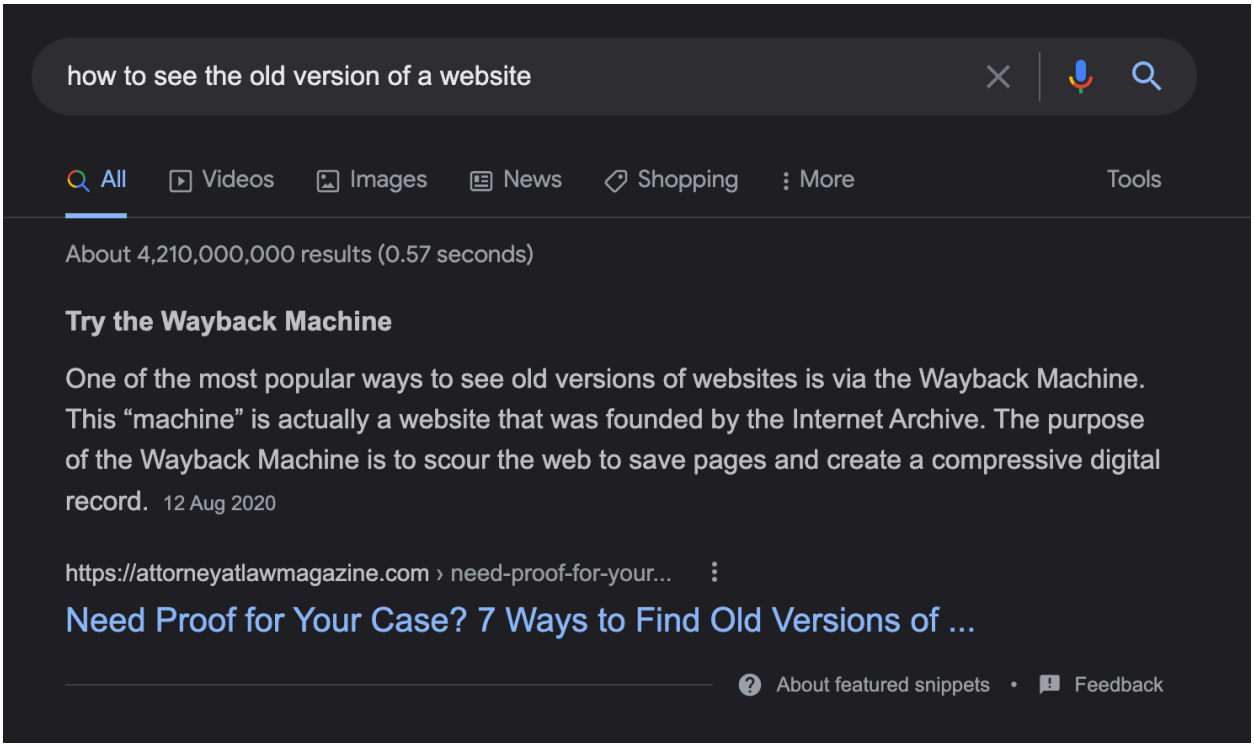
BO1337{xAlep_WriteUp}

root@localhost:~$ echo "b4771 0f 1337"

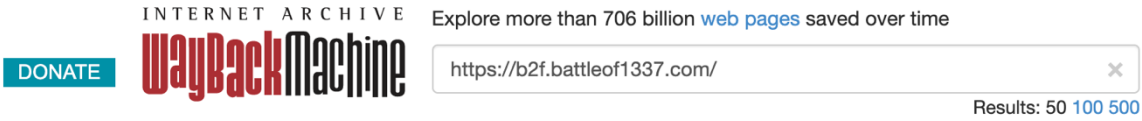
BATTLE_OF_1337

CTF 2022

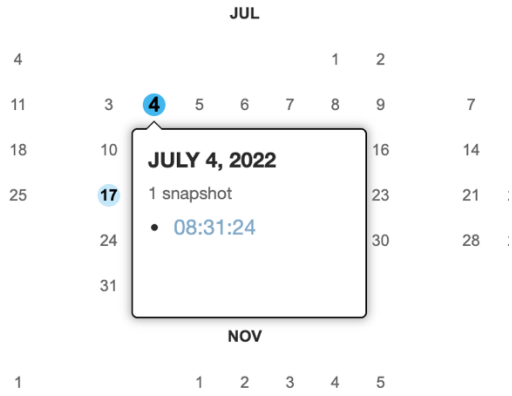
Isn't cool if we can go back in time? But how?



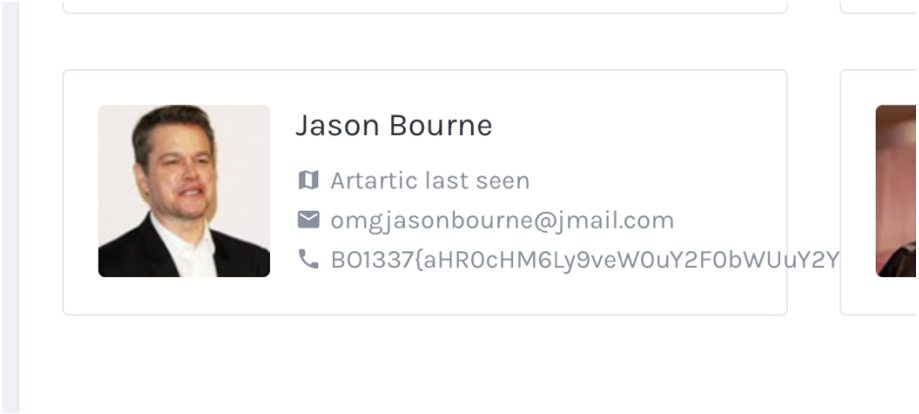
Google is the most powerful tools in osint. First we have to search on how to get back to the old version of the website. Then google suggested **Wayback Machine.**



Simply enter the link URL of the challenge website.

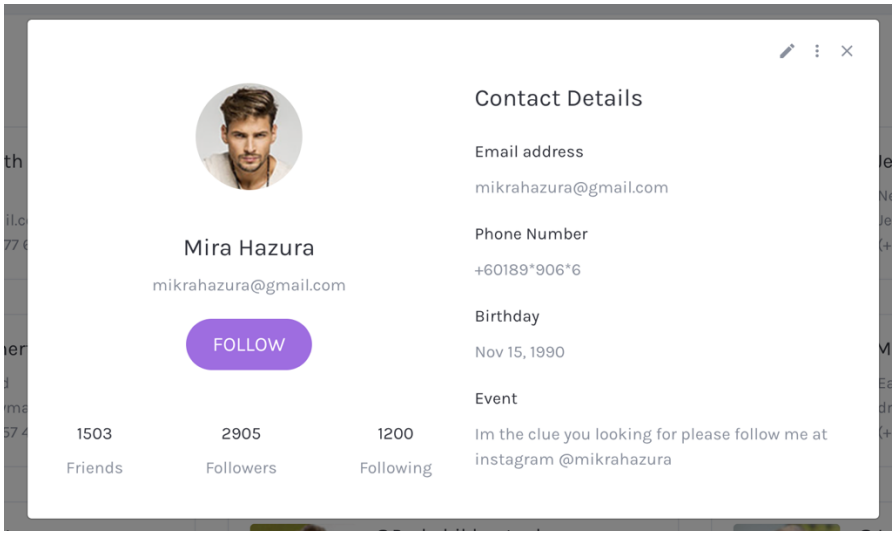


We would like something like this, meaning that someone used to change something in the website. So clicked on the timestamp.

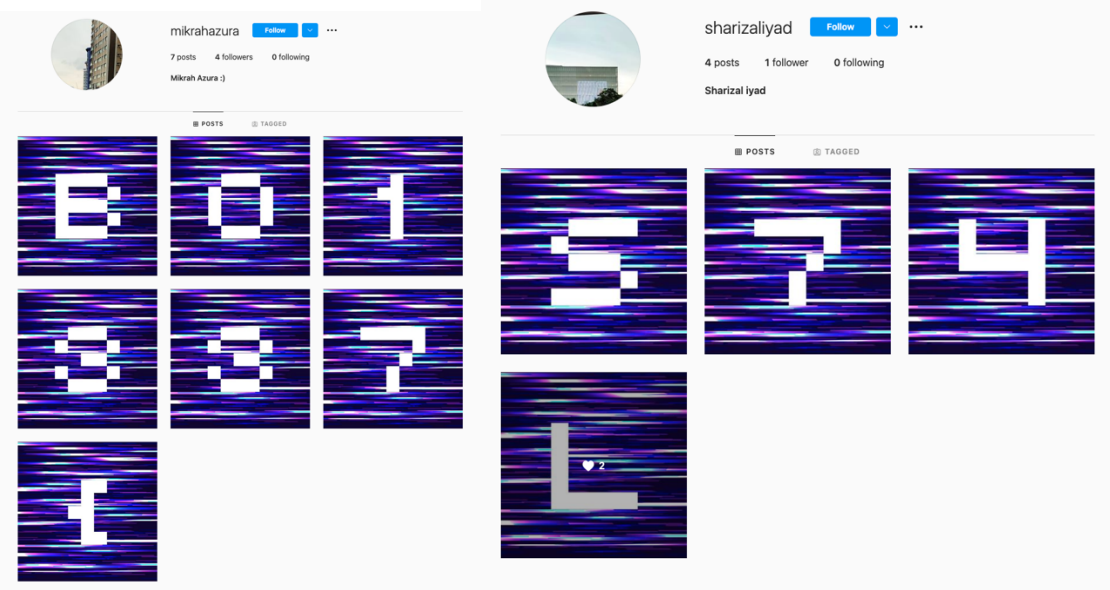


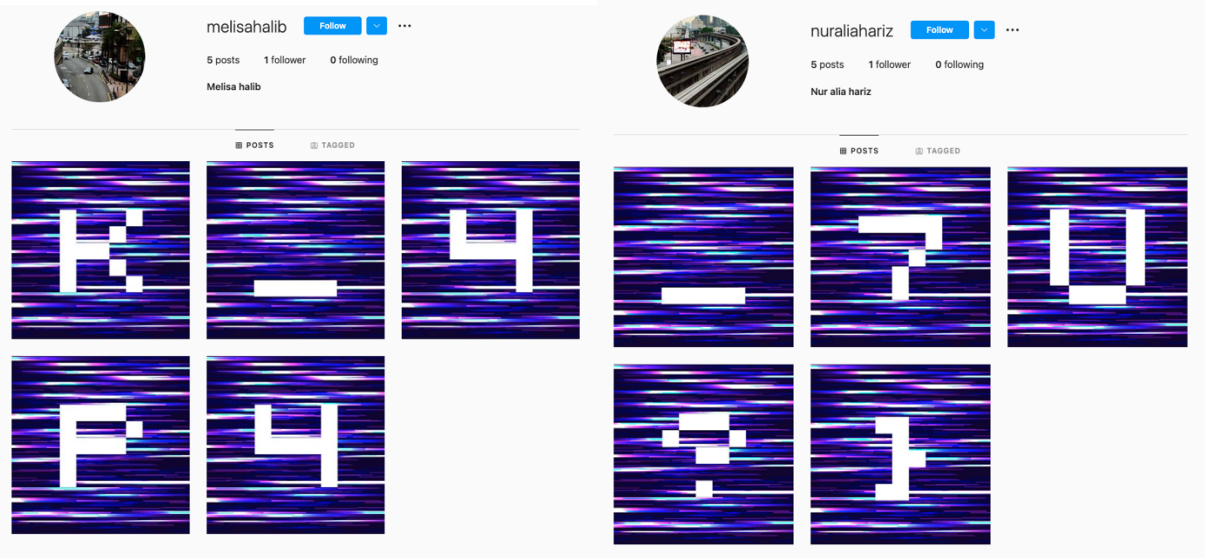
Flag : BO1337{aHR0cHM6Ly9veW0uY2F0bWUuY2Y=}

Huh I might miss something? Do it for the gram? WHAT????!!

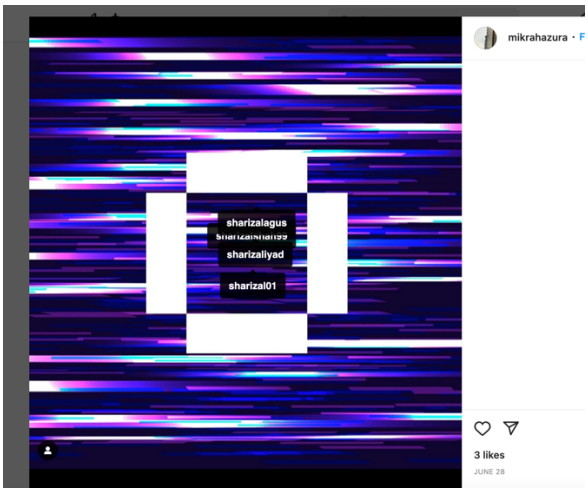


Explore the website given, once you click on any of the card. You will get the next clue in Event. But, who is @mikrahazura? Let's search it in Instagram.





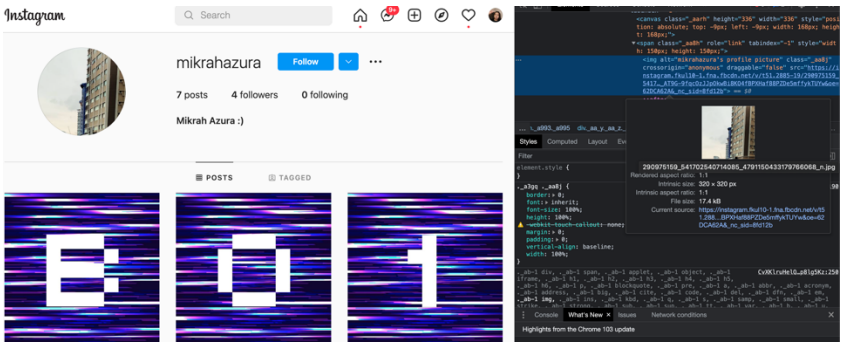
Ehh???!! How come I got 4 instagram account? Rileks on each of the picture, you would notice they tagged. So see all the picture, and you will get 4 instagram account in total.



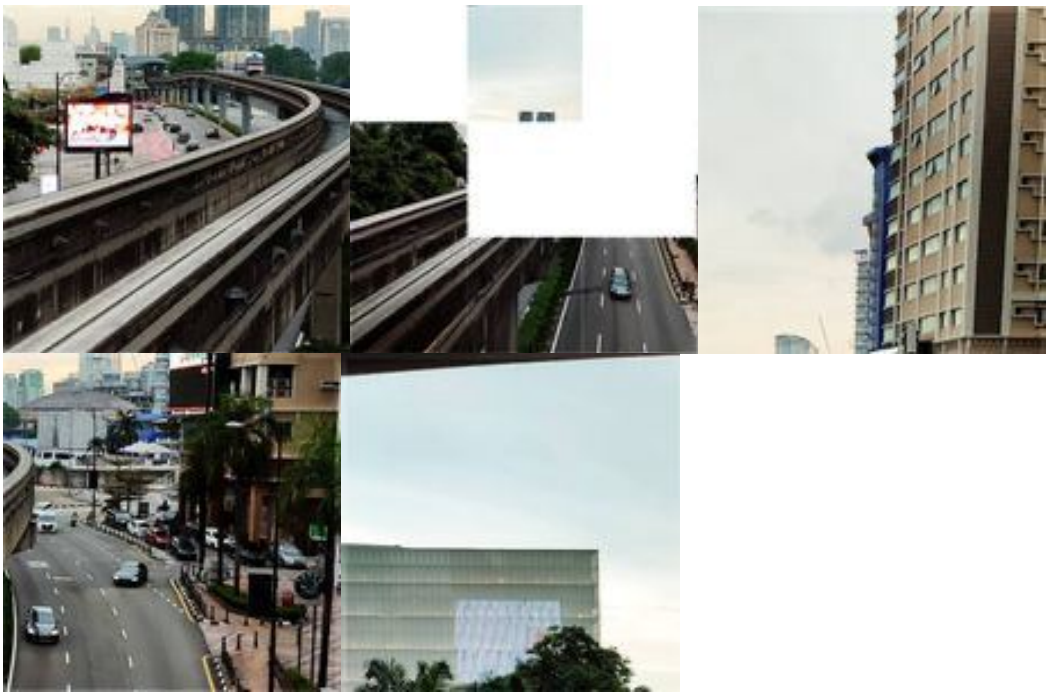
Where's the flag? Simply combine all the picture to get the flag.

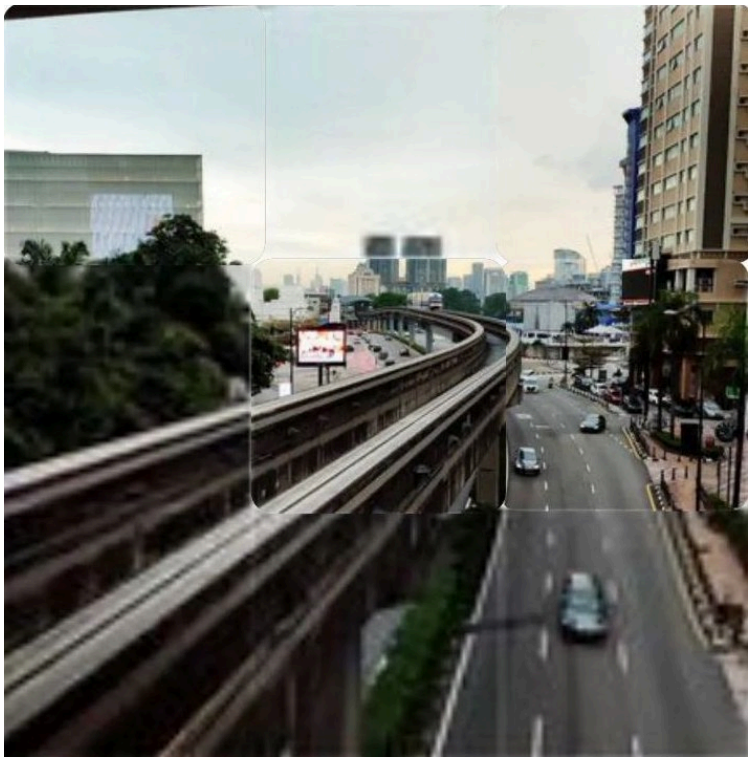
Flag: BO1337{S74LK_4P4_7U?}

Keep stalking? Why???!!!
If you stalk deep enough, you will notice that the Instagram account profile picture, all of it is like a puzzle. Lets see.



You can save the image in Instagram by inspect the element.



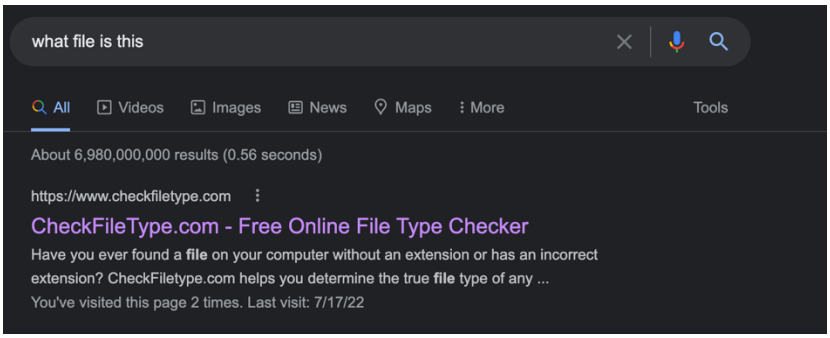


Im using Instagram to mix and match the picture. So as we can see, it looks like somewhere in Kuala Lumpur right? Is it LRT? Is it Jalan? GUESS IT!

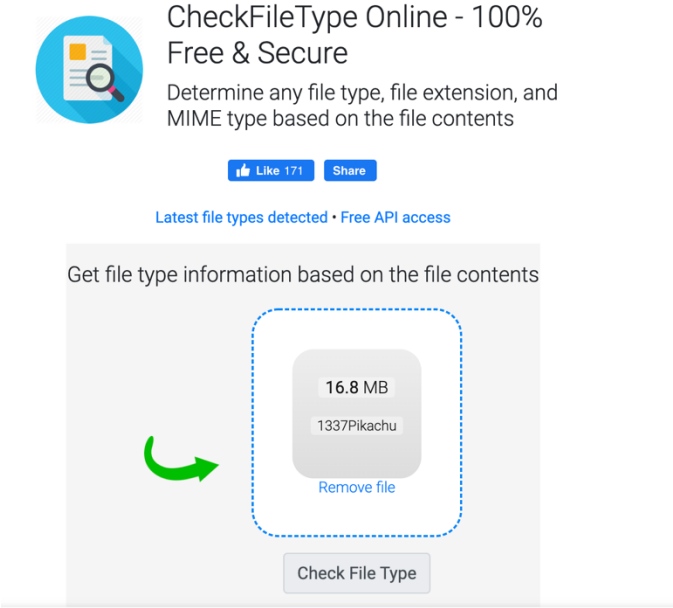
Flag: BO1337{Imbi}

In this challenge, we will be given a file. So first of all, we have to check what type of file is this.

Filename: 1337Pikachu



Simply google “What file is this” in google and take the one at the top.



Drag the file in the given field.

File Type: Game Boy Advance ROM image: "POKEMON EMER" (BPEE01, Rev.00)

How did we do?

Ahaaa. We got the file type. It would be Game Boy Advance ROM image to simply if you guys are an OG pokemon player, you will know its gba.
Now change the file extension to .gba and start playing in any emulator. In my case, im using OpenEmu since not all emulator can be played in MacOS

You have to play the game for around 2,3 minutes. Talk to the mother and everything until you found this FAT BOY!

Flag: BO1337{91091b84a367c97a93eb7b5ba35e850e}

RedPoint

443

Simple Question, Just find the flag

Yeah simple question. Just find the flag in the image below

Flag: BO1337{screwdriver}

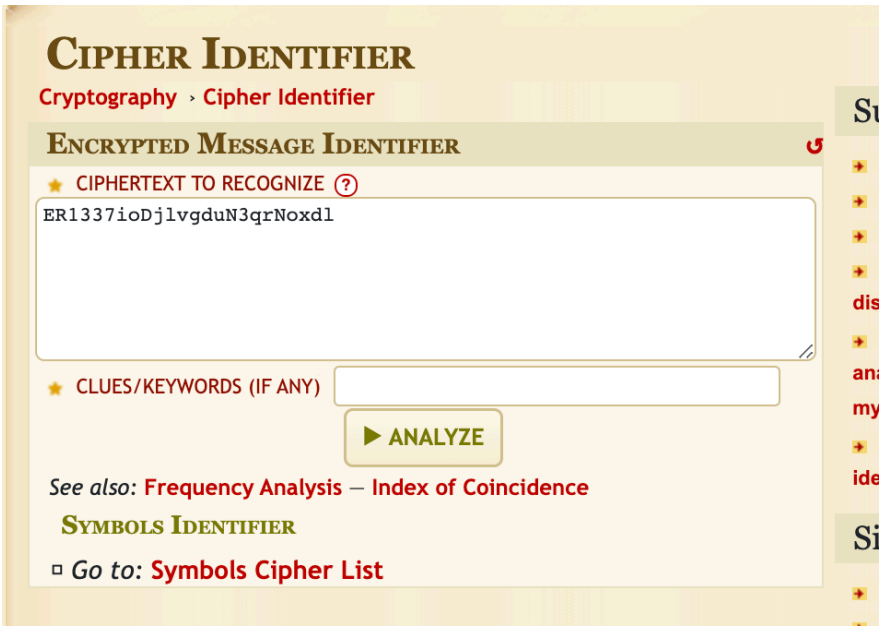
First download the file given.

We will got this random sajak from ali? Maybe? And also we got this number number. First I thought it is old keypad decryption. But NO!

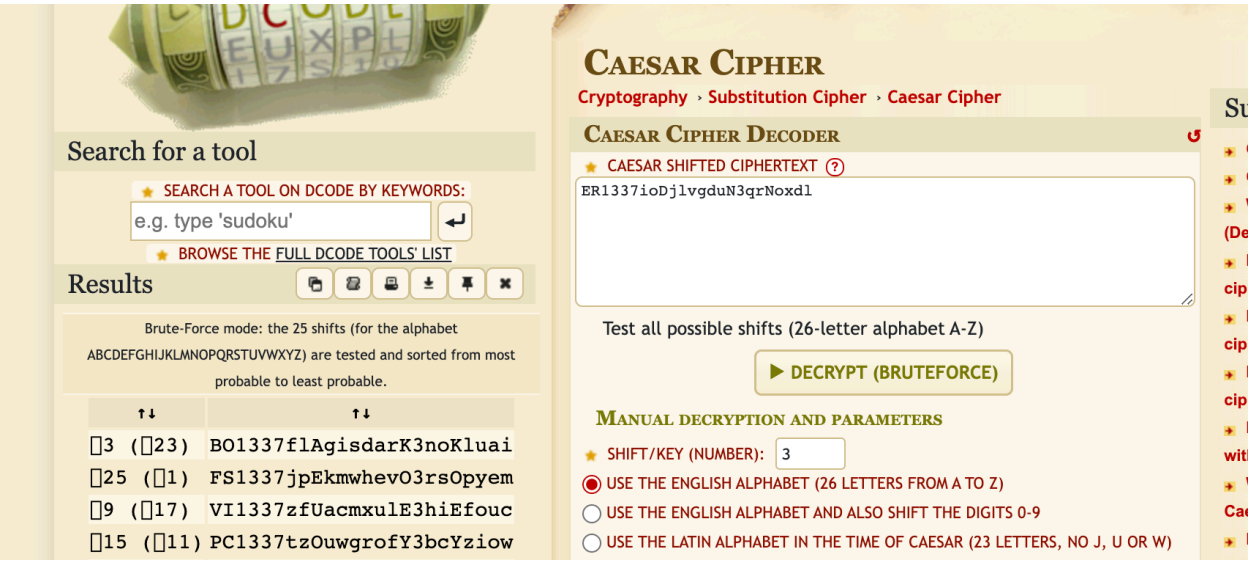
If we see the first in the random number, it is 5:6:2 . 5 Stand for line number 5, 6 stand for 6th word in that line, 2 stand for the second alphabet in the word.

After that, we will get **ER1337ioDjlvgduN3qrNoxdl**

Simply search for any decryptor or cipher identifier in google. Then analyze it !



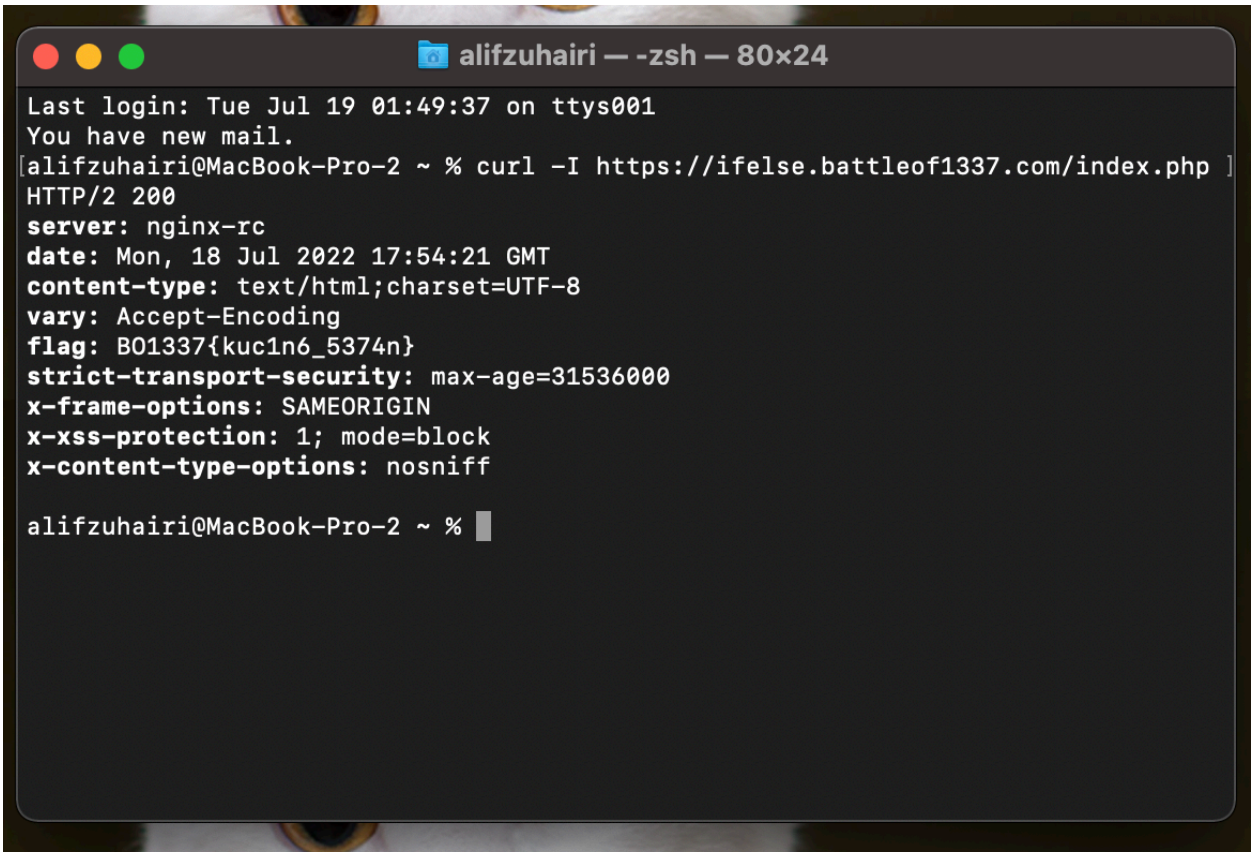
After that, I manage to identify the decoder for this which is Caesar Cipher.



Flag: BO1337{flAgisdarK3noKlua}

For this one, just open the website and terminal (or cmd for windows)

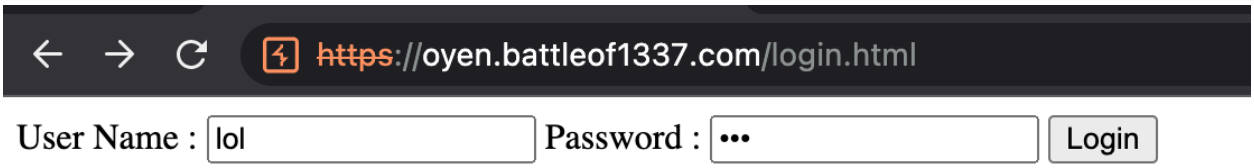
Use command : Curl -I https://ifelse.battleof1337.com/index.php



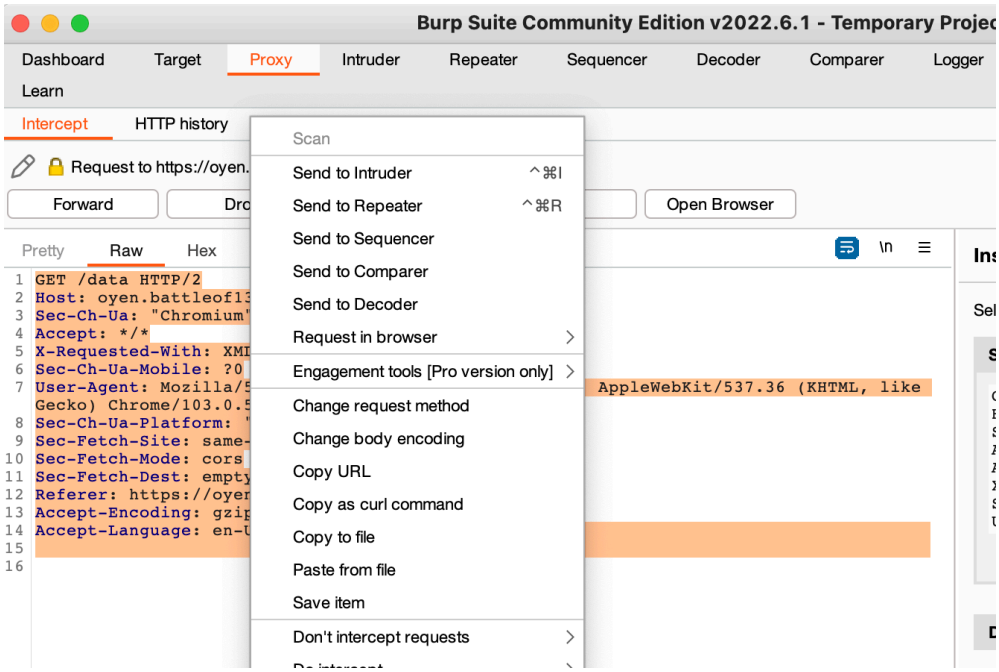
Flag: BO1337{kuc1n6_5374n}

Let's HACK some storage shall we?

First of all, I'm using Burp suite since it would make me looks like a hacker.



Put anything on the username and password. And turn on the intercept.



Copy the code and send it to Repeater.

Request Response

Pretty Raw Hex Render

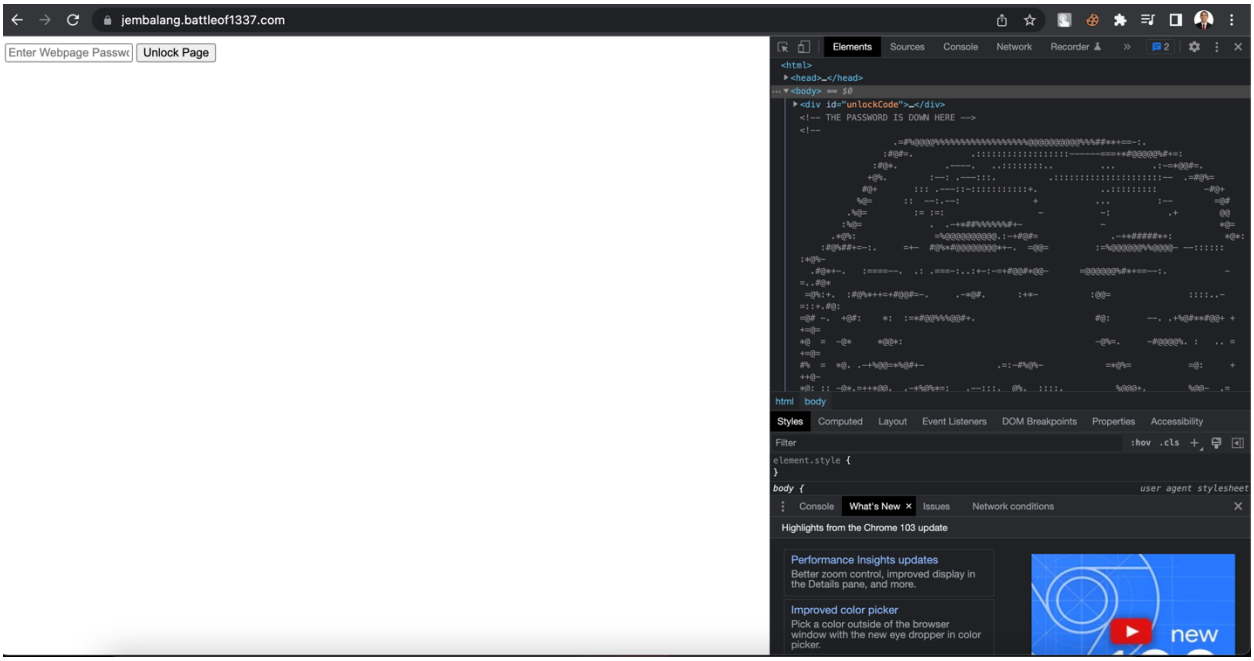
```
1  HTTP/2 200 OK
2  Server: nginx-rc
3  Date: Mon, 18 Jul 2022 17:57:06 GMT
4  Content-Length: 180
5  Vary: Accept-Encoding
6  Last-Modified: Sun, 03 Jul 2022 13:19:00 GMT
7  Etag: "b4-5e2e67666ee13"
8  Accept-Ranges: bytes
9  Strict-Transport-Security: max-age=31536000
10 X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
13
14 {
     "user":{
       "normal":{
         "userID":"1",
         "username":"BattleOf1337",
         "password":"BattleOf1337"
       },
       "super":{
         "userID":"356a192b7913b04c54574d18c28d46e6395428ab",
         "username":"root",
         "password":""
       }
     }
   }
```

Tadaaa ~~ We got the username and password. Now login. The website is empty. So we have to view source of the website. We will got this new file:

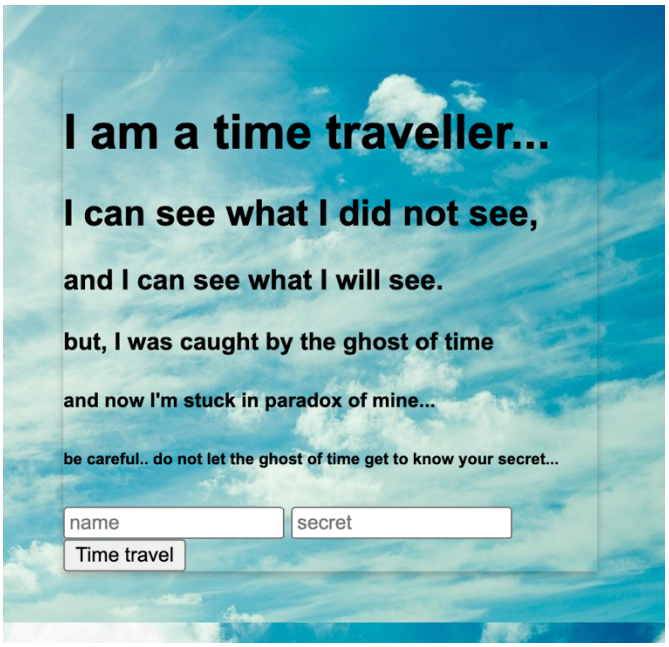

```
let database="data";$.get(database,function(a)
{jsons=JSON.parse(a),getFlag=jsons.user.super,window.localStorage.userID==getFlag.userID&&alert("BO1337{a2c13e70ff50376e259ddb5bd5e54a69b16e569f}"),0==window.localStorage.length&&
(window.location="login.html")});
```

Flag: BO1337{a2c13e70ff50376e259ddb5bd5e54a69b16e569f}

WARNING : DON'T PLAY THIS CHALLENGE IF YOU ARE NOT READY FOR BHAAAAA
DO IT ON YOUR OWN RISK !



Once we open the website, we have to unlock the page. But we don't have the password right? Yeah the dev already left the Password. THE PASSWORD IS **DOWN HERE**



DON'T LET THE GHOST KNOW YOUR SECRET! Meaning that don't ever put the password in the textfield. So I tried to inspect element. And I found this javascript function.

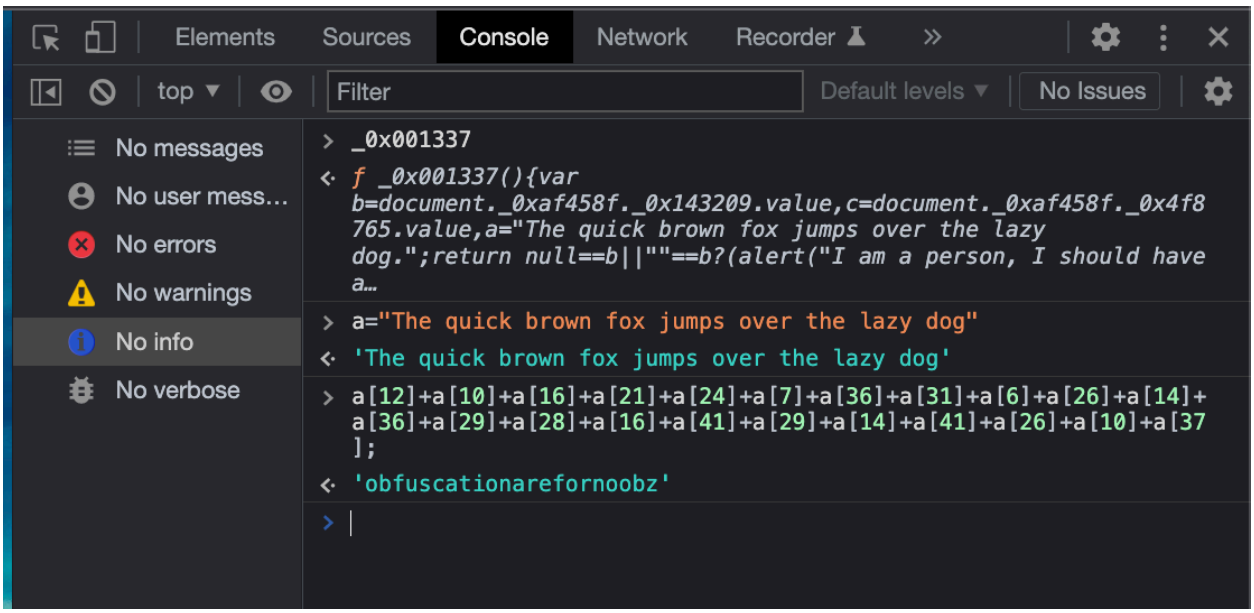
```
    <h4>but, I was caught by the ghost of time</h4>
    <h5>and now I'm stuck in paradox of mine...</h5>
    <h6>be careful.. do not let the ghost of time get to know your secret...</h6>
  ▶<form method="post" name="_0xaf458f" onsubmit="return _0x001337()">…</form>
  </div>
  <script src="4b97781….js"></script>
 </body>
</html>
```

Copy the javascript function in console.

July 19, 2022 at 2:04 AM

```
const _0x872f99=document.getElementById("_0x1a990e");function _0x001337(){var
b=document._0xaf458f._0x143209.value,c=document._0xaf458f._0x4f8765.value,a="The quick brown fox
jumps over the lazy dog.";return null==b||""==b?(alert("I am a person, I should have a name."),!
1):c==a[12]+a[10]+a[16]+a[21]+a[24]+a[7]+a[36]+a[31]+a[6]+a[26]+a[14]+a[36]+a[29]+a[28]+a[16]+a[
41]+a[29]+a[14]+a[41]+a[26]+a[10]+a[37]?(alert("Thank you.. now I am
free.."),document.getElementById("_0x387654").style.visibility="hidden",document.getElementById("_0xa
4557d").style.backgroundImage="url(74eee63dc70adf02e115e178e360f8c875471ded66f9e64d91ad4121
2d50433b.jpeg)",!1):void 0}function _0x069420()
{document.getElementById("_0x387654").style.visibility="hidden",document.getElementById("_0x4f7a88"
).style.visibility="visible"}_0x872f99.addEventListener("input",_0x069420);
```

We will get this type of script.



Then just assign the sentences into a. Then since it is in array, we can combine it together. Just copy the array at the console and we will get the flag.

Flag: BO1337{obfuscationarefornoobz}