

BO1337{xAlep_WriteUp}

root@localhost:~\$ echo “b477l3 of l337”



Back To The Future

⌚ 50

- Delorean if only we can see back our pass is it great?

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

how to see the old version of a website

All Videos Images News Shopping More Tools

About 4,210,000,000 results (0.57 seconds)

Try the Wayback Machine

One of the most popular ways to see old versions of websites is via the Wayback Machine. This “machine” is actually a website that was founded by the Internet Archive. The purpose of the Wayback Machine is to scour the web to save pages and create a compressive digital record. 12 Aug 2020

<https://attorneyatlawmagazine.com> › need-proof-for-your... :: Need Proof for Your Case? 7 Ways to Find Old Versions of ...

About featured snippets • Feedback

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**.

INTERNET ARCHIVE Explore more than 706 billion web pages saved over time

DONATE WayBackMachine https://b2f.battleof1337.com/ ×

Results: 50 100 500

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.

Jason Bourne

Artartic last seen

omgjasonbourne@jmail.com

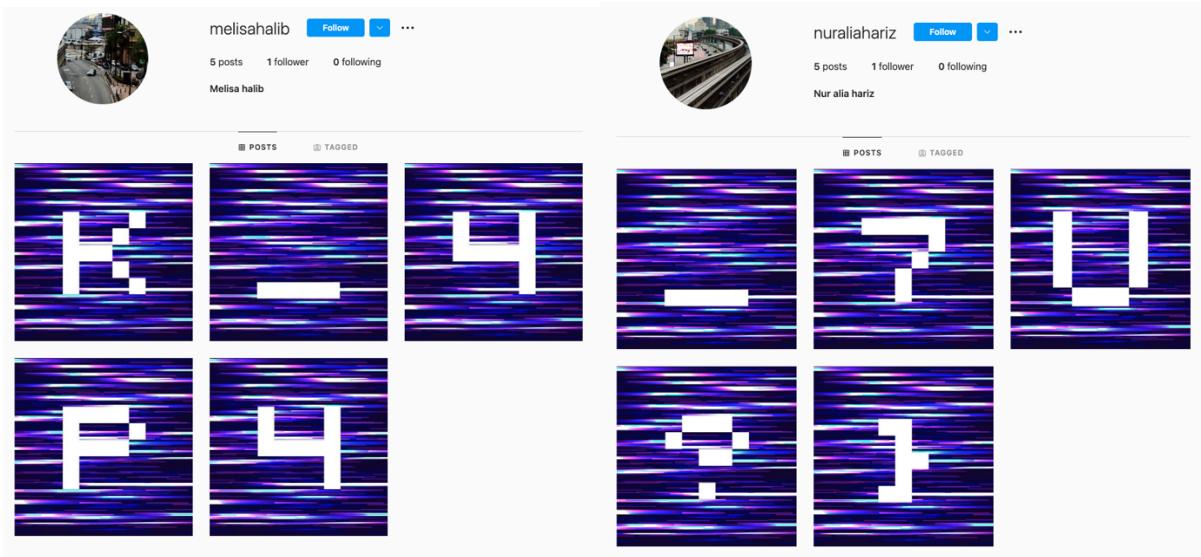
BO1337{aHR0cHM6Ly9veW0uY2F0bWUuY2Y=}

Flag : BO1337{aHR0cHM6Ly9veW0uY2F0bWUuY2Y=}

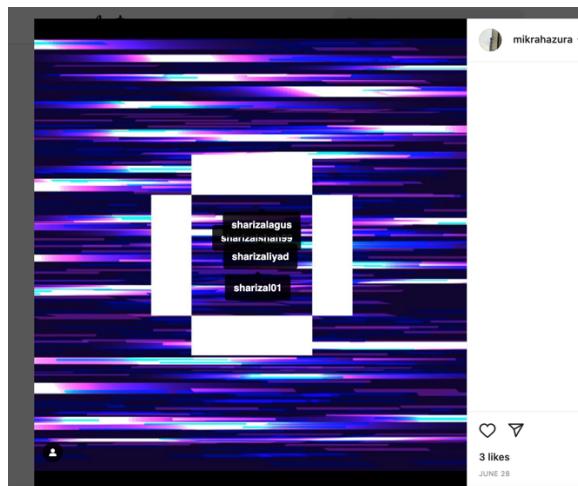


Huh I might miss something? Do it for the gram? WHAT????!!

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.



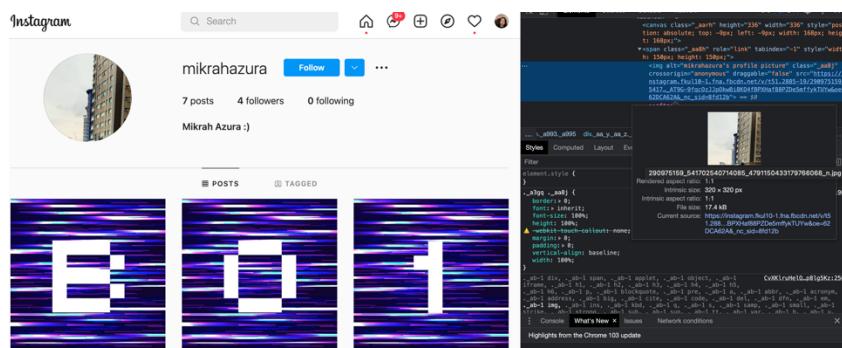
Where's the flag? Simply combine all the picture to get the flag.

Flag: BO1337{S74LK_4P4_7U?}

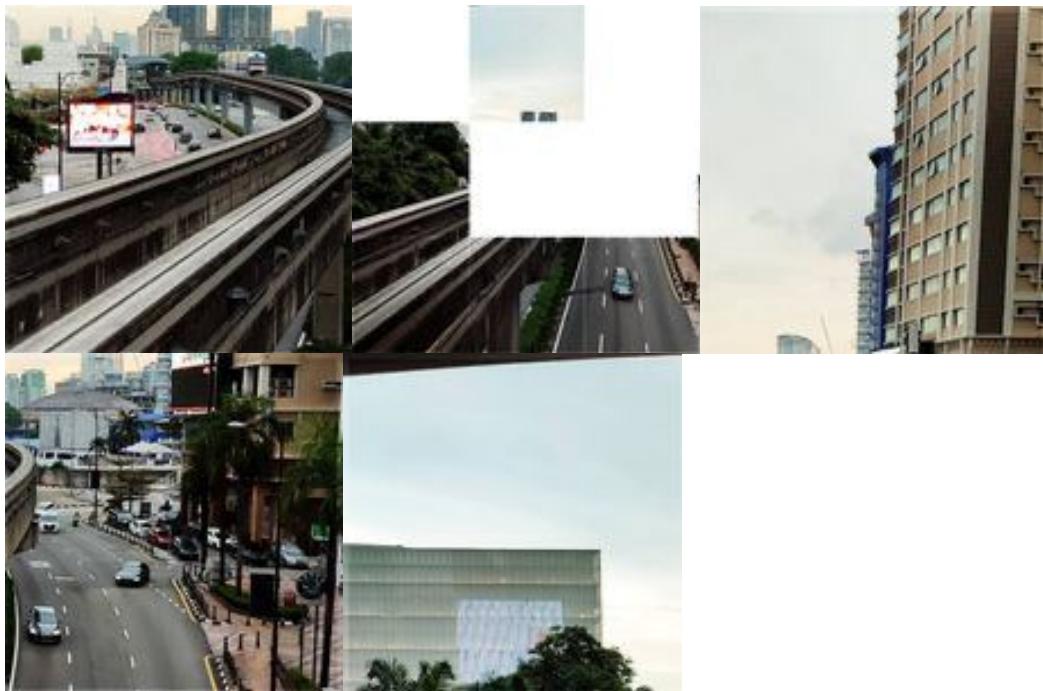


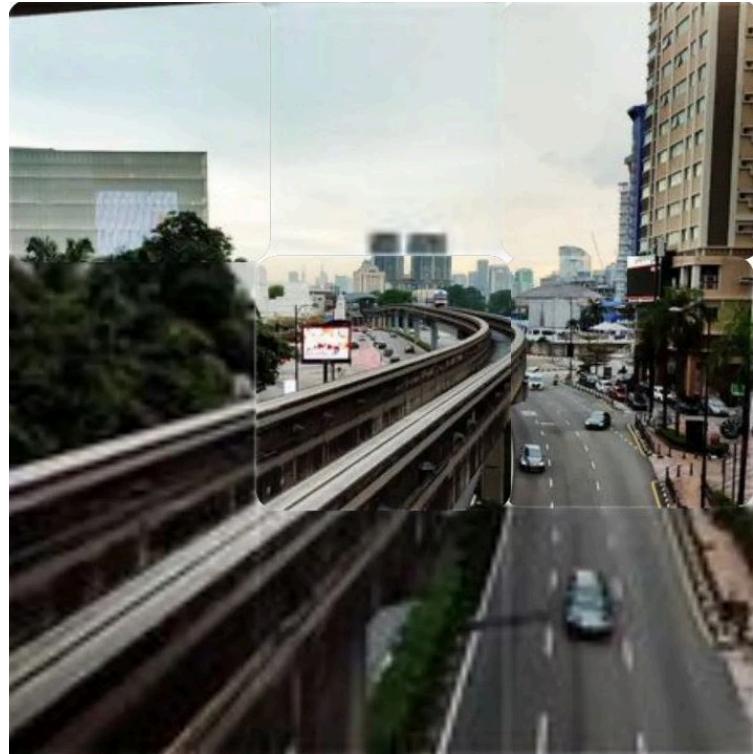
Keep stalking? Why??!!

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.





I'm 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

The screenshot shows a Google search results page with a dark theme. The search query "what file is this" is entered in the search bar. Below the search bar, there are filters for "All", "Videos", "Images", "News", "Maps", and "More". The "All" filter is selected. The results section shows a snippet from CheckFileType.com with the following text:
About 6,980,000,000 results (0.56 seconds)
<https://www.checkfiletype.com> :
CheckFileType.com - Free Online File Type Checker
Have you ever found a file on your computer without an extension or has an incorrect extension? CheckFileType.com helps you determine the true file type of any ...
You've visited this page 2 times. Last visit: 7/17/22

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

The screenshot shows the CheckFileType.com website. The logo features a blue circle with a white document and magnifying glass icon. The main heading is "CheckFileType Online - 100% Free & Secure". Below the heading, it says "Determine any file type, file extension, and MIME type based on the file contents". There are "Like 171" and "Share" buttons. A green curved arrow points to a dashed blue box containing a file preview. The preview shows a file named "1337Pikachu" with a size of "16.8 MB" and a "Remove file" button. Below the preview is a "Check File Type" button. At the bottom left, it says "Latest file types detected • Free API access".

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.

A terminal window showing a file named "sajak_ali.txt". The file contains a large amount of text in a ciphered or encoded format, consisting of several lines of characters.

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

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 **ER1337ioDjlvgduN3qrNoxdI**

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

CIPHER IDENTIFIER

Cryptography > Cipher Identifier

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE ②
ER1337ioDj1vgduN3qrNoxdl

★ CLUES/KEYWORDS (IF ANY)

► ANALYZE

See also: Frequency Analysis – Index of Coincidence

SYMBOLS IDENTIFIER

□ Go to: Symbols Cipher List

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

CAESAR CIPHER

Cryptography > Substitution Cipher > Caesar Cipher

CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT ②
ER1337ioDj1vgduN3qrNoxdl

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY (NUMBER):

USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
 USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9
 USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

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>

```
Last login: Tue Jul 19 01:49:37 on ttys001
You have new mail.
[alifzuhairi@MacBook-Pro-2 ~ % curl -I https://ifelse.battleof1337.com/index.php ]
HTTP/2 200
server: nginx-rc
date: Mon, 18 Jul 2022 17:54:21 GMT
content-type: text/html; charset=UTF-8
vary: Accept-Encoding
flag: B01337{kuc1n6_5374n}
strict-transport-security: max-age=31536000
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff

alifzuhairi@MacBook-Pro-2 ~ %
```

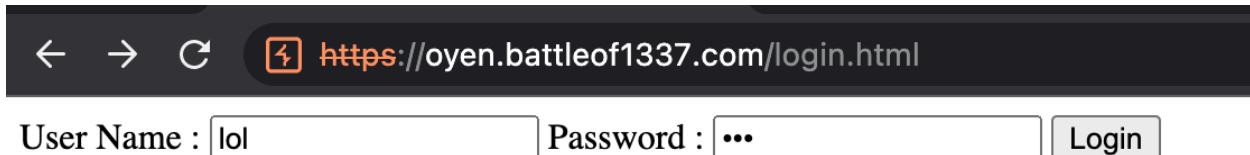
Flag: B01337{kuc1n6_5374n}

Break The Storage

50

Let's HACK some storage shall we?

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



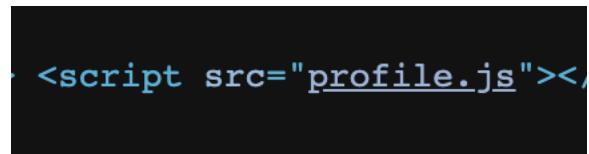
Put anything on the username and password. And turn on the intercept.

The screenshot shows the Burp Suite interface. The 'Proxy' tab is active. On the left, there's a list of intercepted requests. One specific request is selected and highlighted with a yellow background. A context menu is open over this request, listing various actions such as 'Scan', 'Send to Intruder', 'Send to Repeater', etc. The 'Send to Repeater' option is highlighted with a yellow background, indicating it is the current action being considered.

Copy the code and send it to Repeater.

Request	Response
Pretty	Raw
Hex	Render
<pre> 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": "" } } } </pre>	

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:



```

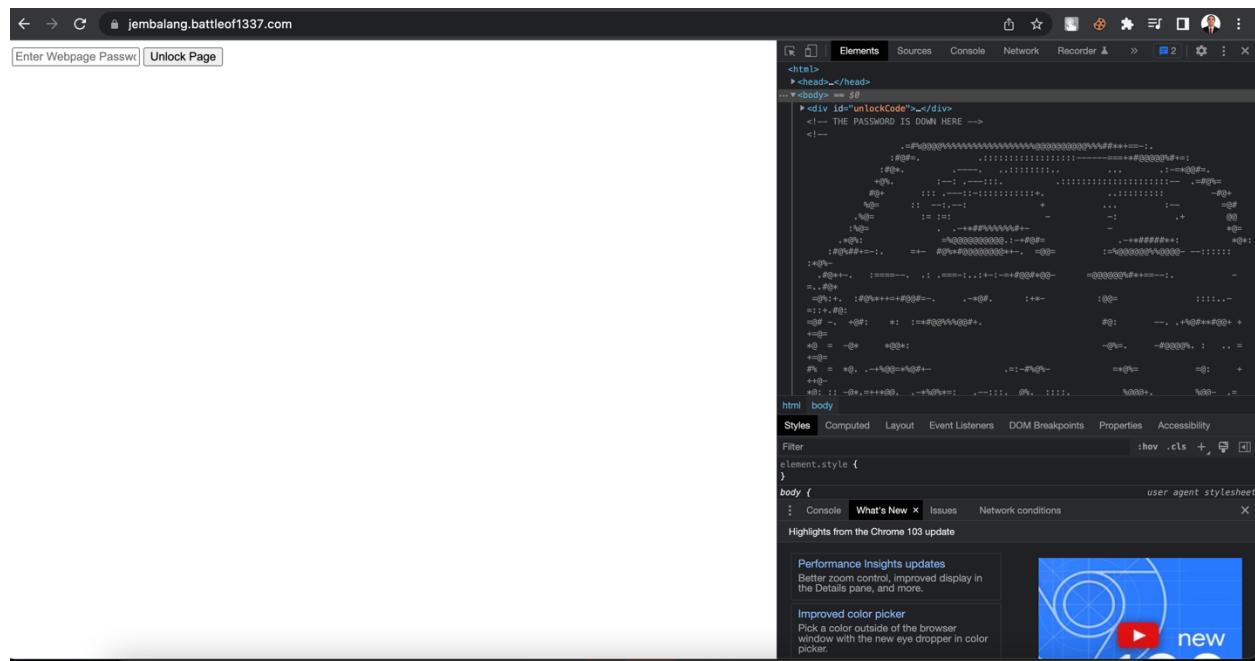
let database="data";$.get(database,function(a)
{jsons=JSON.parse(a).getFlag=jsons.user.super,window.localStorage.userID==getFlag.userID&&alert("BO1337{a2c13e70ff50376e259ddb5bd5e54a69b16e569f}"),0==window.localStorage.length&&
(window.location="login.html"));

```

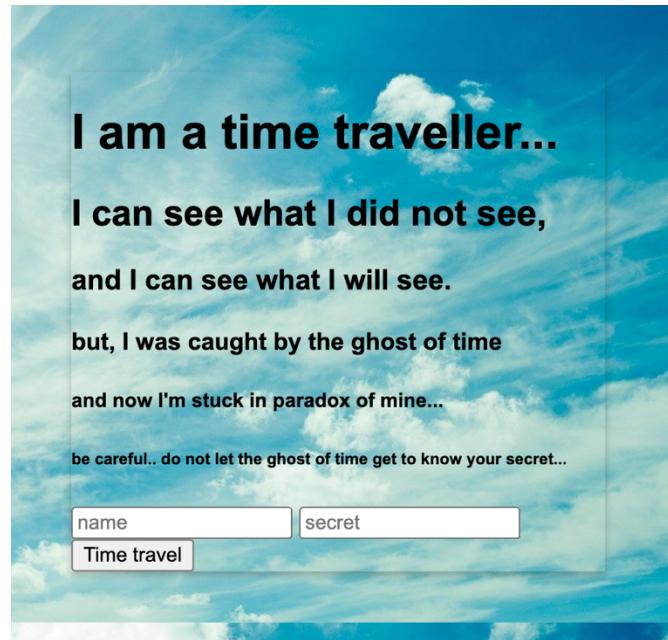
Flag: BO1337{a2c13e70ff50376e259ddb5bd5e54a69b16e569f}



**WARNING : DON'T PLAY THIS CHALLENGE IF YOU ARE NOT READY FOR BHAAAAAA
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.

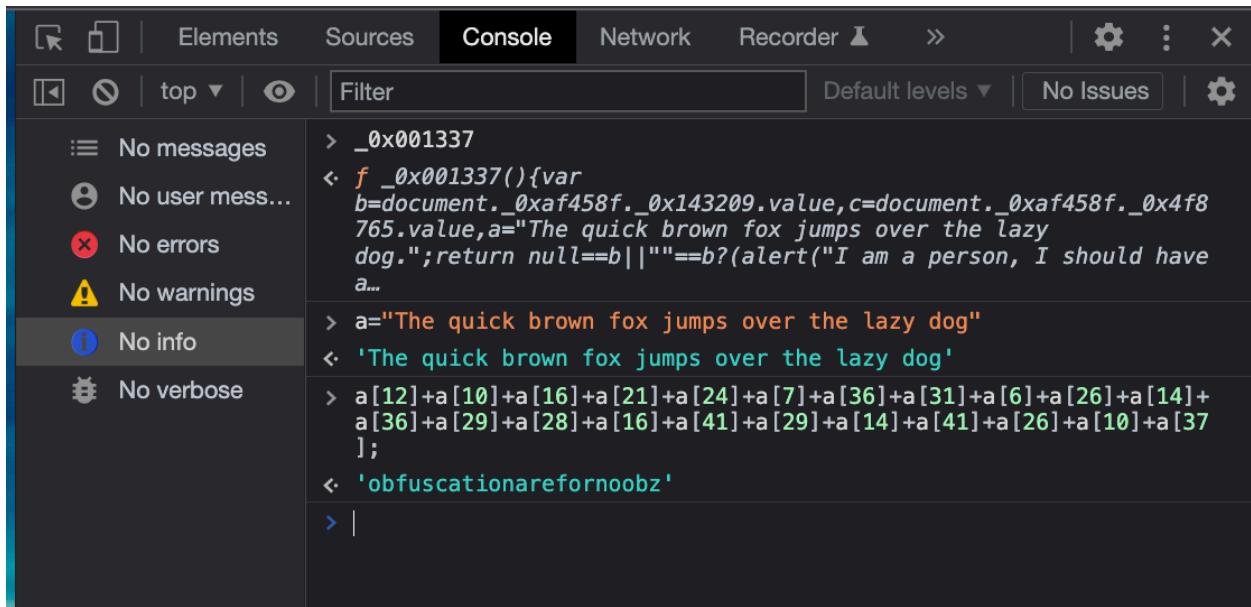
```
<h4>but, I was caught by the ghost of time</h4>
<h5>and now I'm stuck in paradox of mine...</h5>
<h6>be careful.. do not let the ghost of time get to know your secret...</h6>
►<form method="post" name="_0xaf458f" onsubmit="return _0x001337()">...</form>
</div>
<script src="4b97781....js"></script>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



The screenshot shows the Chrome DevTools interface with the 'Console' tab selected. On the left, there's a sidebar with various status indicators: 'No messages', 'No user mess...', 'No errors', 'No warnings', 'No info' (which is currently selected), and 'No verbose'. The main console area contains the following obfuscated code:

```
> _0x001337
< f _0x001337(){var
b=document._0xa4f458f._0x143209.value,c=document._0xa4f458f._0x4f8
765.value,a="The quick brown fox jumps over the lazy
dog.;"return null==b||""==b?(alert("I am a person, I should have
a...
> a="The quick brown fox jumps over the lazy dog"
< 'The quick brown fox jumps over the lazy dog'
> 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]
];
< 'obfuscationarefornoobz'
> |
```

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}