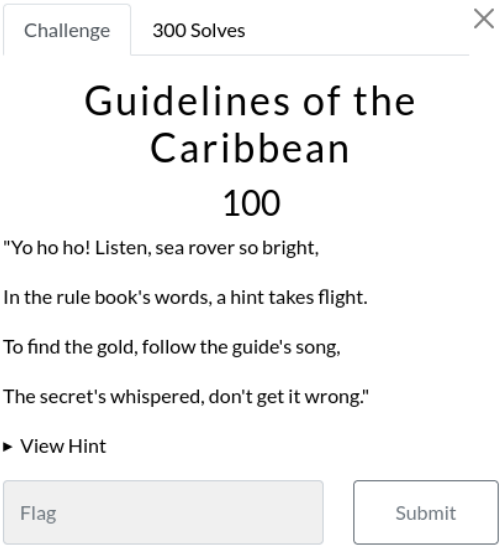
Questcon CTF Writeup

Ctftime link -> https://ctftime.org/event/2141/
Discord -> https://discord.gg/nHXaRhTbkS

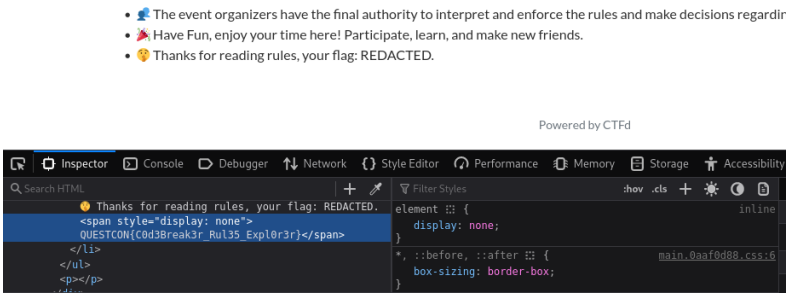
Our team solved all challenges in this ctf !!!

Misc

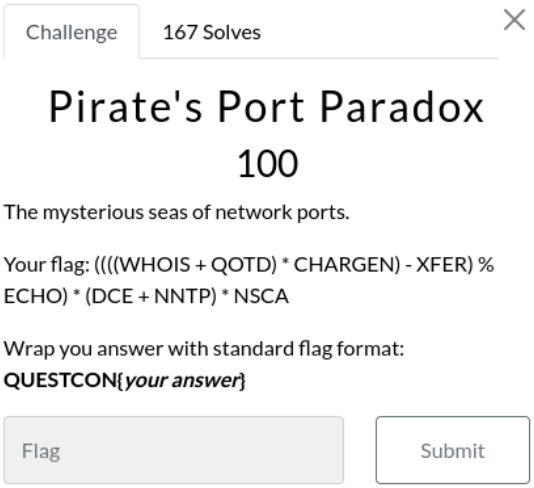
Guidelines of the Caribbean



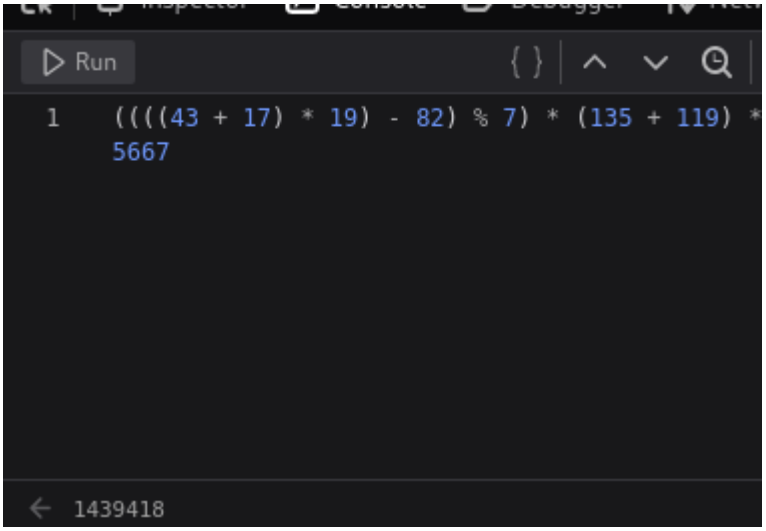
Simple , only need to check guidelines and u will see , “your flag , REDACTED” so inspect it.
QUESTCON{C0d3Break3r_Rul35_Expl0r3r}



Pirate's Port Paradox (solved by teammate)

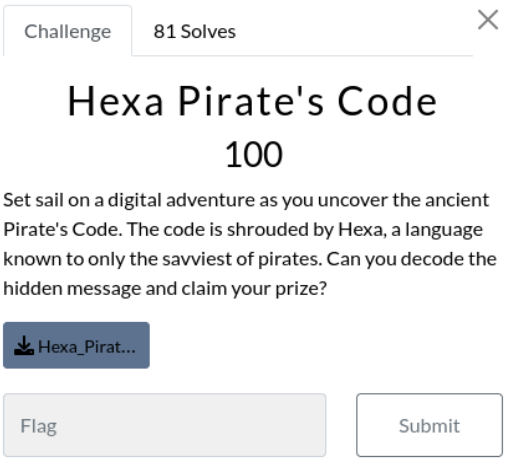


We need to find network ports of whois , qotd ,chargen and so on .Then calculate using the given formula.



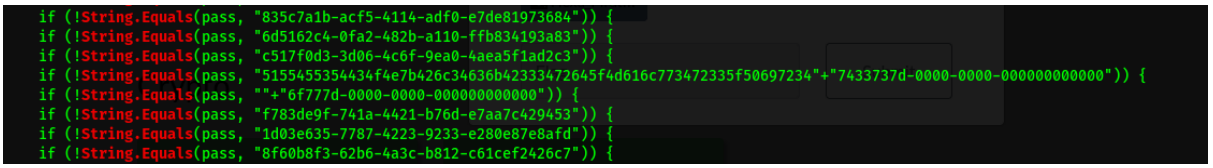
QUESTCON{1439418}

Hexa Pirate's Code



In this chall , a zip file is given, so unzip it and u can see a lot of files with hashed name !!! But when u check'em with strings or cat , these are html documents. When u check in details, u'll see suspicious pass validation!

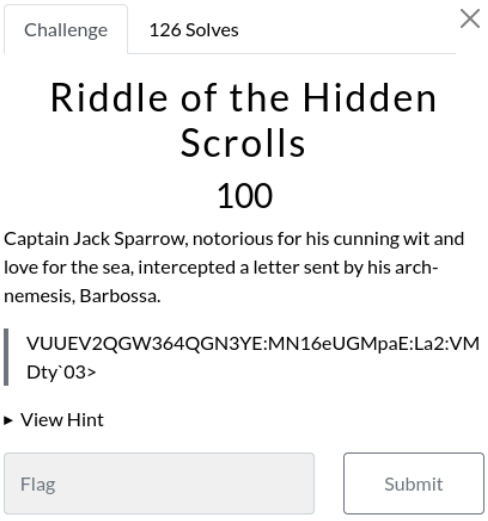
So use grep to find all validations of all files.
strings * | grep 'String.Equals'
Then u will see a validation that is longer than the other.



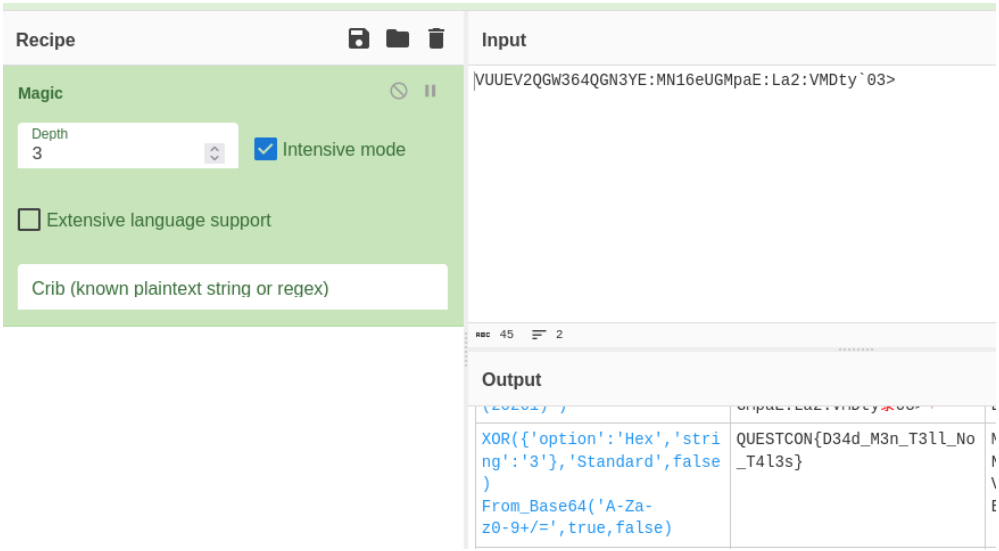
So I copied and translated hex to text AND got the flag.

Crypto

Riddle of the Hidden Scrolls (solved by teammate)



Super simple , just put it in [CyberChef] and drag Magic , Then flag is out!!!

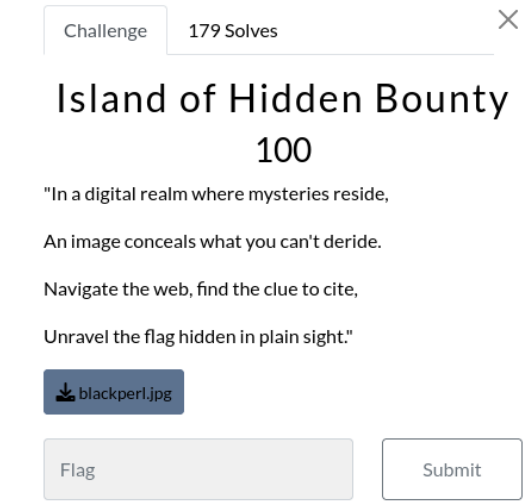


Sparrow's Cryptographic Treasure

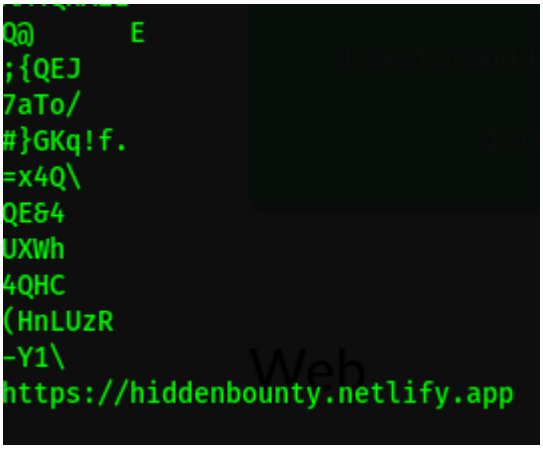
The chall gives us a txt file , We have
N = 882564595536224140639625987659416029426239230804614613279163
E = 65537
C = 164269225538436495685306542268826436068505673594249194166792
In this file . It's beginner level rsa and we can decrypt using [dcode.fr/rsa-cipher] tool.

Forensics

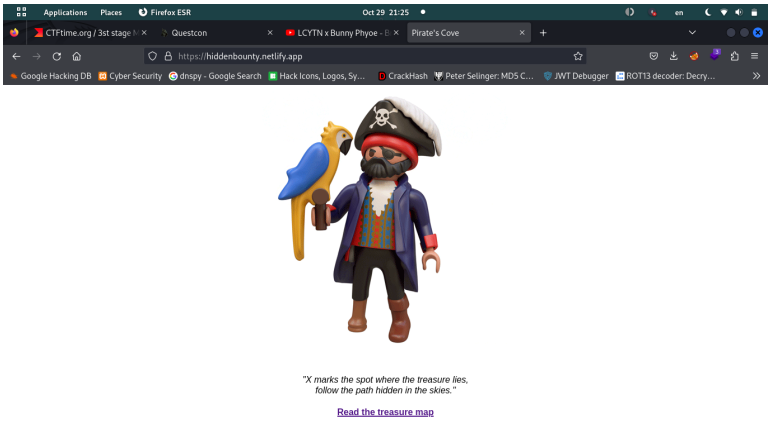
Island of Hidden Bounty



In this challenge, an image file is given . At first, I checked this image with strings cmd and an url is found.



Then I visited this link and checked if there was robots.txt directory or not . But … it worked.

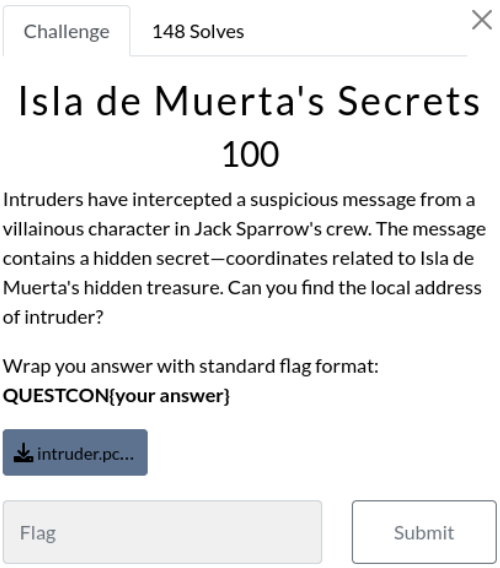


```
User-agent: *
Disallow: /HiddenInMist.html
```

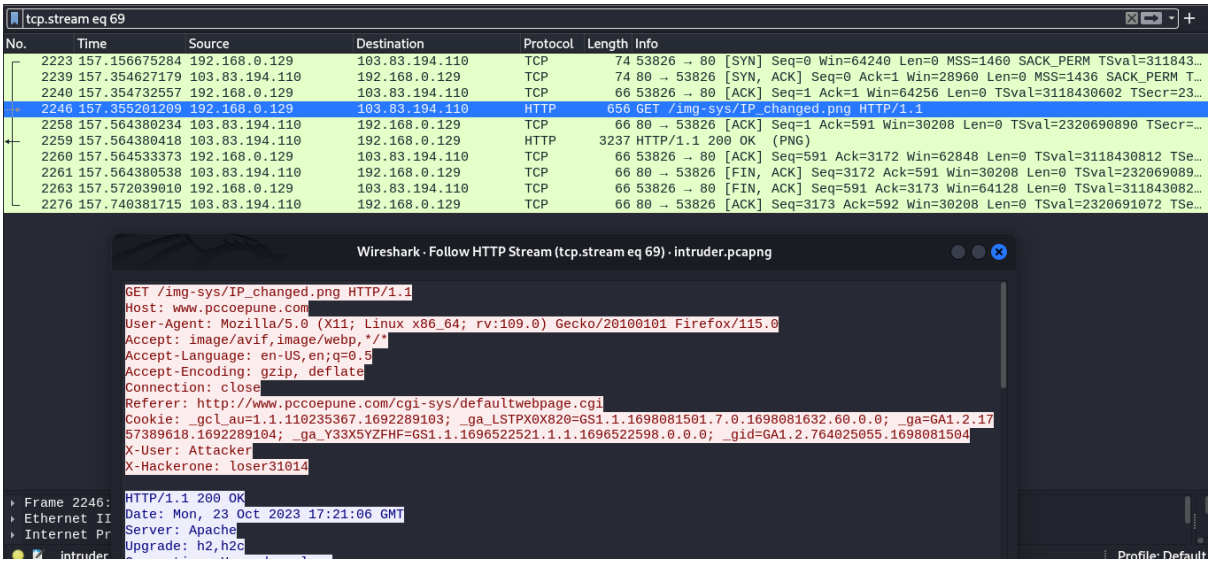
And I continued visiting of hidden directory then flag is out

QUESTCON{X_M4rk5Th3Digit4lTr34sur3}

Isla de Muertas Secrets



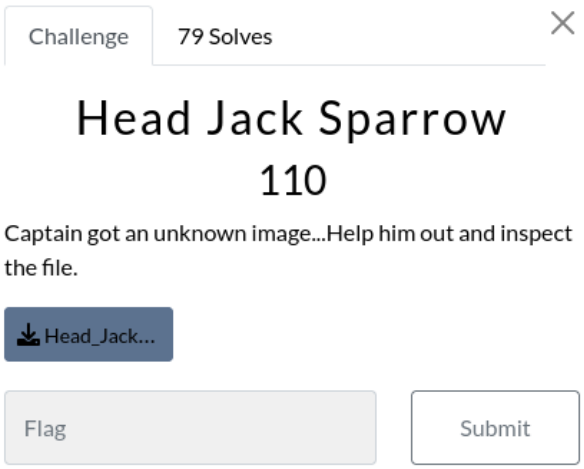
A pcapng file is given. So I checked with wireshark tools . First I filtered with http protocol .Then I found suspicious traffic that has IP_Changed.png



Then I followed http stream and saw X-User is Attacker so his destination ip can be local address . I put it in flag format and it's correct!

QUESTCON{192.168.0.129}

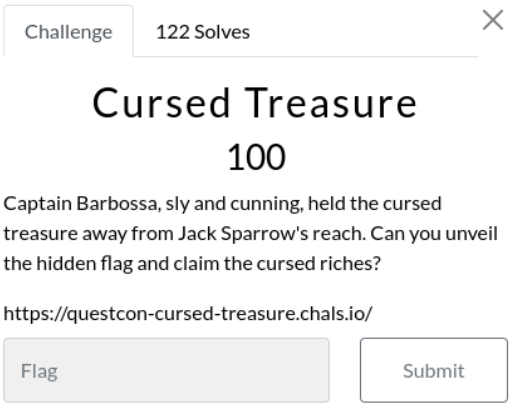
Head Jack Sparrow



The given image is with wrong header. So I fixed magic header
89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52
And got a png. the flag is there but u need to zoom in :3

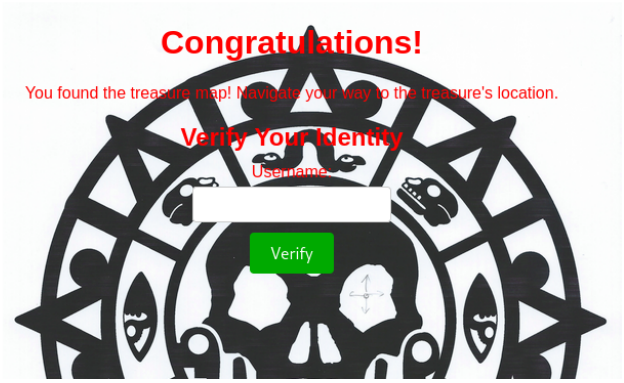
Web

Cursed Treasure

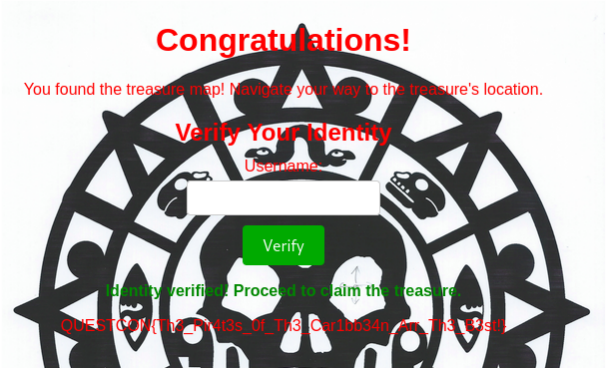


This challenge is eazy af. First I visit the given link and click on a map.
The parameter is like ,
id=e25388fde8290dc286a6164fa2d97e551b53498dcbf7bc378eb1f178
check type of hash with has-identifier tool and it's sha224 hash
When I dehash it , it shows 1.So parameter will be id=1.I dehashed the second one and is also id=2, But the third parameter values is 4, So 3 is missing. That's why I used an online tool that can hash 3 into sha225 values and I set

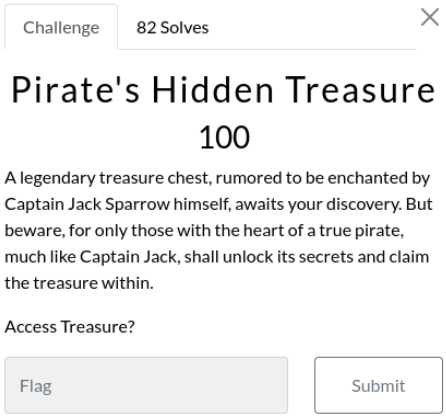
id=4cfc3a1811fe40afa401b25ef7fa0379f1f7c1930a04f8755d678474
It worked and I found a hidden page that can login .



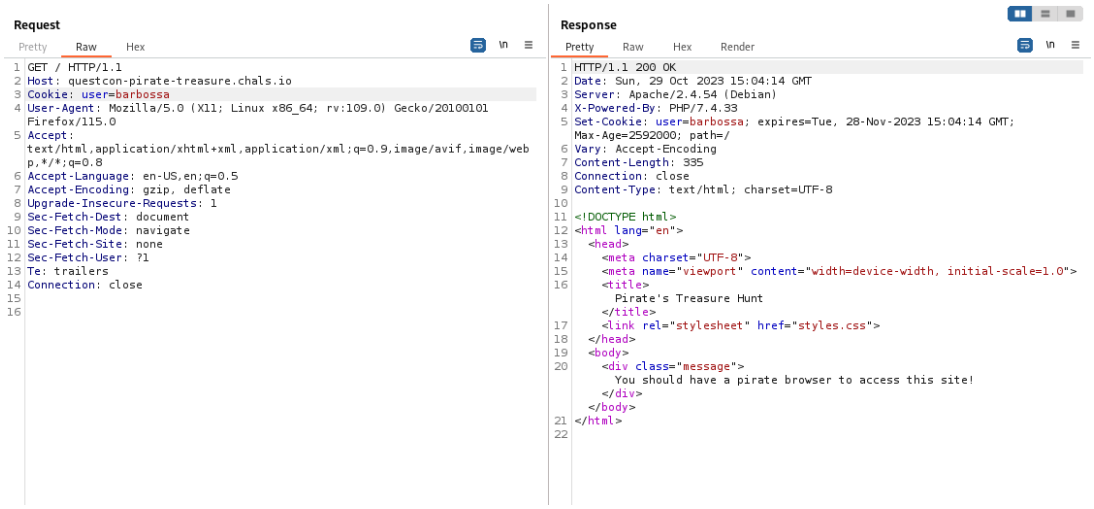
I know username is Barbossa coz it's given in challenge description! Then flag is out!



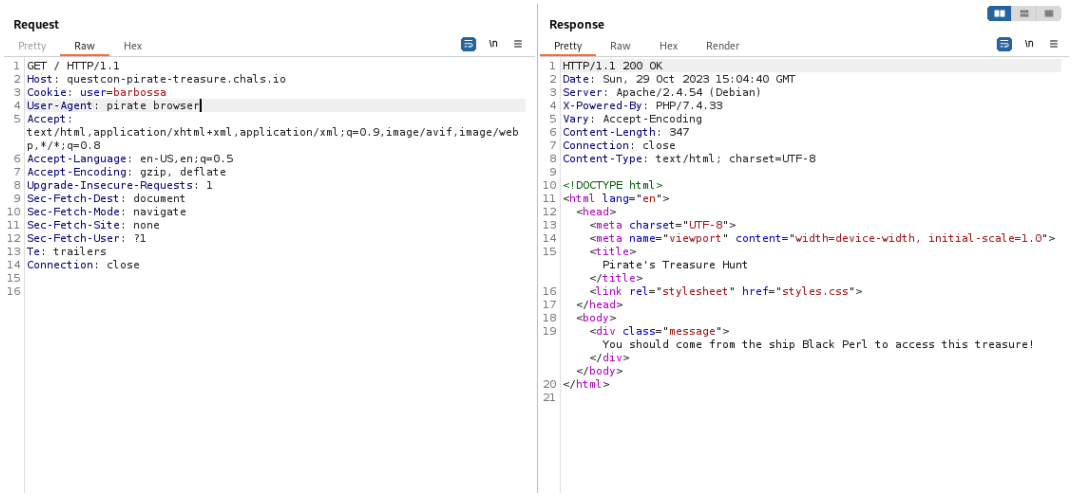
Pirate's Hidden Treasure



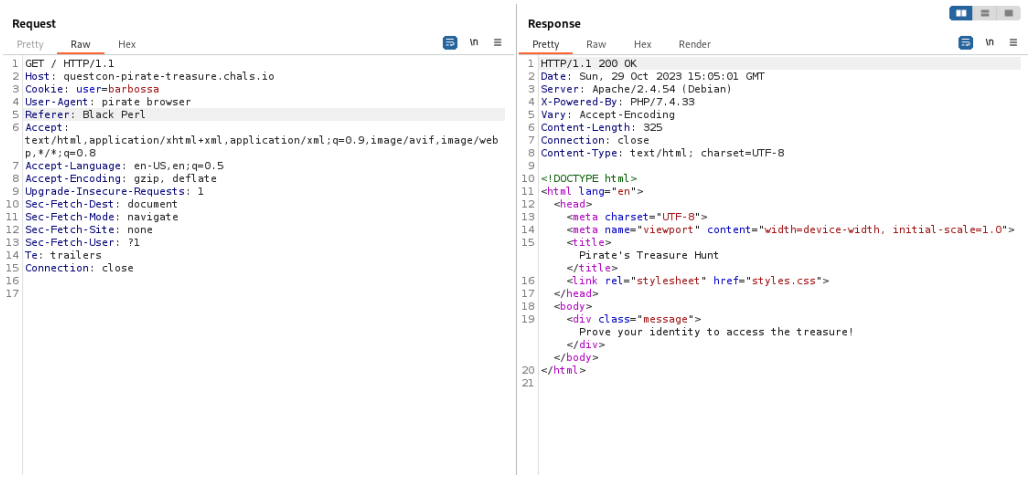
It's a great challenge! First I visited the given link and it says "You should have pirate browser"



So I bypassed editing User-Agent: pirate browser. But I got another filter "You Should come from the ship Black Perl"



I know I should add Referer : Black Perl , So I added and requested it again



Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: questcon-pirate-treasure.chals.io
Cookie: user=barbossa
User-Agent: pirate browser
Referer: Black Perl
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

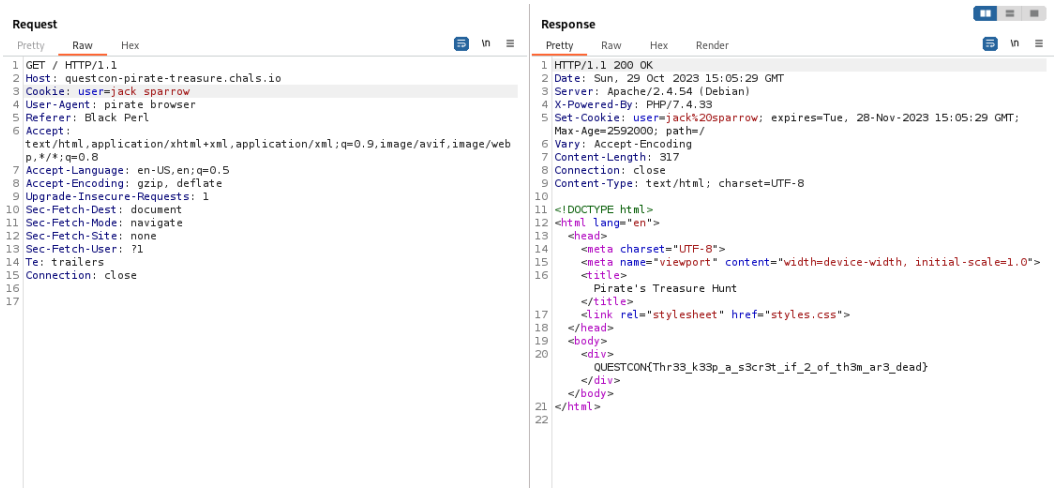
Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 29 Oct 2023 15:05:01 GMT
Server: Apache/2.4.54 (Debian)
X-Powered-By: PHP/7.4.33
Vary: Accept-Encoding
Content-Length: 325
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      Pirate's Treasure Hunt
    </title>
    <link rel="stylesheet" href="styles.css">
  </head>
  <body>
    <div class="message">
      Prove your identity to access the treasure!
    </div>
  </body>
</html>
```

I have to identify to access the browser ,So we clearly read the challenge description ,we can solve it ezly .only jack sparrow can unlock secret. So I changed cookie value as jack sparrow and got the flag



Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: questcon-pirate-treasure.chals.io
Cookie: user=jack sparrow
User-Agent: pirate browser
Referer: Black Perl
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response

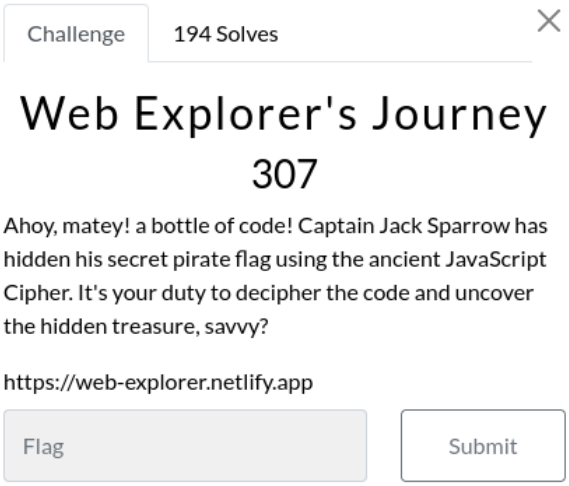
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 29 Oct 2023 15:05:29 GMT
Server: Apache/2.4.54 (Debian)
X-Powered-By: PHP/7.4.33
Set-Cookie: user=jack%20sparrow; expires=Tue, 28-Nov-2023 15:05:29 GMT;
Max-Age=2592000; path=/
Vary: Accept-Encoding
Content-Length: 317
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      Pirate's Treasure Hunt
    </title>
    <link rel="stylesheet" href="styles.css">
  </head>
  <body>
    <div>
      QUESTCON{Thr33_k33p_a_s3cr3t_if_2_of_th3m_ar3_dead}
    </div>
  </body>
</html>
```

QUESTCON{Th3_Pir4t3s_0f_Th3_Car1bb34n_Arr_Th3_B3st!}

Web Explorer's Journey



In this challenge ,encoded flag value is given.

So I checked source code and found something.In source code, the real encoded flag and a javascript file are found.

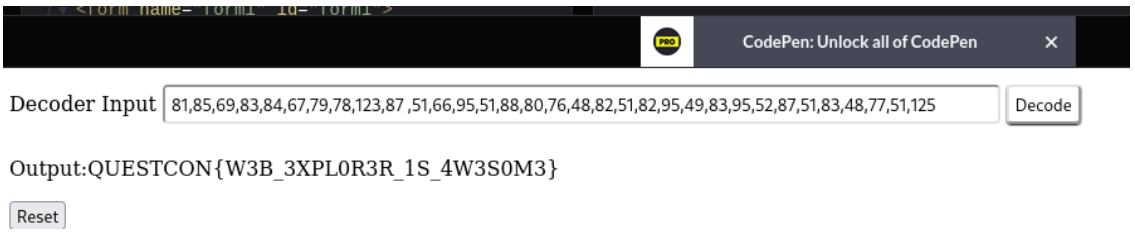
```
<head>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>Web Explorer's Journey</title>
  <link rel="stylesheet" href="./styles.css" />
</head>
<body>
  <h1>
    Pirates are warming up for the next adventure. Can you find the flag!!!
  </h1>
  <div class="container">
    Your flag is:
    <div id="flag">
      818569838467797812387516695518880764882518295498395528751834877511 25
    </div>
    <div class="displaynone">
      NOTE: Flag contains only capial letters, numbers and curly brackets.
    </div>
  </div>

  <script src="script.js"></script>
</body>
</html>
```

```
let flag = "flag{Test_Flag}";
let encryptedFlag = "";
function encodeFlag() {
  for (let i = 0; i < flag.length; i++) {
    encryptedFlag += flag.charCodeAt(i);
  }
}

encodeFlag();
document.getElementById("flag").innerHTML = encryptedFlag;
```

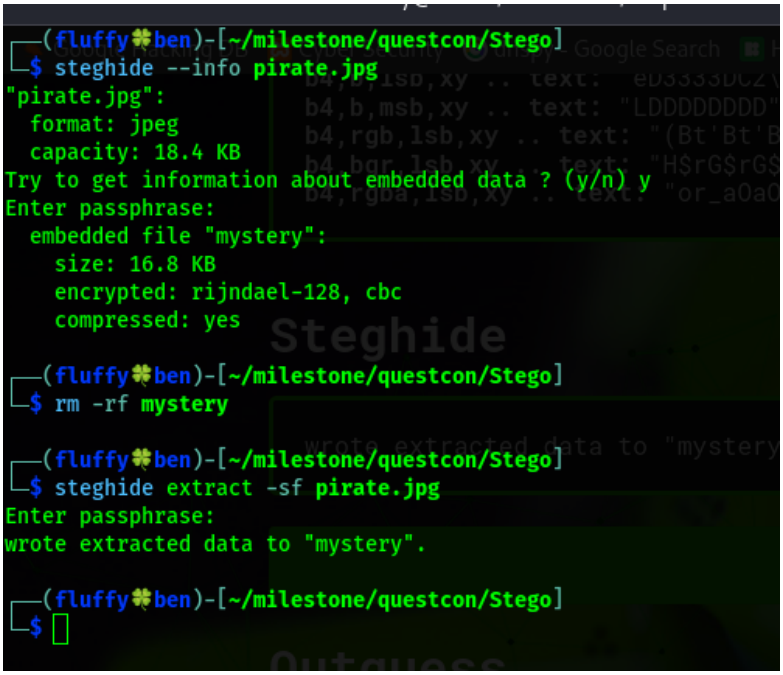
I analysed it and knew that they are decimal codes
So I made them in this format
81,85,69,83,84,67,79,78,123,87,51,66,95,51,88,80,76,48,82,51,82,95,49,83,95,52,87,51,83,48,77,51,125
And used an online tool to decode it then flag is out.



Stegano

Mystery

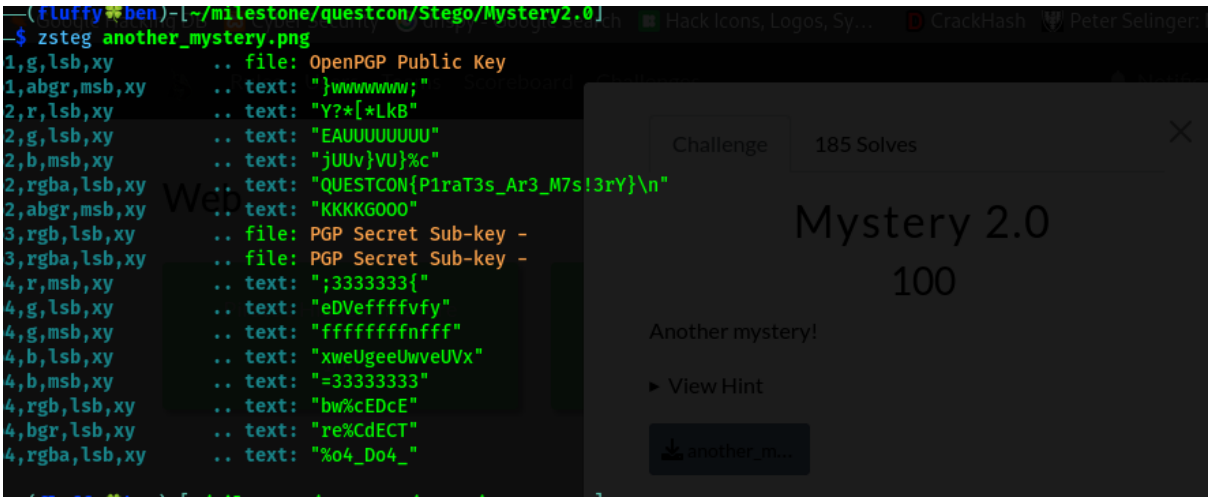
I downloaded the image and checked with steghide .I need a password to extract data.So at first I tried with pirate as pw but didn't work because it doesn't need pw. Just hit enter and mystery file is out.



Mystery is also an image file so I checked with exiftool and base64 value is found.So I decoded and flag is out

Mystery 2.0

I checked the given png file with zsteg and flag is out. Super ez



Author : Min Yell Si Thu
Nov 25 ,2023
Hope we can explore new new things together
Have fun guyss