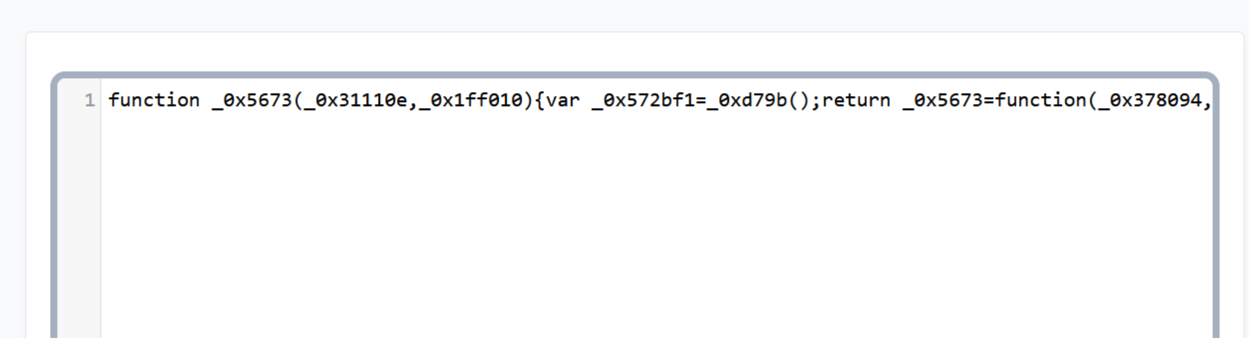


{ } 4b977818abed7...f42c4716993.js
4b977818abed7...f42c4716993.js ✕
{ }
(1, 1)

```
                               .-*%@%+-.     .:::::::::::::....        .---.     %@.
                                    -+%@%*=.                  ...........          #@*
                                        :+#@@#+=-:.                              -@@=
                                            .-+*#%@@@#*+=:.                  .-+@@+.
                                                    .:-+*#%@@%##***++++++**#@@#+:


*/

function _0x5673(_0x31110e,_0x1ff010){var _0x572bf1=_0xd79b();return _0x5673=function(_0x378094,_0x36c5

function _0x006298(){
var _0x578239=document._0xaf458f._0x143209.value;
var _0x628945=document._0xaf458f._0x4f8765.value;

var _0x4f8700 = "The quick brown fox jumps over the lazy dog."

if (_0x578239==null || _0x578239==""){
  alert("I am a person, I should have a name.");
```

https://jembalang.battleof1337.com/4b977818abed7a8a6cc0b1d5724801ee9eb95dca6f60e7e2f08fdf42c4716993.js

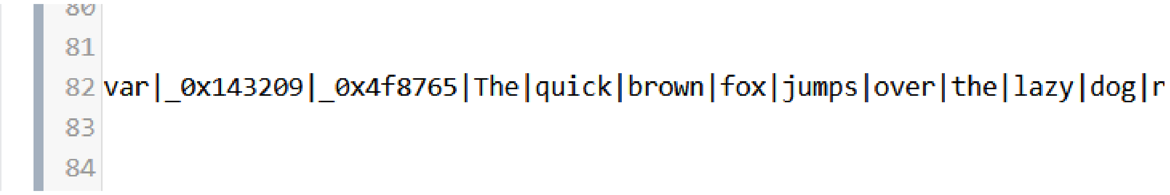
We do notice that there long string javascript name. By analysis, we do notice that is obfuscate.



```
function _0x5673(_0x31110e,_0x1ff010){var _0x572bf1=_0xd79b();return _0x5673=function(_0x378094,
```

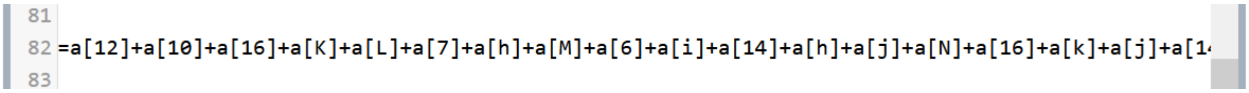
In order to deobfuscate the javascript, we rely on online tool to open and read.

https://www.seosniffer.com/javascript-deobfuscator



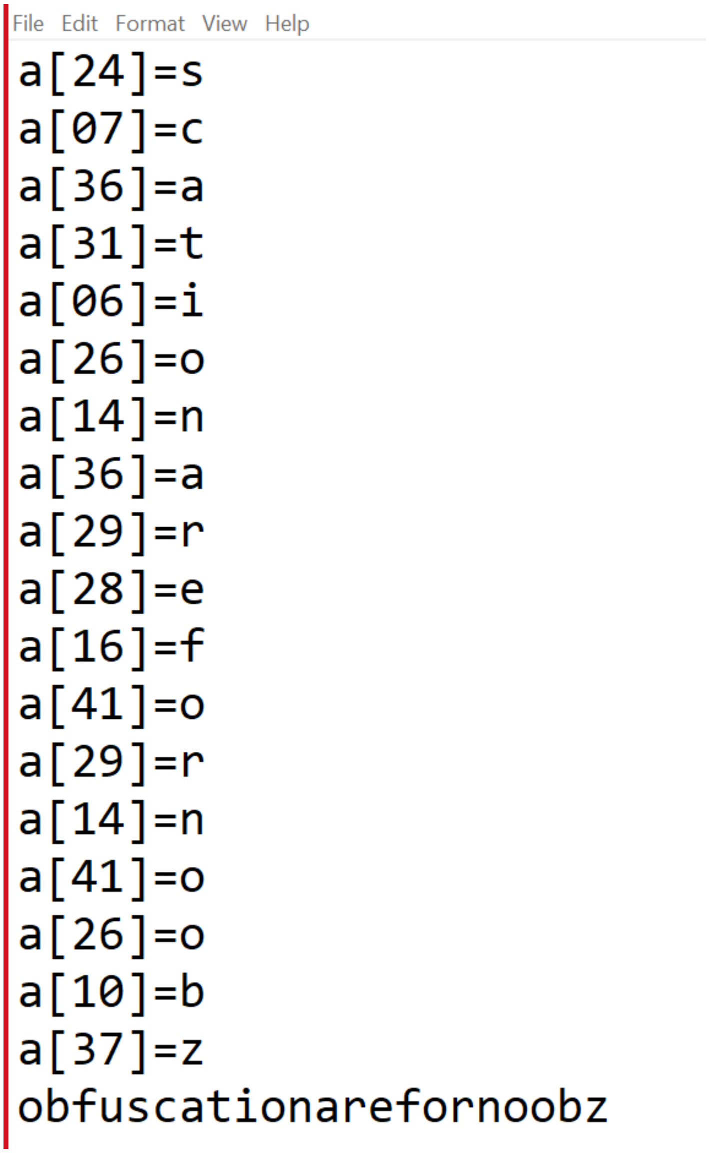
```
var|_0x143209|_0x4f8765|The|quick|brown|fox|jumps|over|the|lazy|dog|r
```

By analysis, we know that the key word is `The quick brown fox jumps over the lazy dog`



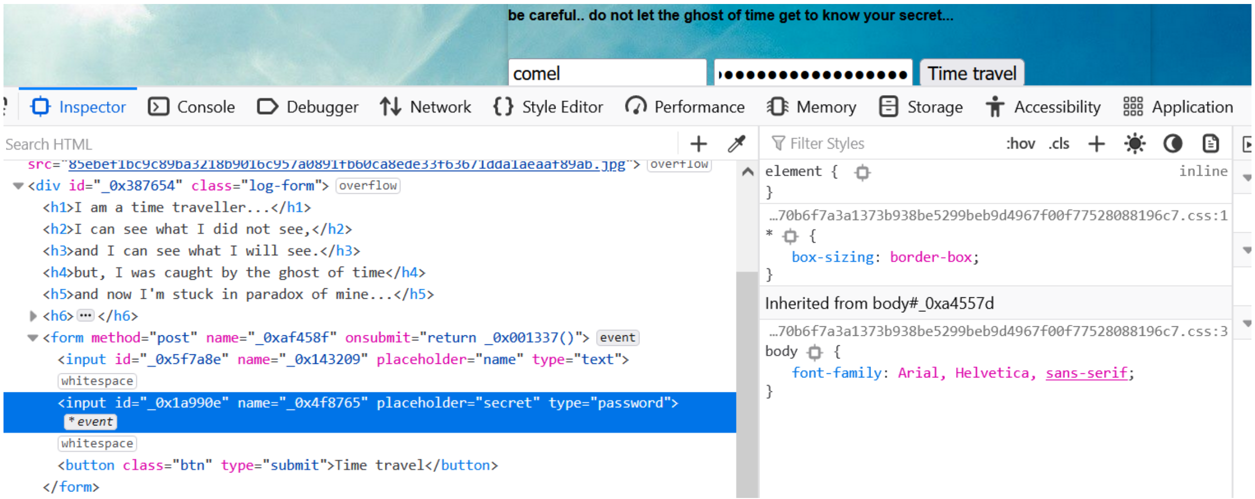
```
=a[12]+a[10]+a[16]+a[K]+a[L]+a[7]+a[h]+a[M]+a[6]+a[i]+a[14]+a[h]+a[j]+a[N]+a[16]+a[k]+a[j]+a[1
```

As common programmer, the count start from 0. For e.g. a[12] is **o**.



```
a[24]=s
a[07]=c
a[36]=a
a[31]=t
a[06]=i
a[26]=o
a[14]=n
a[36]=a
a[29]=r
a[28]=e
a[16]=f
a[41]=o
a[29]=r
a[14]=n
a[41]=o
a[26]=o
a[10]=b
a[37]=z
obfuscationarefornoobz
```

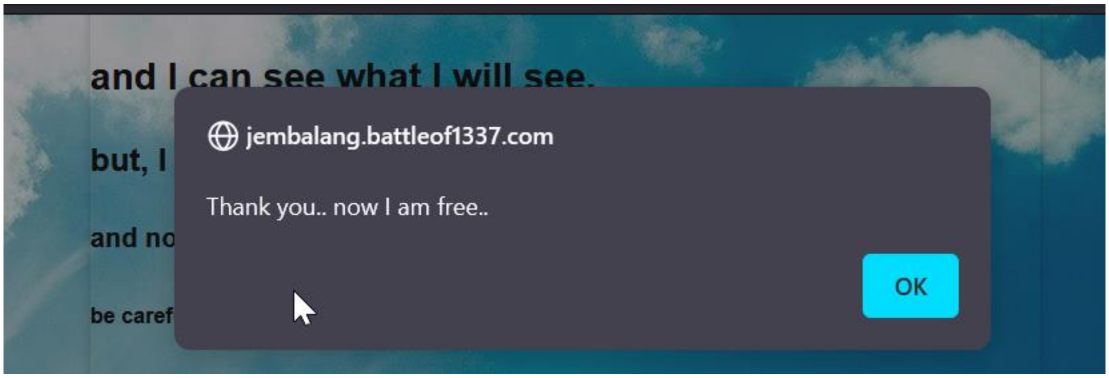
By manually decode is showed obfuscationarefornoobz.



```
src="85ebef1bc9c89ba3218b9016c957a0891fb60ca8ede33f63671dda1aeaaf89ab.jpg"> overflow
<div id="_0x387654" class="log-form"> overflow
  <h1>I am a time traveller...</h1>
  <h2>I can see what I did not see,</h2>
  <h3>and I can see what I will see.</h3>
  <h4>but, I was caught by the ghost of time</h4>
  <h5>and now I'm stuck in paradox of mine...</h5>
  <h6> ··· </h6>
  <form method="post" name="_0xaf458f" onsubmit="return _0x001337()"> event
    <input id="_0x5f7a8e" name="_0x143209" placeholder="name" type="text">
    whitespace
    <input id="_0x1a990e" name="_0x4f8765" placeholder="secret" type="password">
     * event
    whitespace
    <button class="btn" type="submit">Time travel</button>
  </form>
```

```
element {                                                  inline
}
…70b6f7a3a1373b938be5299beb9d4967f00f77528088196c7.css:1
* {
   box-sizing: border-box;
}
Inherited from body#_0xa4557d
…70b6f7a3a1373b938be5299beb9d4967f00f77528088196c7.css:3
body {
   font-family: Arial, Helvetica, sans-serif;
}
```

By putting random username and password from that we manually decode. We know we successfully decode.

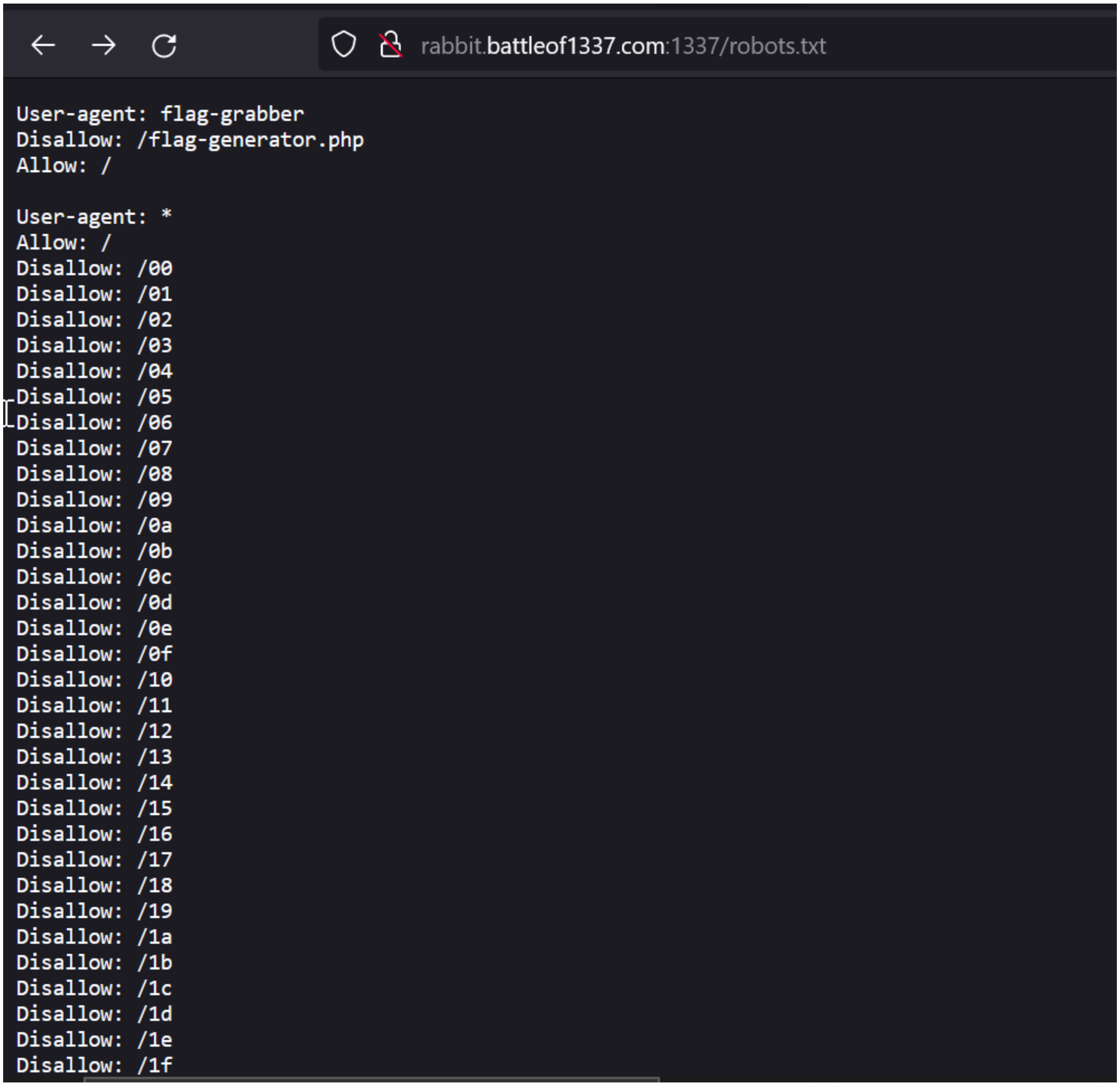


jembalang.battleof1337.com

Thank you.. now I am free..

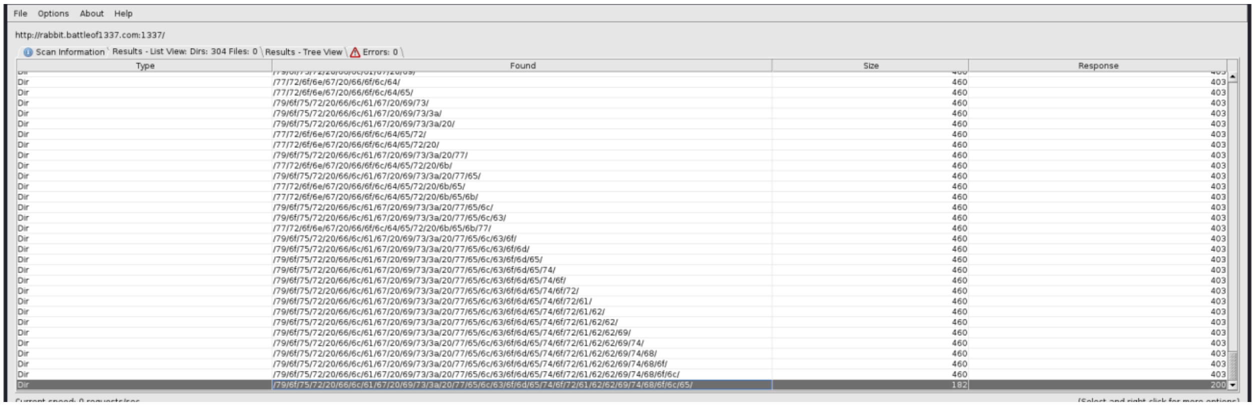
Flag = BO1337{obfuscationarefornoobz}

ALICE IN WONDERLAND



```
User-agent: flag-grabber
Disallow: /flag-generator.php
Allow: /

User-agent: *
Allow: /
Disallow: /00
Disallow: /01
Disallow: /02
Disallow: /03
Disallow: /04
Disallow: /05
Disallow: /06
Disallow: /07
Disallow: /08
Disallow: /09
Disallow: /0a
Disallow: /0b
Disallow: /0c
Disallow: /0d
Disallow: /0e
Disallow: /0f
Disallow: /10
Disallow: /11
Disallow: /12
Disallow: /13
Disallow: /14
Disallow: /15
Disallow: /16
Disallow: /17
Disallow: /18
Disallow: /19
Disallow: /1a
Disallow: /1b
Disallow: /1c
Disallow: /1d
Disallow: /1e
Disallow: /1f
```

By opening robots.txt is showed lot of path folder.



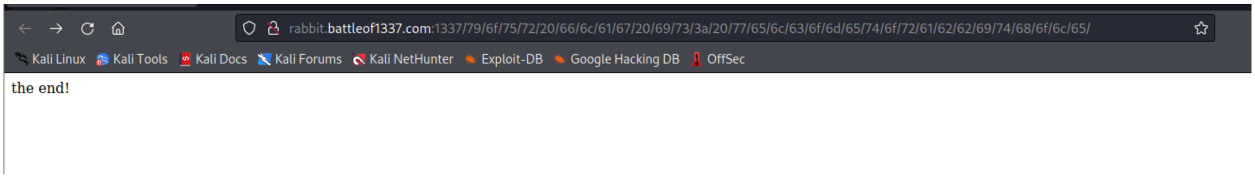
http://rabbit.battleof1337.com:1337/

Type	Found	Size	Response
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/20/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/20/6b/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/20/6b/65/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/20/6b/65/6b/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/	460	403
Dir	/77/72/6f/6e/67/20/66/6f/6c/64/65/72/20/6b/65/6b/77/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/	460	403
Dir	/79/6f/75/72/20/66/6c/61/67/20/69/73/3a/20/77/65/6c/63/6f/6d/65/74/6f/72/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	460	403
Dir	/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/	182	200

Current speed: 0 requests/sec

(Select and right click for more options)

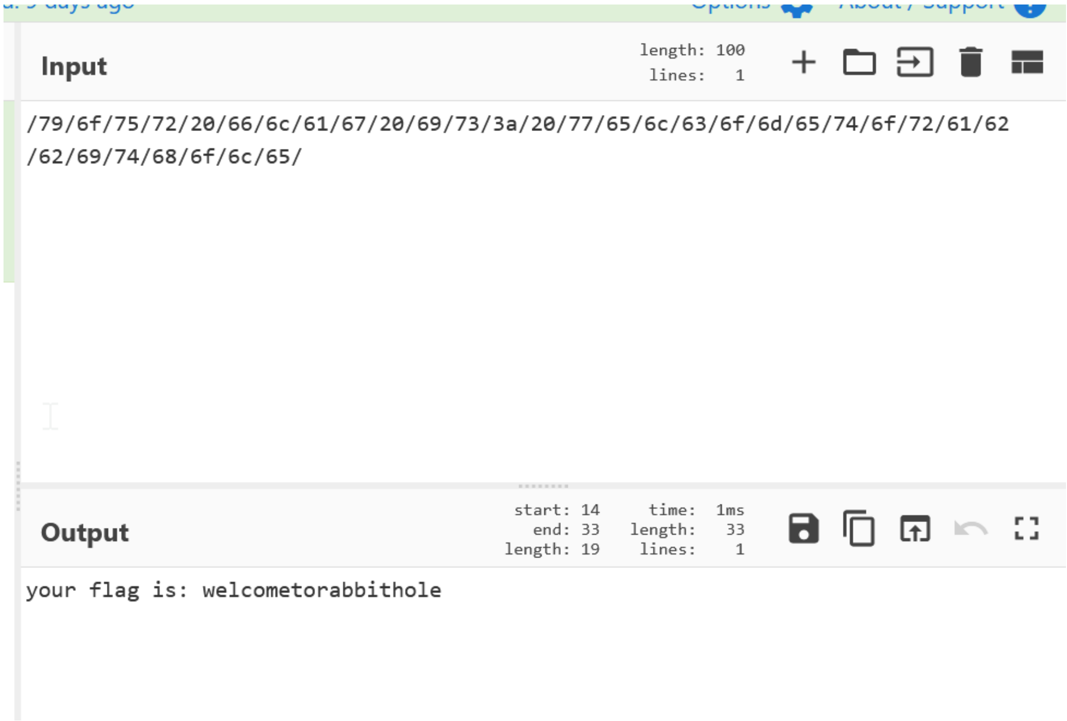
In order to do automated search, we using tool from OWASP dirbuster. Enable recursion on.



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/

the end!

Is showed the end.



length: 100
lines: 1

```
/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/
```

start: 14
end: 33
length: 19
time: 1ms
length: 33
lines: 1

```
your flag is: welcometorabbithole
```

By simply decode from hex to string is showed the flag.

Flag = BO1337{welcometorabbithole}