

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

Challenge 300 Solves X

Guidelines of the Caribbean

100

"Yo ho ho! Listen, sea rover so bright,
In the rule book's words, a hint takes flight.
To find the gold, follow the guide's song,
The secret's whispered, don't get it wrong."

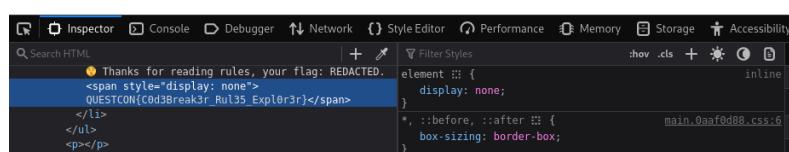
► View Hint

Flag Submit

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

- 🌐 The event organizers have the final authority to interpret and enforce the rules and make decisions regarding them.
- 🎉 Have Fun, enjoy your time here! Participate, learn, and make new friends.
- 📖 Thanks for reading rules, your flag: REDACTED.

Powered by CTFd



Pirate's Port Paradox (solved by teammate)

Challenge

167 Solves



Pirate's Port Paradox

100

The mysterious seas of network ports.

Your flag: (((WHOIS + QOTD) * CHARGEN) - XFER) %
ECHO) * (DCE + NNTP) * NSCA

Wrap your answer with standard flag format:

QUESTCON{*your answer*}

Flag

Submit

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

```
Run { } ^ v Q |  
1 (((43 + 17) * 19) - 82) % 7) * (135 + 119) *  
5667  
← 1439418
```

QUESTCON{1439418}

Hexa Pirate's Code

Challenge

81 Solves



Hexa Pirate's Code

100

Set sail on a digital adventure as you uncover the ancient Pirate's Code. The code is shrouded by Hexa, a language known to only the savviest of pirates. Can you decode the hidden message and claim your prize?

Hexa_Pirat...

Flag

Submit

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!

```
    return new String(CharArrayReplica.Create((length > 32) ? StringRandom.Next((int)length) :
```

```
})
```

```
protected void Page_load(object sender, EventArgs e) {
```

```
    var pass = Request.Headers["X-siLock-Comment"];
```

```
    if (!String.Equals(pass, "6a4426ab-71c7-44d0-afbb-70403f23c9aa")) {
```

```
        Response.StatusCode = 404;
```

```
        return;
```

```
    }
```

```
    Response.AppendHeader("X-siLock-Comment", "comment");
```

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.

```
if (!String.Equals(pass, "835c7a1b-acf5-4114-adf0-e7de81973684")) {
```

```
if (!String.Equals(pass, "6d5162c4-0fa2-482b-a110-ffb834193a83")) {
```

```
if (!String.Equals(pass, "c517fd03-3d06-4c6f-9ea0-4aea5f1ad2c3")) {
```

```
if (!String.Equals(pass, "5155455354434f4e7b426c34636b42333472645f4d616c773472335f50697234"+"7433737d-0000-0000-000000000000")) {
```

```
if (!String.Equals(pass, ""+6f77d-0000-0000-000000000000)) {
```

```
if (!String.Equals(pass, "f783de9f-741a-4421-b76d-e7aa7c429453")) {
```

```
if (!String.Equals(pass, "1d03ee35-7787-4223-9233-e280e87e8af4")) {
```

```
if (!String.Equals(pass, "8f60b8f3-62b6-4a3c-b812-c61cef2426c7")) {
```

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

Hex	To	Text
5155455354434f4e7b426c34636b423334726 45f4d616c773472335f506972347433737d		QUESTCON{Bl4ckB34rd_Malw4r3_Pir4t3s}

Crypto

Riddle of the Hidden Scrolls (solved by teammate)

Challenge 126 Solves X

Riddle of the Hidden Scrolls

100

Captain Jack Sparrow, notorious for his cunning wit and love for the sea, intercepted a letter sent by his arch-nemesis, Barbossa.

VUUEV2QGW364QGN3YE:MN16eUGMpaE:La2:VM
Dty'03>

► View Hint

Flag

Submit

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

Sparrow's Cryptographic Treasure

Challenge

292 Solves



Sparrow's Cryptographic Treasure

100

Jack Sparrow has encrypted a secret message using RSA cryptography to protect the location of his hidden treasure.

Cryptogra...

Flag

Submit

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

Challenge 179 Solves X

Island of Hidden Bounty

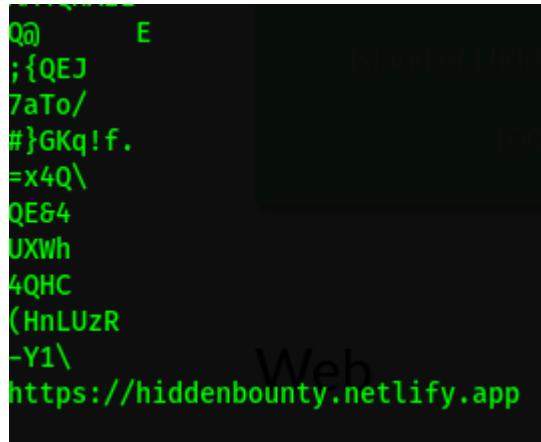
100

"In a digital realm where mysteries reside,
An image conceals what you can't deride.
Navigate the web, find the clue to cite,
Unravel the flag hidden in plain sight."

 blackperl.jpg

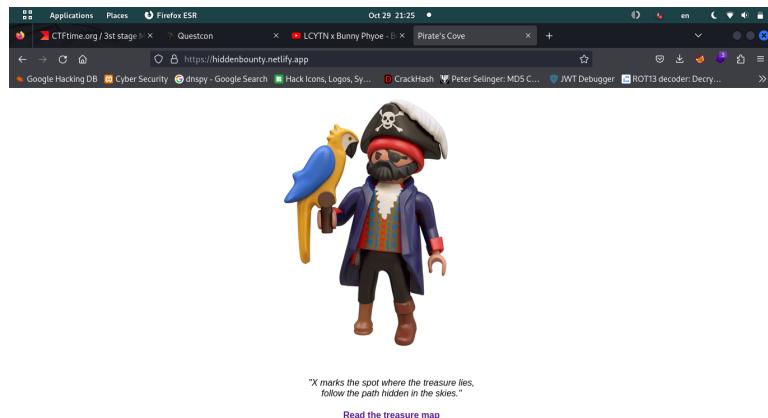
Flag Submit

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



```
Q@      E
;{QEJ
7aTo/
#}GKq!f.
=x4Q\
QE&4
UXWh
4QHC
(HnLUzR
-Y1\          Web
https://hiddenbounty.netlify.app
```

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

Challenge 148 Solves X

Isla de Muerta's Secrets

100

Intruders have intercepted a suspicious message from a villainous character in Jack Sparrow's crew. The message contains a hidden secret—coordinates related to Isla de Muerta's hidden treasure. Can you find the local address of intruder?

Wrap your answer with standard flag format:

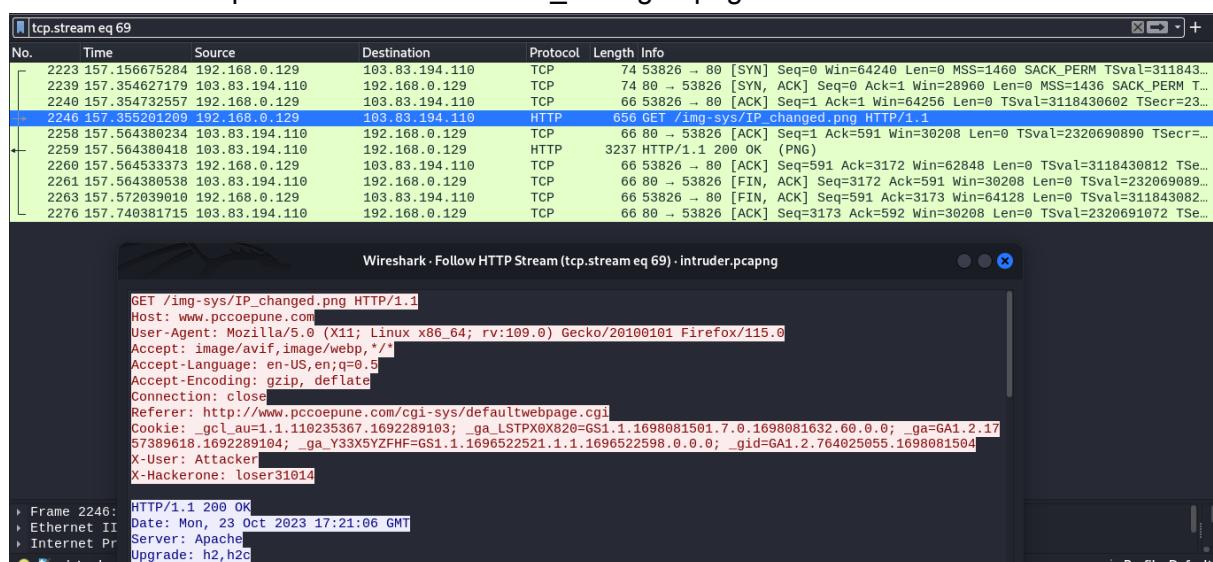
QUESTCON{your answer}

 intruder.pcapng

Flag

Submit

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



The Wireshark interface shows a packet capture titled "tcp.stream eq 69". A specific packet, frame 2246, is selected. The details pane shows the following request:

```
GET /img-sys/IP_changed.png HTTP/1.1
Host: www.pccoeepune.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://www.pccoeepune.com/cgi-sys/defaultwebpage.cgi
Cookie: _gcl_au=1.1.110235367.1692289103; _ga_LSTPX0X820=GS1.1.1698081501.7.0.1698081632.60.0.0; _ga=GA1.2.1757389618.1692289104; _ga_Y33X5YZFHF=GS1.1.1696522521.1.1.1696522598.0.0.0; _gid=GA1.2.764025055.1698081504
X-User: Attacker!
X-Hackerone: loser31014
```

The packet details show the following information:

No.	Time	Source	Destination	Protocol	Length	Info
2223	157.156675284	192.168.0.129	103.83.194.110	TCP	74	53826 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=311843...
2239	157.354627179	103.83.194.110	192.168.0.129	TCP	74	80 → 53826 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1436 SACK_PERM T...
2240	157.354732557	192.168.0.129	103.83.194.110	TCP	66	53826 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3118430602 TSeqr=23...
2246	157.355201209	192.168.0.129	103.83.194.110	HTTP	656	GET /img-sys/IP_changed.png HTTP/1.1
2258	157.564380234	103.83.194.110	192.168.0.129	TCP	66	80 → 53826 [ACK] Seq=1 Ack=591 Win=30208 Len=0 TSval=2320690890 TSeqr=...
2259	157.564380418	103.83.194.110	192.168.0.129	HTTP	3237	HTTP/1.1 200 OK (PNG)
2260	157.564533373	192.168.0.129	103.83.194.110	TCP	66	53826 → 80 [ACK] Seq=591 Ack=3172 Win=62848 Len=0 TSval=3118430812 TSe...
2261	157.564380538	103.83.194.110	192.168.0.129	TCP	66	80 → 53826 [FIN, ACK] Seq=3172 Ack=591 Win=30208 Len=0 TSval=232069089...
2263	157.572039010	192.168.0.129	103.83.194.110	TCP	66	53826 → 80 [FIN, ACK] Seq=591 Ack=3173 Win=64128 Len=0 TSval=311843082...
2276	157.740381715	103.83.194.110	192.168.0.129	TCP	66	80 → 53826 [ACK] Seq=3173 Ack=592 Win=30208 Len=0 TSval=2320691072 TSe...

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}

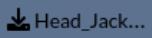
Head Jack Sparrow

Challenge 79 Solves X

Head Jack Sparrow

110

Captain got an unknown image...Help him out and inspect the file.

 Head_Jack...

Flag Submit

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

Challenge

122 Solves

X

Cursed Treasure

100

Captain Barbossa, sly and cunning, held the cursed treasure away from Jack Sparrow's reach. Can you unveil the hidden flag and claim the cursed riches?

<https://questcon-cursed-treasure.chals.io/>

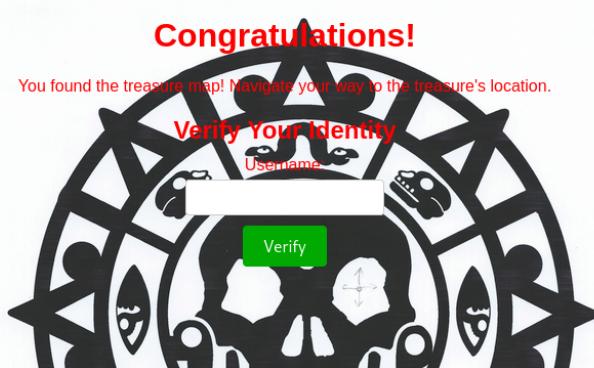
Flag

Submit

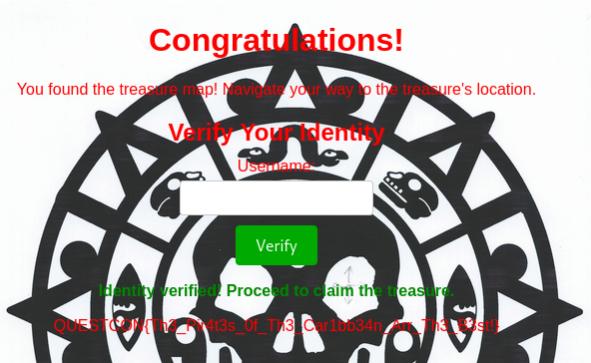
This challenge is eazy af. First I visit the given link and click on a map. The parameter is like ,
id=e25388fde8290dc286a6164fa2d97e551b53498dcbf7bc378eb1f178
check type of hash with has-identifier tool and it's sha224 hash
When I dehash it , it shows 1.So parameter will be id=1.I dehashed the second 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=4cf3a1811fe40afa401b25ef7fa0379f1f7c1930a04f8755d678474

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

Challenge | **82 Solves**

Pirate's Hidden Treasure

100

A legendary treasure chest, rumored to be enchanted by Captain Jack Sparrow himself, awaits your discovery. But beware, for only those with the heart of a true pirate, much like Captain Jack, shall unlock its secrets and claim the treasure within.

Access Treasure?

Flag

[Submit](#)

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

Request

Pretty Raw Hex

1 GET / HTTP/1.1
2 Host: question-pirate-treasure.chals.io
3 Cookie: user=barbossa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Sun, 29 Oct 2023 15:04:14 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Set-Cookie: user=barbossa; expires=Tue, 28-Nov-2023 15:04:14 GMT;
Max-Age=3600; path=/
6 Vary: Accept-Encoding
7 Content-Length: 335
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11 <!DOCTYPE html>
12 <html lang="en">
13 <head>
14 <meta charset="UTF-8">
15 <meta name="viewport" content="width=device-width, initial-scale=1.0">
16 <title>
Pirate's Treasure Hunt
</title>
17 <link rel="stylesheet" href="styles.css">
18 </head>
19 <body>
20 <div class="message">
You should have a pirate browser to access this site!
</div>
</body>
21 </html>
22

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

Request

Pretty Raw Hex

1 GET / HTTP/1.1
2 Host: questcon-pirate-treasure.chals.io
3 Cookie: user=barbossa
4 User-Agent: pirate browser!
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Sun, 29 Oct 2023 15:04:40 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Vary: Accept-Encoding
6 Content-Length: 347
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="en">
12 <head>
13 <meta charset="UTF-8">
14 <meta name="viewport" content="width=device-width, initial-scale=1.0">
15 <title>
16 <!-- Pirate's Treasure Hunt -->
17 </title>
18 <body>
19 <div class="message">
20 <p>You should come from the ship Black Perl to access this treasure!</p>
21 </div>
22 </body>
23 </html>

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

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: queston-pirate-treasure.chals.io
3 Cookie: user=barbossa
4 User-Agent: pirate browser
5 Referer: Black Perl
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 29 Oct 2023 15:05:01 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Vary: Accept-Encoding
6 Content-Length: 325
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0">
15     <title>
16       Pirate's Treasure Hunt
17     </title>
18     <link rel="stylesheet" href="styles.css">
19   </head>
20   <body>
21     <div class="message">
Prove your identity to access the treasure!
</div>
</body>
</html>
21
```

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	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET / HTTP/1.1 2 Host: question-pirate-treasure.chals.io 3 Cookie: user=jack_sparrow 4 User-Agent: pirate browser 5 Accept: */*;q=1 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1 14 Te: trailers 15 Connection: close 16 17	1 HTTP/1.1 200 OK 2 Date: Sun, 29 Oct 2023 15:05:29 GMT 3 Server: Apache/2.4.54 (Debian) 4 X-Powered-By: PHP/7.4.33 5 Set-Cookie: user=jack420sparrow; expires=Tue, 28-Nov-2023 15:05:29 GMT; Max-Age=20200000; path=/ 6 Vary: Accept-Encoding 7 Content-Length: 317 8 Connection: close 9 Content-Type: text/html; charset=UTF-8 10 11 <!DOCTYPE html> 12 <html lang="en"> 13 <head> 14 <meta charset="UTF-8"> 15 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 16 <title> 17 </title> 18 <link rel="stylesheet" href="styles.css"> 19 </head> 20 <body> 21 <div> 22 QUESTCON{Thr33_k33p_a_s3cr3t_if_2_of_th3m_ar3_d3ad} 23 </div> 24 </body> 25 </html>

QUESTCON{Th3_Pir4t3s_0f_Th3_Car1bb34n_Arr_Th3_B3st!}

Web Explorer's Journey

Challenge 194 Solves X

Web Explorer's Journey

307

Ahoj, matey! a bottle of code! Captain Jack Sparrow has hidden his secret pirate flag using the ancient JavaScript Cipher. It's your duty to decipher the code and uncover the hidden treasure, savvy?

<https://web-explorer.netlify.app>

Flag Submit

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">
        8185698384677978123875166955188076488251829549839552875183487751125
    </div>
    <div class="displaynone">
        NOTE: Flag contains only capital 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.

<form name="main" action="http://www.w3schools.com/tryit.asp?filename=tryhtml_iframe" target="mainframe">

CodePen: Unlock all of CodePen X

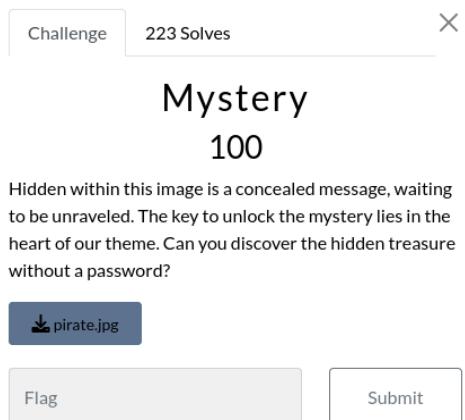
Decoder Input Decode

Output: QUESTCON{W3B_3XPL0R3R_1S_4W3S0M3}

Reset

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.

```
(fluffy㉿ben)-[~/milestone/questcon/Stego]
$ steghide --info pirate.jpg
"pirate.jpg":
  format: jpeg
  capacity: 18.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
embedded file "mystery":
  size: 16.8 KB
  encrypted: rijndael-128, cbc
  compressed: yes
Steghide
(Fluffy㉿ben)-[~/milestone/questcon/Stego]
$ rm -rf mystery
wrote extracted data to "mystery"
(Fluffy㉿ben)-[~/milestone/questcon/Stego]
$ steghide extract -sf pirate.jpg
Enter passphrase:
wrote extracted data to "mystery".
(Fluffy㉿ben)-[~/milestone/questcon/Stego]
$ 
```

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

```

File Name : Hacking DB mystery
Directory : D4,D,ISO... text: eD333DUZ\ \ \ \ \
File Size : 17 kB text: "LDDDDDDDD"
File Modification Date/Time : 2023:10:29 21:56:08+06:30
File Access Date/Time : 2023:10:29 21:56:07+06:30
File Inode Change Date/Time : 2023:10:29 21:56:08+06:30
File Permissions : -RW-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Exif Byte Order : Big-endian (Motorola, MM)
Processing Software : Hacker
Make : Alert
Camera Model Name : Alert
Exif Version : 0230
Components Configuration : Y, Cb, Cr, -
Flashpix Version : 0100
Image Unique ID : UVVFU1RDT057TXk1dDNyeV8xc180dzNzMG1lIX0=
Image Width : 360
Image Height : 360
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 1
Image Size : 360x360
Megapixels : 0.130
Reading: /app/uploads/f7f84710d77ce3af95b9a0852
Extracting storable bits: 366199 bits
Steg retrieved: seed: 61385, len: 19164

[fluffy@ben]~/.milestone/questcon/Stego]
$ echo "UVVFU1RDT057TXk1dDNyeV8xc180dzNzMG1lIX0=" | base64 -d
QUESTCON{My5t3ry_is_4w3s0me!}

[fluffy@ben]~/.milestone/questcon/Stego]
$ 

```

Mystery 2.0

Challenge

185 Solves

X

Mystery 2.0

100

Another mystery!

► View Hint

 another_m...

Flag

Submit

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

```
-(fluffy㉿ben)-[~/milestone/questcon/Stego/Mystery2.0] $ zsteg another_mystery.png
1,g,lsb,xy      .. file: OpenPGP Public Key
1,abgr,msb,xy   .. text: "}wwwwww;" -> scoreboard
2,r,lsb,xy      .. text: "Y?*[*LKB"
2,g,lsb,xy      .. text: "EAUUUUUUUU"
2,b,msb,xy      .. text: "jUUv}VU}%c"
2,rgba,lsb,xy  .. text: "QUESTCON{PiraT3s_Ar3_M7s!3rY}\n"
2,abgr,msb,xy   .. text: "KKKG000"
3,rgb,lsb,xy    .. file: PGP Secret Sub-key -
3,rgba,lsb,xy   .. file: PGP Secret Sub-key -
4,r,msb,xy      .. text: ";3333333{"
4,g,lsb,xy      .. text: "eDVeffffvfy"
4,g,msb,xy      .. text: "fffffffnnfff"
4,b,lsb,xy      .. text: "xweUgeeUwveUVx"
4,b,msb,xy      .. text: "=33333333"
4,rgb,lsb,xy    .. text: "bw%cEDcE"
4,bgr,lsb,xy   .. text: "re%CdECT"
4,rgba,lsb,xy  .. text: "%o4_Do4_"

Challenge 185 Solves
Mystery 2.0
100
Another mystery!
▶ View Hint
Download another_m...
```

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