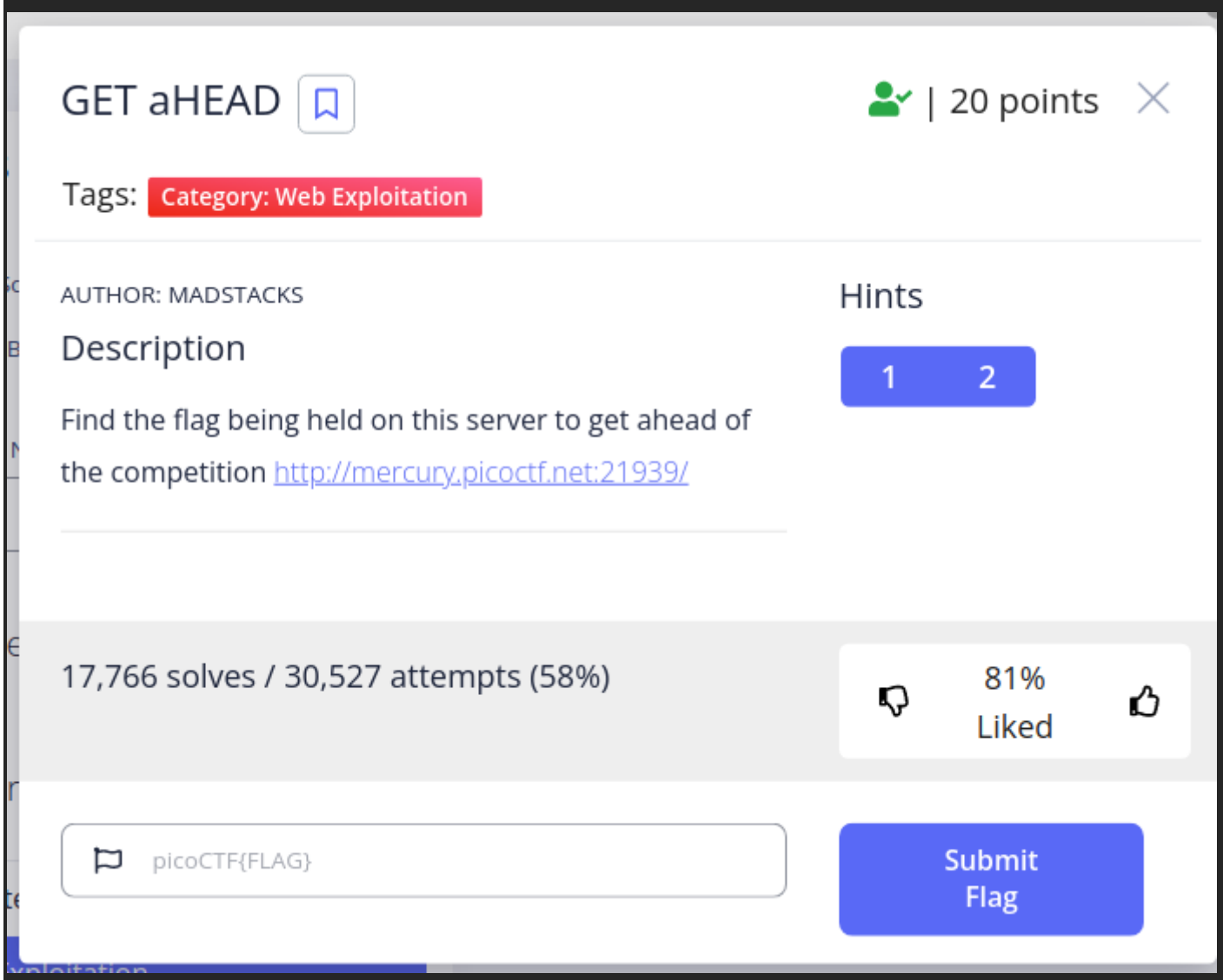
# picoCTF_WebExploration

Skills Learned:

- Burp Suite (Request Header Manipulation, Cookies, METHODS)
- web enumeration (dirsearch)
- html, css, .js
- /robots.txt, /.DS_Store
- md5 collisons
- cookie encryption

Skills Needed:

- Web Assembly/Debugging
- How to break cookie encryptionencrytion



```
10 Connection: close
11 Referer: http://mercury.picoctf.net:21939/index.php?
12 Upgrade-Insecure-Requests: 1
13
14
```

Search... 0 matches

```
otstrap.min.css">
10  <style>
      body{
        background-color:blue;
      }
    </style>
11 </head>
12 <body>
13   <div class="container">
14     <div class="row">
15       <div class="col-md-6">
16         <div class="panel panel-primary" style="
           margin-top:50px">
17           <div class="panel-heading">
```

Search... 0 matches

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Us

1 × ...

Send Cancel < > Target: ht

changed "post" to "head"

Request

Pretty R Hex \n

```
1 HEAD /index.php HTTP/1.1
2 Host: mercury.picoctf.net:21939
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 0
9 Origin: http://mercury.picoctf.net:21939
10 Connection: close
11 Referer: http://mercury.picoctf.net:21939/index.php?
12 Upgrade-Insecure-Requests: 1
13
14
```

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4l1ty_6ef27873}
3 Content-type: text/html; charset=UTF-8
4
5
```

INS Rec Que Boc Rec Rec Res

Changing POST request to HEAD in the Repeter

Cookies | 40 points

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

## Description

Who doesn't love cookies? Try to figure out the best one.

http://mercury.picoctf.net:17781/

## Hints

(None)

13,311 solves / 22,356 attempts (60%)

58% Liked

picoCTF{FLAG}

Submit Flag

Cookies Home

Cookies Home

Welcome to my cookie search page. See how much I like different kinds of cookies!

snickerdoodle

Search

© PicoCTF

| # | Host | Method | URL |
|---|---|---|---|
| 68 | http://mercury.picoctf.net:17781 | GET | / |
| 69 | https://ajax.googleapis.com | GET | /ajax/libs/jquery/3.3.1/jquery.m |
| 70 | https://maxcdn.bootstrapcdn.com | GET | /bootstrap/3.3.7/js/bootstrap.m |
| 71 | http://mercury.picoctf.net:17781 | POST | /search |
| 72 | http://mercury.picoctf.net:17781 | GET | /check |

tried "chocolate chip"

Request

Pretty Raw Hex \n

```
1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:17781
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://mercury.picoctf.net:17781/
8 Connection: close
9 Cookie: name=1
10 Upgrade-Insecure-Requests: 1
11
12
```

Send Cancel

Request

Pretty Raw Hex \n

```
1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:17781
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://mercury.picoctf.net:17781/
8 Connection: close
9 Cookie: name=18
10 Upgrade-Insecure-Requests: 1
11
12
```

changing the value until

Response

Pretty Raw Hex Render

Cookies Home

Flag:

the flag pops

picoCTF{3v3ry1_t0v3s_c00k135_bb3b3535}

## Insp3ct0r

50 points

Tags: Category: Web Exploitation

AUTHOR: ZARATEC/DANNY

### Description

Kishor Balan tipped us off that the following code may need inspection:

https://jupiter.challenges.picoctf.org/problem/41511/ (link) or

http://jupiter.challenges.picoctf.org:41511

### Hints

1 2

40,924 solves / 109,152 attempts (37%)

86% Liked

picoCTF{FLAG}

Submit Flag

## Inspect Me

What | How

**How**

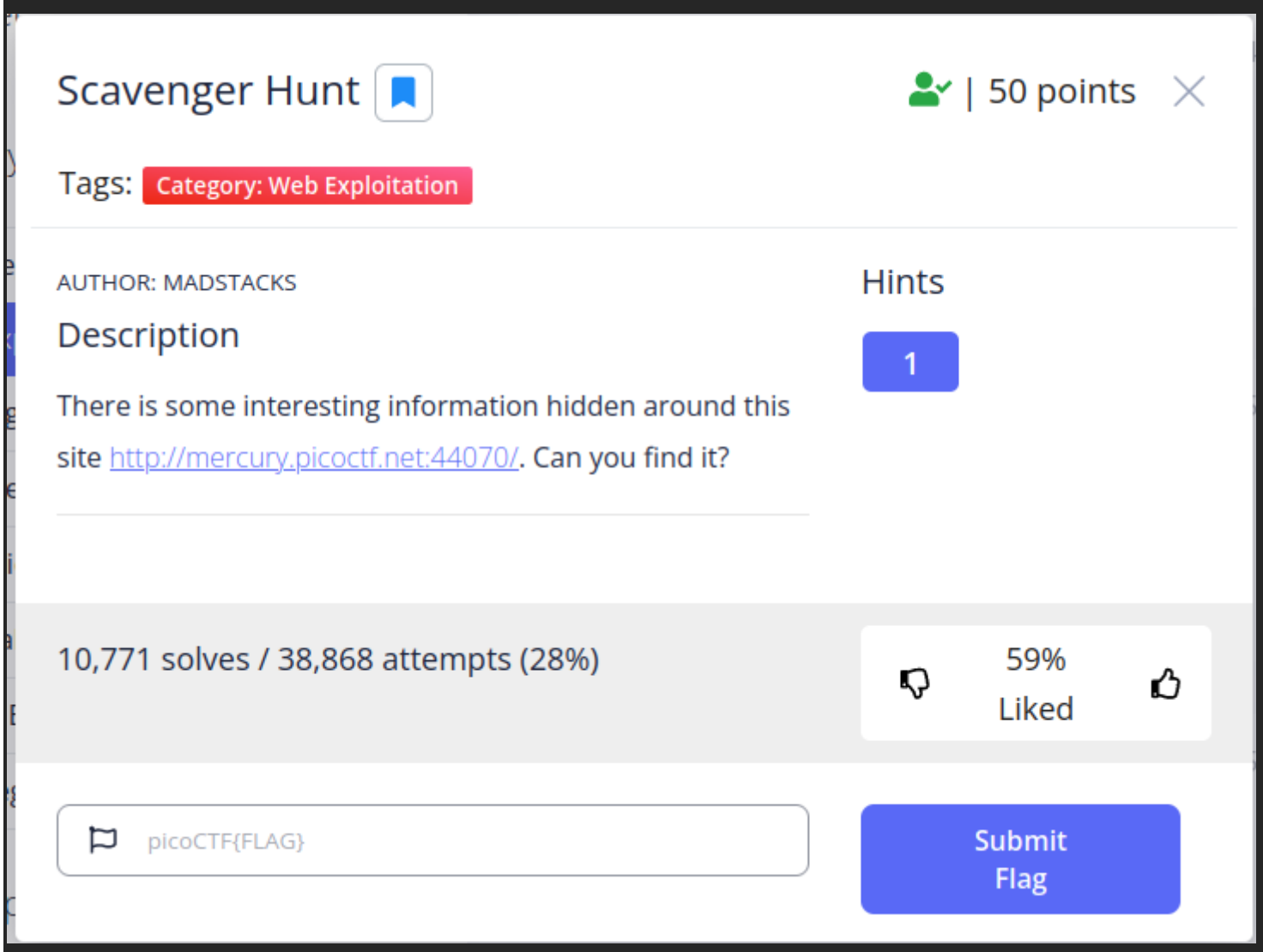
I used these to make this site:
HTML
CSS
JS (JavaScript)

```
DOCTYPE html>
tml> event
head>
 <title>My First Website :)</title>
 <link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
 <link rel="stylesheet" type="text/css" href="mycss.css">
 <script type="application/javascript" src="myjs.js"></script>
/head>
body>
▼<div class="container">
 ▶<header>…</header>
  <button id="defaultOpen" class="tablink" onclick="openTab('tabintro', this, '#222')" style=
  <button class="tablink" onclick="openTab('tababout', this, '#222')" style="background-color
 ▶<div id="tabintro" class="tabcontent" style="display: none;">…</div>
 ▼<div id="tababout" class="tabcontent" style="display: block;">
    <h3>How</h3>
   ▶<p>…</p>
    <!--Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3-->
  </div>
 </div>
/body>
tml>
```

```
}

.tabcontent {
    color: #111;
    display: none;
    padding: 50px;
    text-align: center;
}

#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }

/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```

```
}

window.onload = function() {
    openTab('tabintro', this, '#222');
}

/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?832b0699} */
```

Three-part flag found in the html, css, javascript




In the html

```
  JS (JavaScript)
</p>
<!--Here's the first part of the flag: picoCTF{t-->
</div>
```

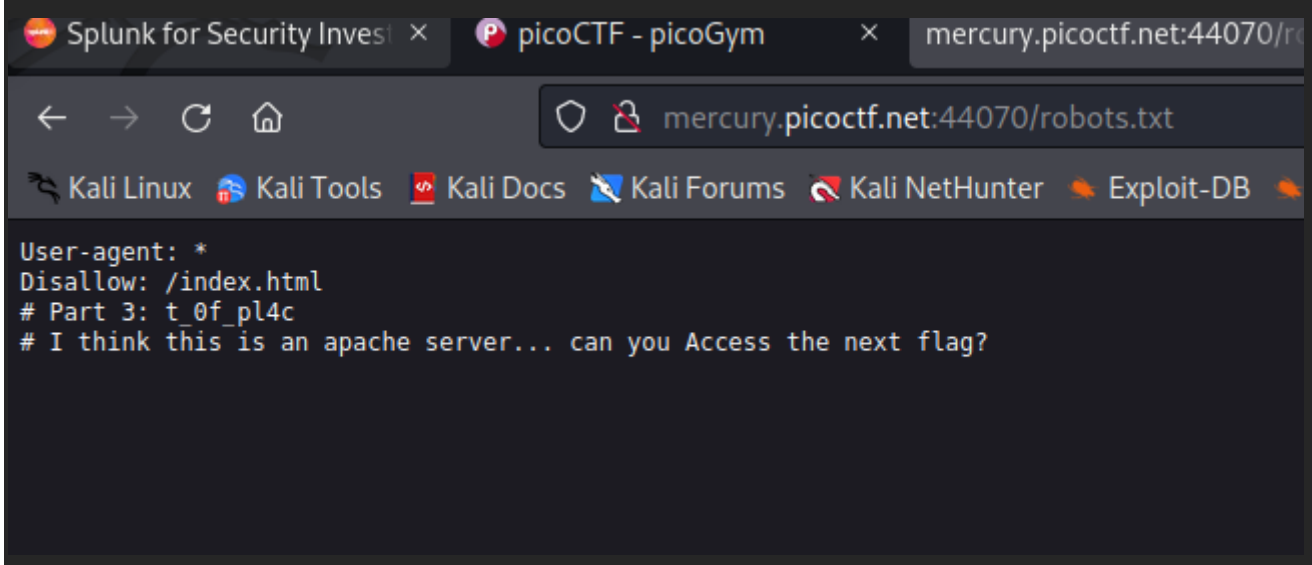
in the css

```
.tabcontent {
    color: #111;
    display: none;
    padding: 50px;
```

```
45      text-align: center;
46  }
47
48  #tabintro { background-color: #ccc; }
49  #tababout { background-color: #ccc; }
50
51  /* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0 */
```

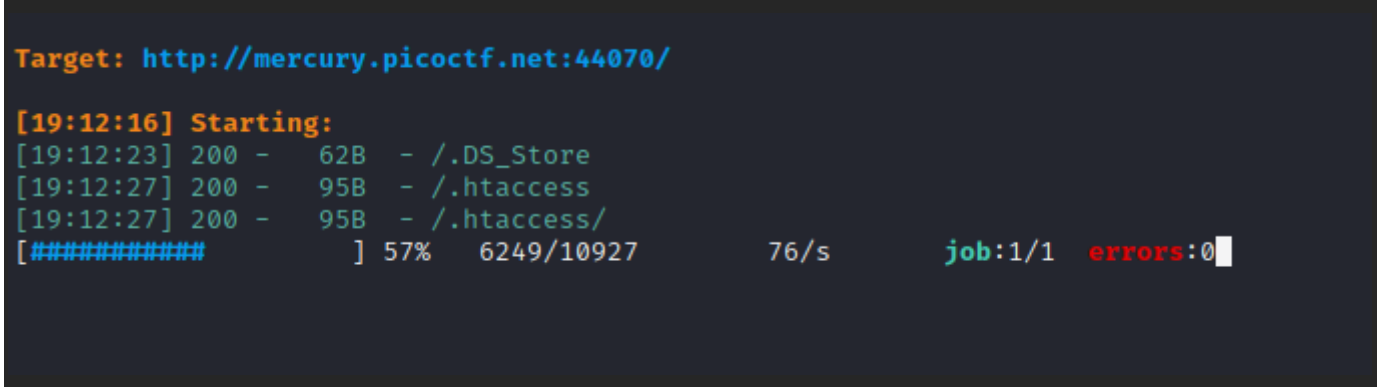
in the javascrript


/robots.txt



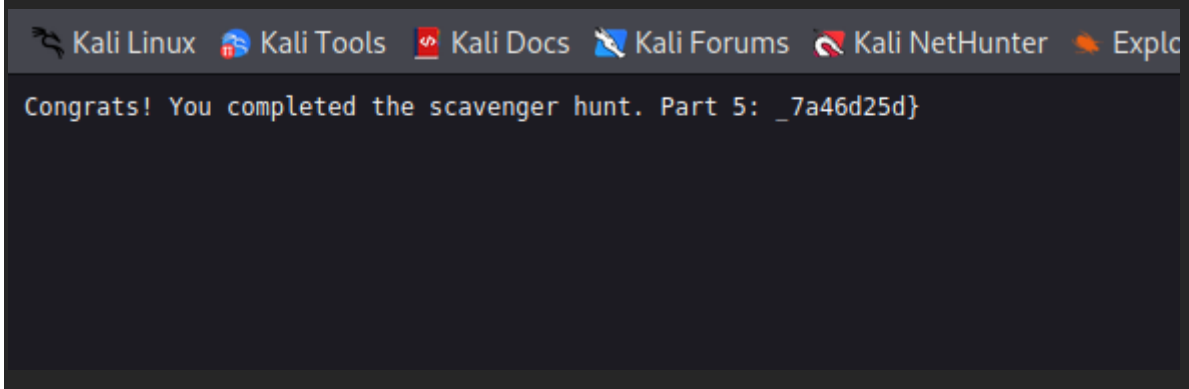

At the point:

dirsearch -u http://mercury.picoctf.net:44070/




found part 5 before 4

/.DS_Store




./htaccess

```
# Part 4: 3s_2_l00k
# I love making websites on my Mac, I can Store a lot of information there.
```

## Some Assembly Required 1

| 70 points

Tags: Category: Web Exploitation

AUTHOR: SEARS SCHULZ

### Description

http://mercury.picoctf.net:55336/index.html

### Hints

(None)

6,449 solves / 8,878 attempts (73%)

65% Liked

picoCTF{FLAG}

Submit Flag

mercury.picoctf.net:55336/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DE

**Enter flag:**

Submit

Looking at html reveals .js

```
<html>
<head>
  <meta charset="UTF-8">
  <script src="G82XCw5CX3.js"></script>
</head>
<body>
  <h4>Enter flag:</h4>
  <input id="input" type="text">
  whitespace
  <button onclick="onButtonPress()">Submit</button> event
  <p id="result">Incorrect!</p>
</body>
</html>
```

.js ~~shows us a hidden directory~~ brings us to a file

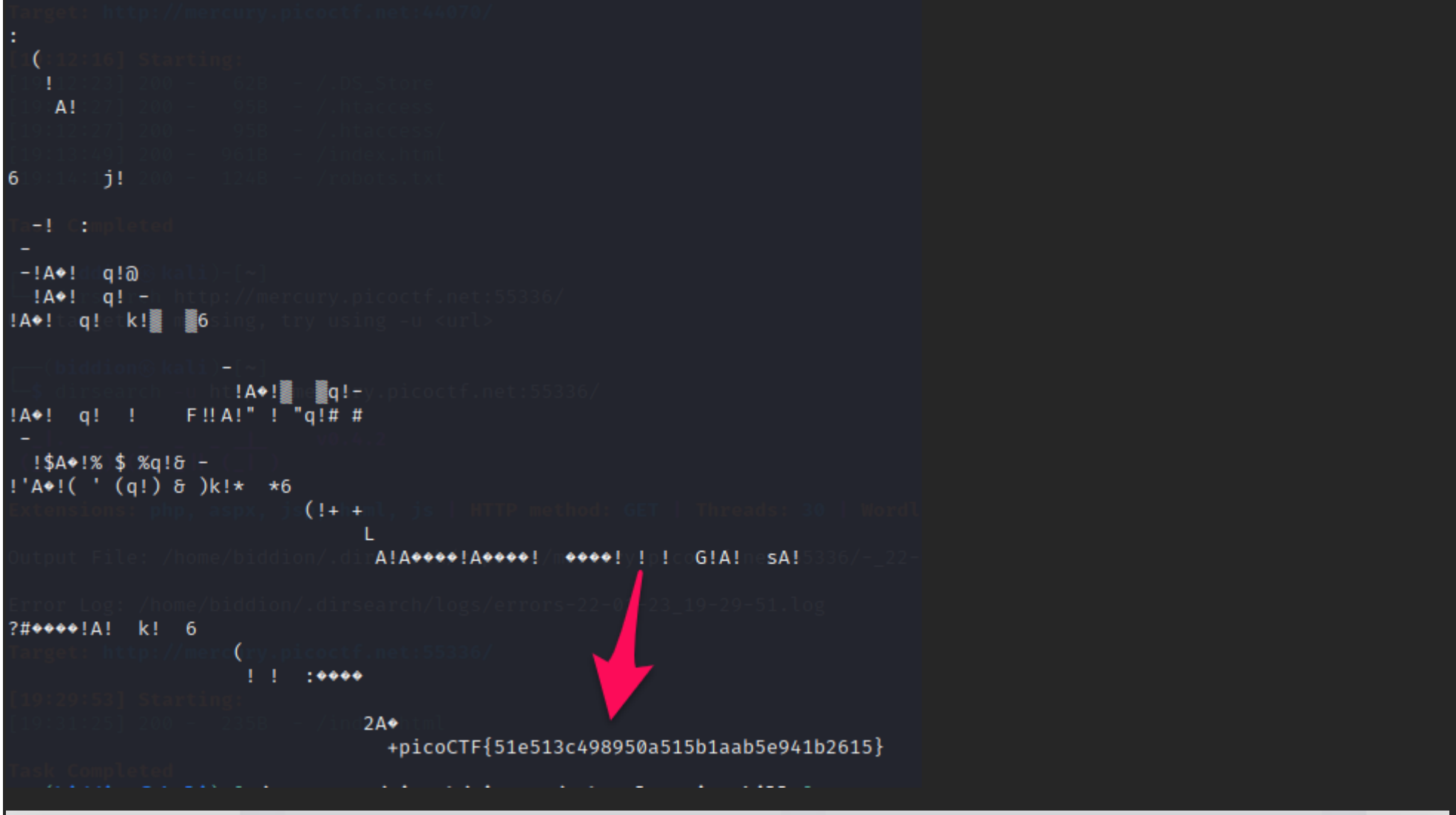
Network Style Editor Performance Memory Storage Accessibility Application

G82XCw5CX3.js

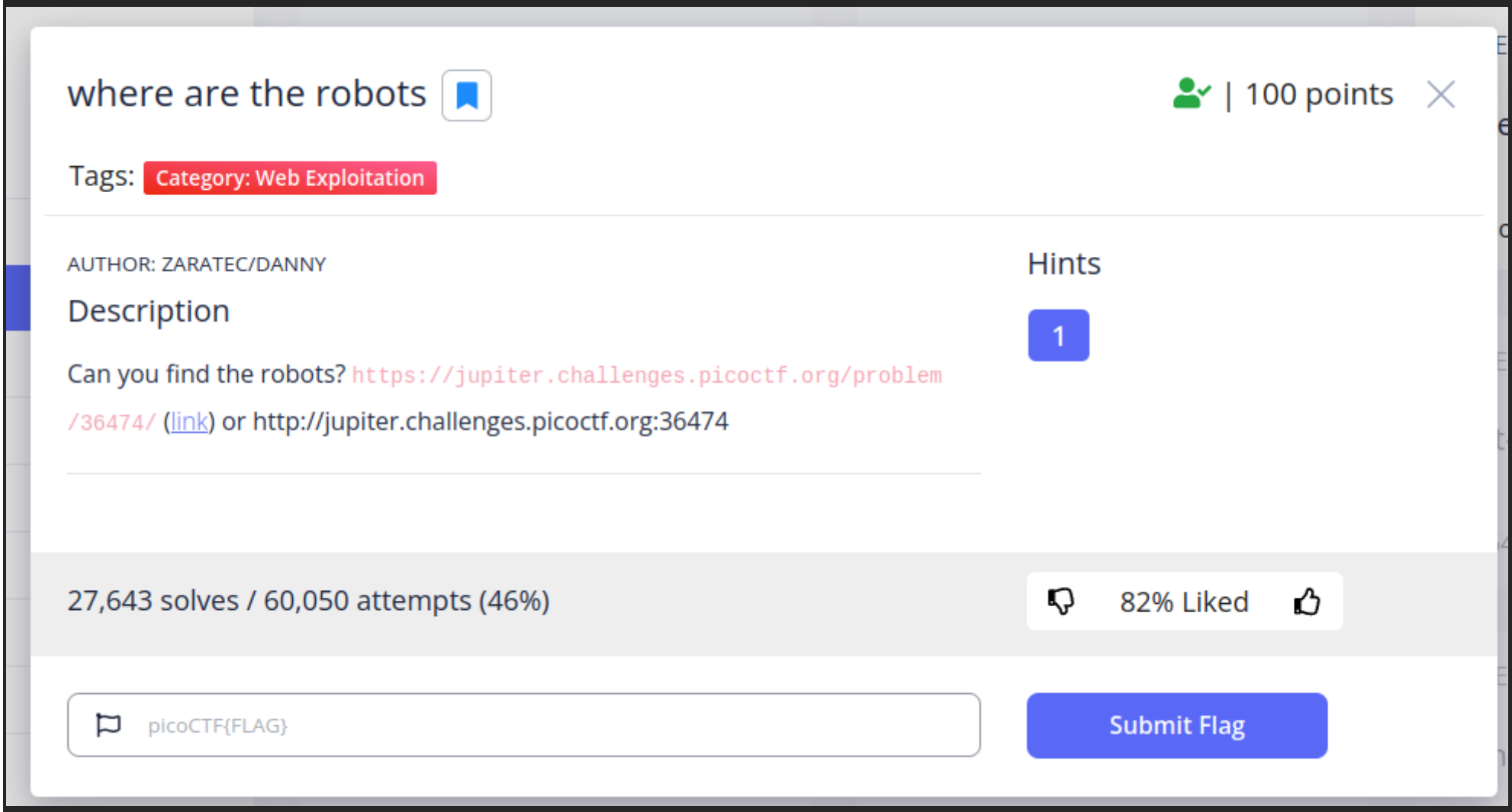
```
1 rHTML','1195047NznhZg','1qfevql','input','1699808QuoWhA','Correct!','check_flag','Incorrect!','./JIFxzHyW8W','23SMpAuA'
```

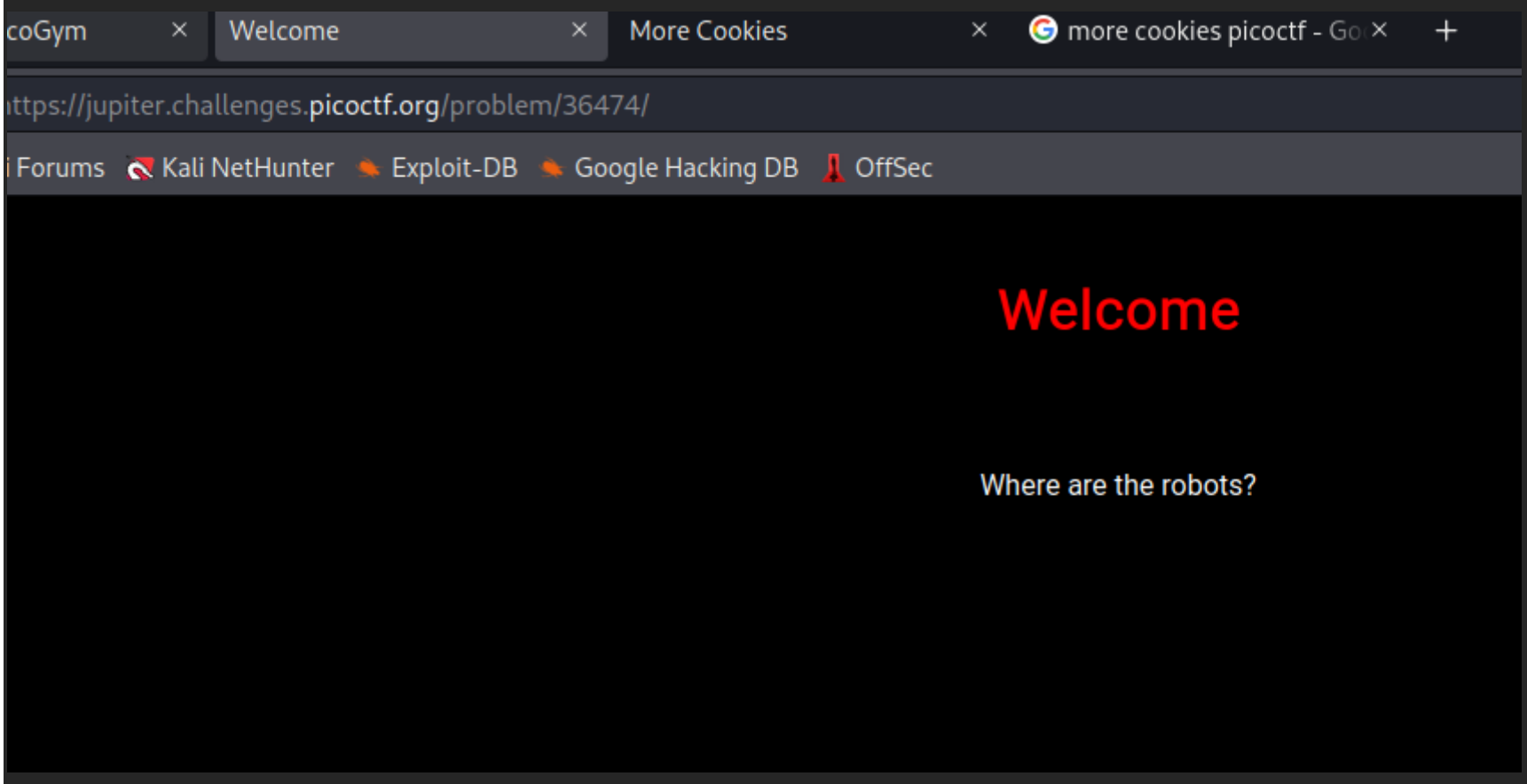
Which has the flag

```
┌──(biddion㉿kali)-[~/Documents/GitHub/picoCTF/WebExplorationSkills]
└─$ cat JIFxzHyW8W
asm````pA◆◆
          A◆
           A◆
            A◆

A◆
 A◆◆
    A
     A
      ◆
       memory__wasm_call_ctorsstrcmp
check_flaginput copy_char
                        __dso_handle
__global_base
__memory_base__heap_base
                __table_base
◆
◆◆#◆◆◆◆!A !  k!  6   6 (   !  6 (!  6
                                  @@ (!A j!           6 -!

:
  (
   !
    A!

6     j!

  -! :
 -
 -!A◆!  q!@
  !A◆!  q! -
!A◆!  q!  k!   6

                 -
                  !A◆!    q!-
!A◆!  q!  !    F!!A!" ! "q!# #
 -
  !$A◆!% $ %q!& -
!'A◆!( ' (q!) & )k!*  *6
                          (!+ +
                               L
                                A!A◆◆◆◆!A◆◆◆◆!  ◆◆◆◆! ! !  G!A!  sA!

?#◆◆◆◆!A!  k!  6
                    (
                     ! !  :◆◆◆◆

                                2A◆
                                  +picoCTF{51e513c498950a515b1aab5e941b2615}
```



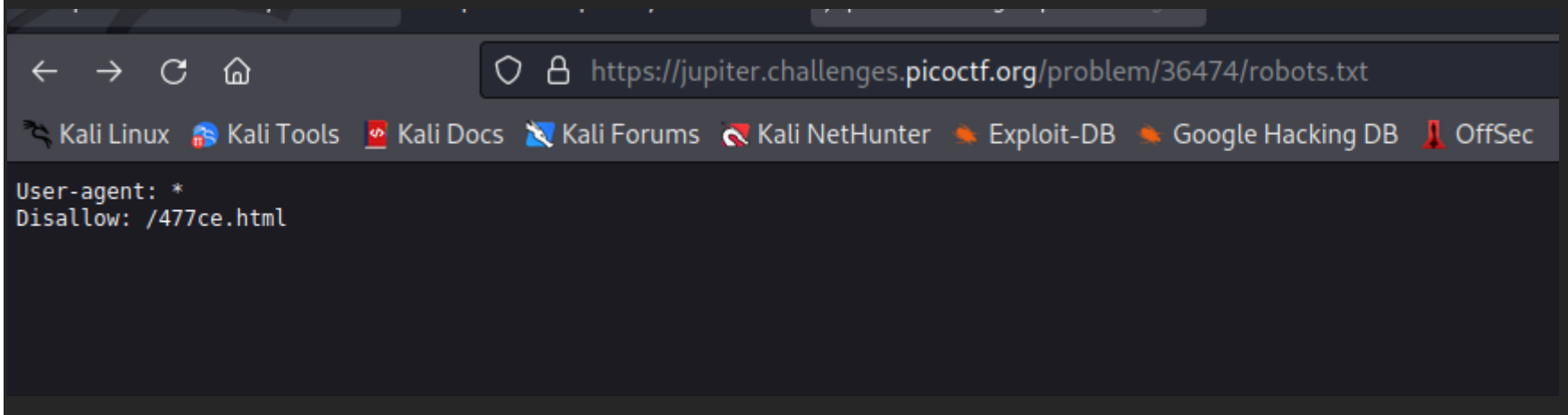
Too Hard; can't do!




This is just following bread crumbs

/robots.txt




/477ce.html

Guess you found the robots
picoCTF{ca1cu1at1ng_Mach1n3s_477ce}

logon | 100 points

Tags: Category: Web Exploitation

AUTHOR: BOBSON

## Description

The factory is hiding things from all of its users. Can you login as Joe and find what they've been looking at? https://jupiter.challenges.picoctf.org/problem/13594/ (link) or http://jupiter.challenges.picoctf.org:13594

Hints

1

19,346 solves / 27,367 attempts (71%)

87% Liked

picoCTF{FLAG}

Submit Flag

CTF - picoGym | Factory Login | jupiter.challenges.picoctf.org | More Cookies | more cookies picoctf - Go

https://jupiter.challenges.picoctf.org/problem/13594/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Factory Login

Home Sign Out

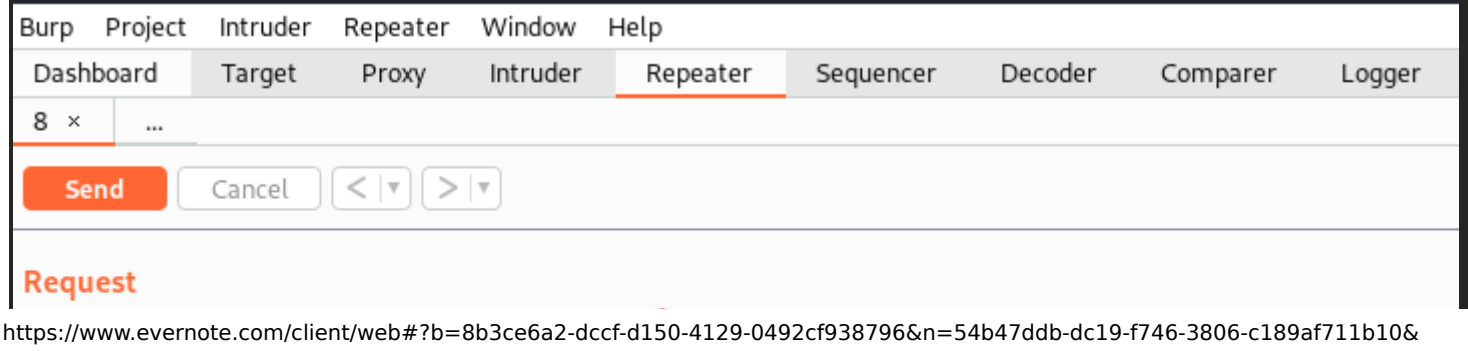
Username

Password

Sign In

© PicoCTF 2019

I tired just changing the value from 'false' to 'true'



```
Pretty Raw Hex \n
1 GET /problem/13594/flag HTTP/1
2 Host: jupiter.challenges.pi    f.org
3 Cookie: _ga=GA1.2.11600198    1642929874; _gid=GA1.2.222856668.1642929874; password=dave;
  username=joe; admin=False
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://jupiter.challenges.picoctf.org/problem/13594/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

8 × ...

Send Cancel < > Targ

**Request**

Pretty Raw Hex \n

```
1 GET /problem/13594/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga=GA1.2.1160019831.1642929874; _gid=GA1.2.222856668.1642929874; password=dave;
  username=joe; admin=True
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: text/html,applica    /xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en
7 Accept-Encoding: gzip, de
8 Referer: https://jupiter.c    es.picoctf.org/problem/13594/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

**Response**

Pretty Raw Hex Render \n

Factory Login

Home Sign Out

**Flag**:

picoCTF{th3_c0nsp1r4cy_l1v3s_d1c24fef}

© PicoCTF 2019

Success!!!

dont-use-client-side | 100 points

Tags: Category: Web Exploitation

AUTHOR: ALEX FULTON/DANNY

Description

Can you break into this super secure portal?

https://jupiter.challenges.picoctf.org/problem/37821/ (link) or

http://jupiter.challenges.picoctf.org:37821

Hints

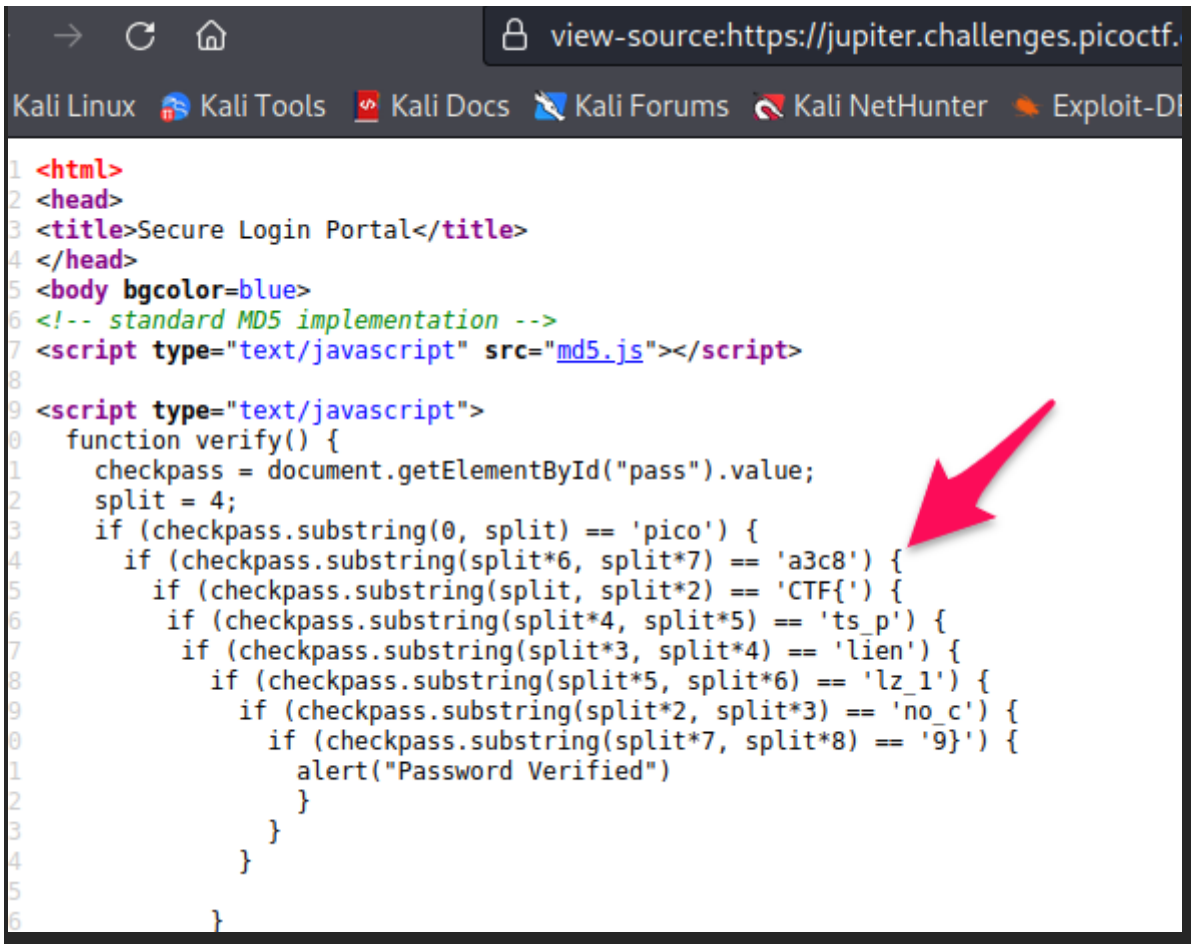
1

19,897 solves / 37,995 attempts (52%)

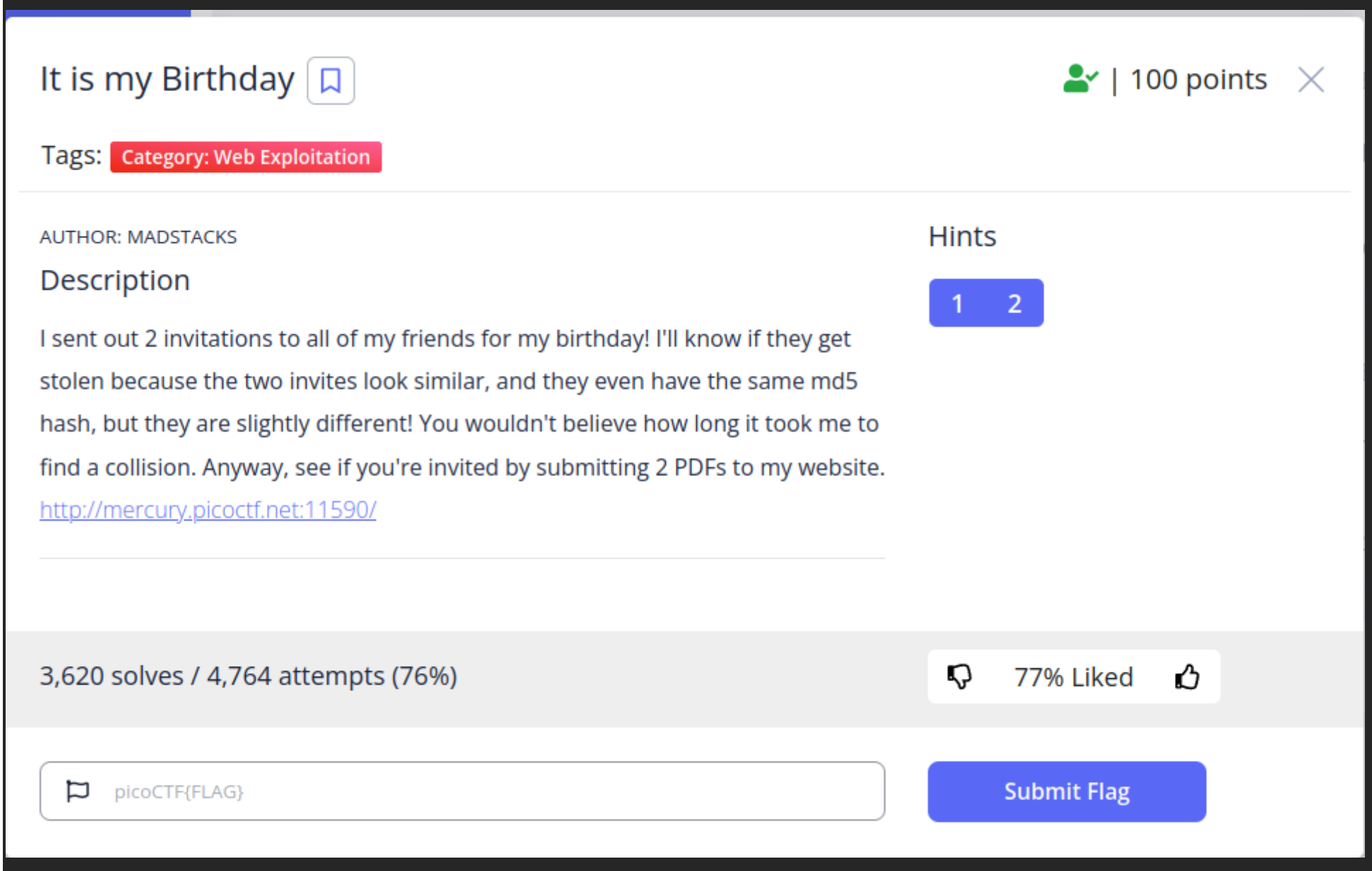
88% Liked

picoCTF{FLAG}

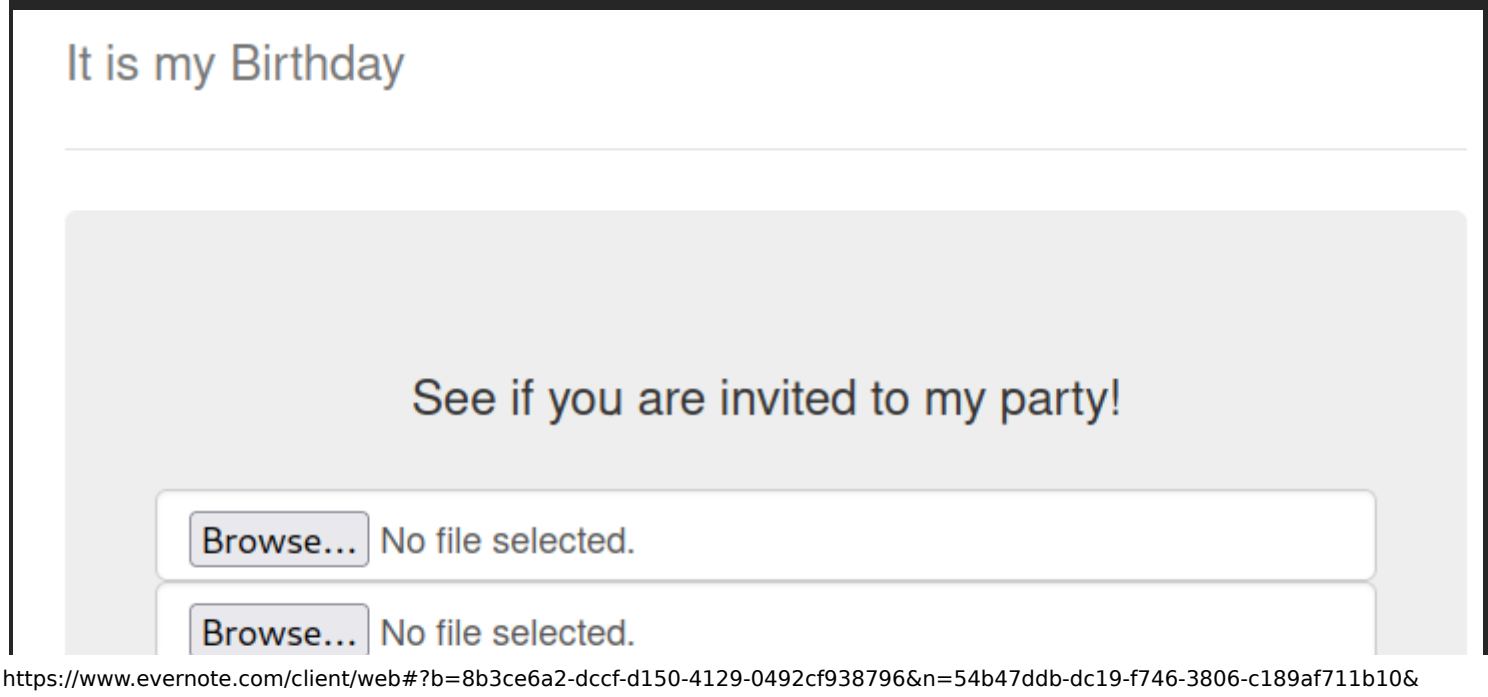
Submit Flag

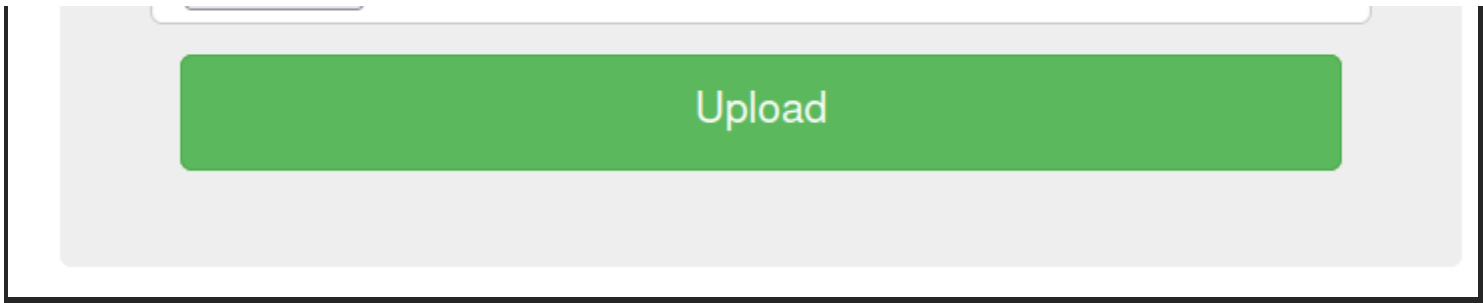



Viewing the code, the flag is in javascript, broken in the clear. I don't know how to write a script that will piece it together but my two eyes do work.

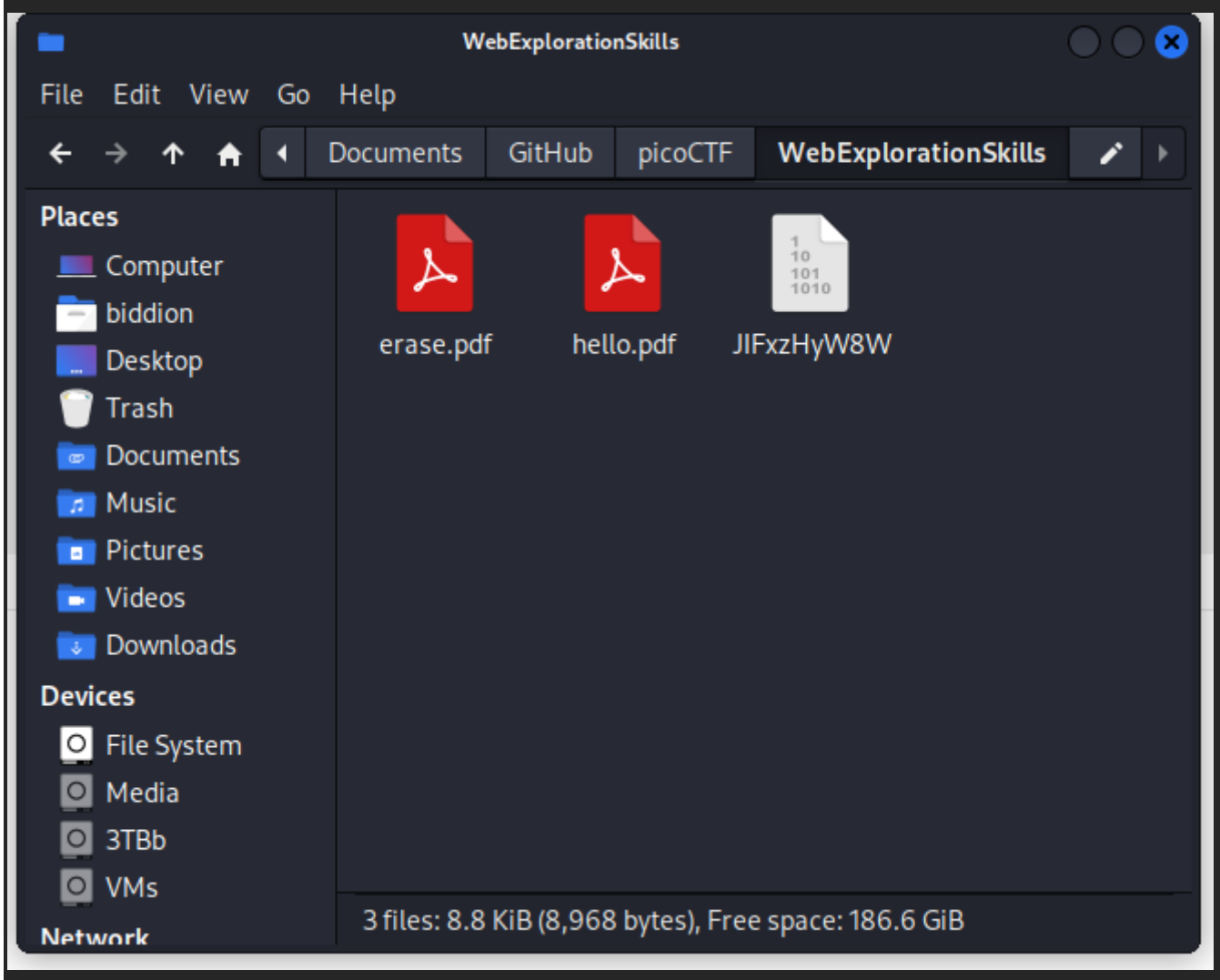



This task involves a collision of two md5 encoded files

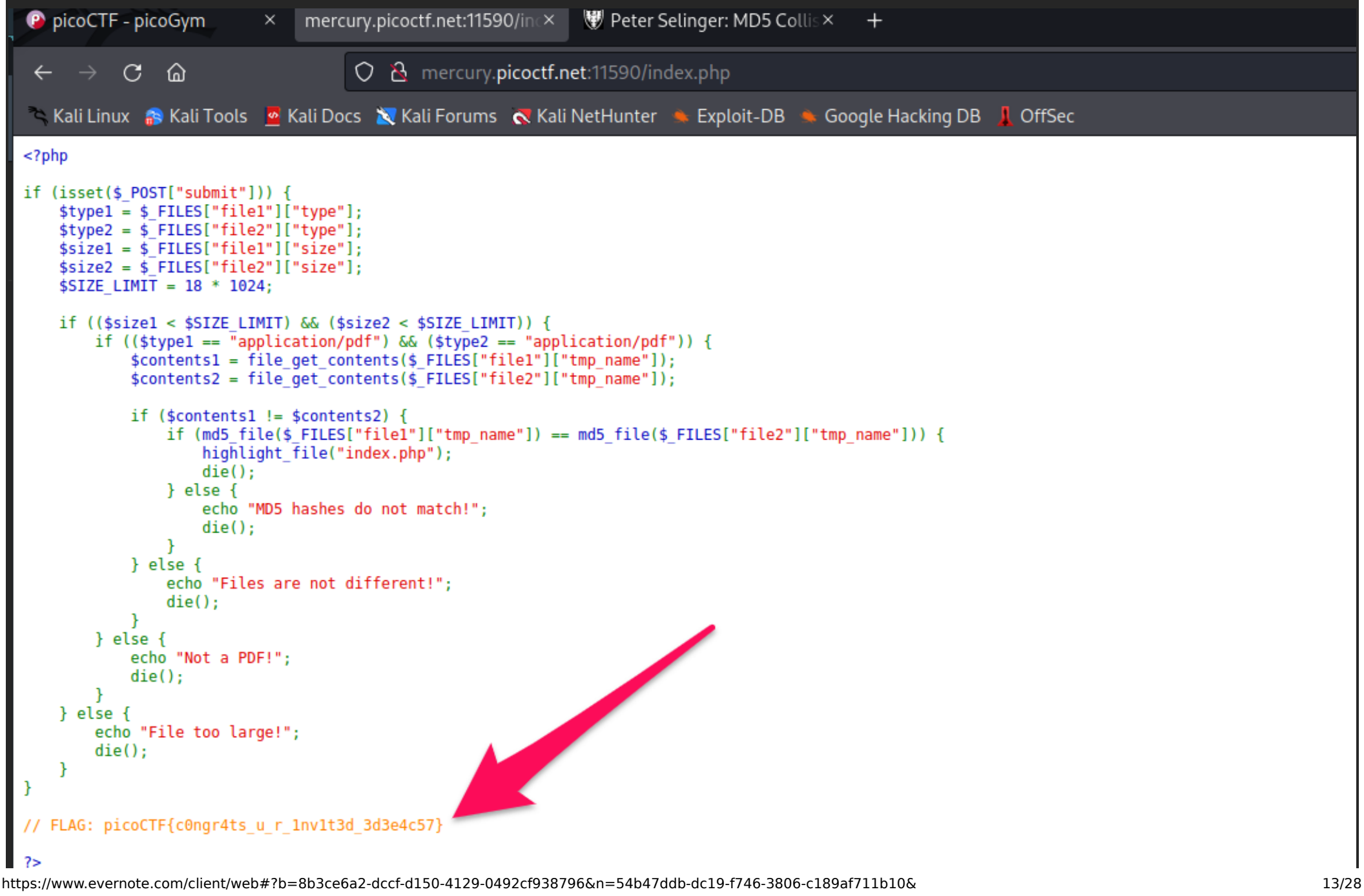





Found this: https://www.mscs.dal.ca/~selinger/md5collision/
Downloaded two files with collisions



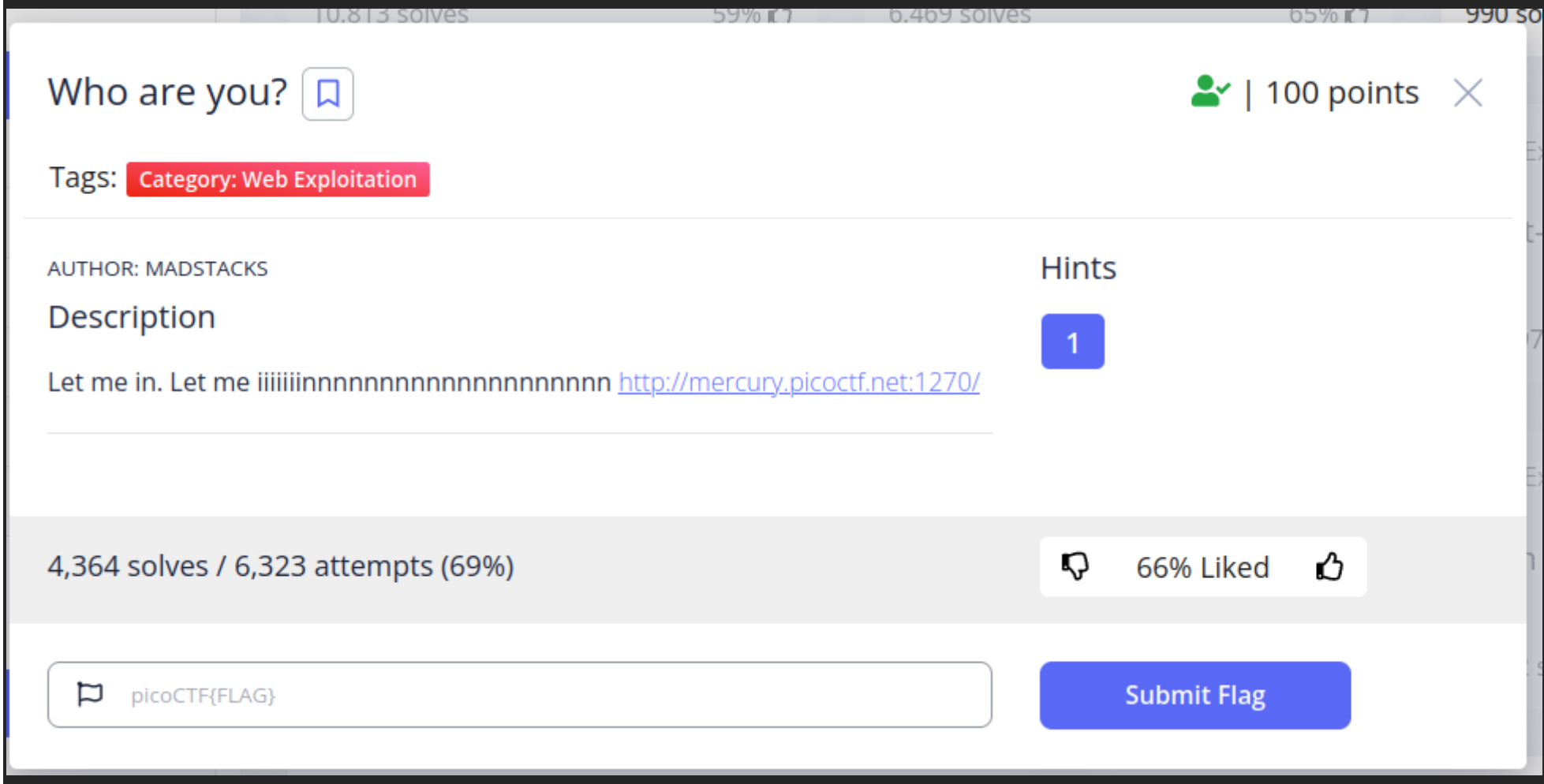

I had to rename the files with .pdf




```php
<?php

if (isset($_POST["submit"])) {
    $type1 = $_FILES["file1"]["type"];
    $type2 = $_FILES["file2"]["type"];
    $size1 = $_FILES["file1"]["size"];
    $size2 = $_FILES["file2"]["size"];
    $SIZE_LIMIT = 18 * 1024;

    if (($size1 < $SIZE_LIMIT) && ($size2 < $SIZE_LIMIT)) {
        if (($type1 == "application/pdf") && ($type2 == "application/pdf")) {
            $contents1 = file_get_contents($_FILES["file1"]["tmp_name"]);
            $contents2 = file_get_contents($_FILES["file2"]["tmp_name"]);

            if ($contents1 != $contents2) {
                if (md5_file($_FILES["file1"]["tmp_name"]) == md5_file($_FILES["file2"]["tmp_name"])) {
                    highlight_file("index.php");
                    die();
                } else {
                    echo "MD5 hashes do not match!";
                    die();
                }
            } else {
                echo "Files are not different!";
                die();
            }
        } else {
            echo "Not a PDF!";
            die();
        }
    } else {
        echo "File too large!";
        die();
    }
}

// FLAG: picoCTF{c0ngr4ts_u_r_1nv1t3d_3d3e4c57}

?>
```

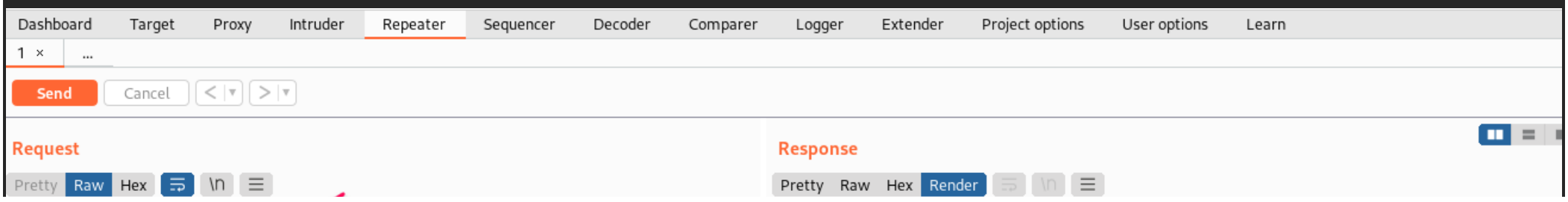
```
<!DOCTYPE html>
<html lang="en">
```

Invitation recieved!




Is "iiiiiiinnnnnnnnnnnnnnnnnnn" a clue?


Hmm. This looks like a job for Burp.



```
GET / HTTP/1.1
Host: mercury.picoctf.net:[illegible]70
User-Agent: PicoBrowser
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


This kid is already getting on my nerves!!!
I think I need a list of request header types
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers
Even better
https://kapeli.com/cheat_sheets/HTTP_Header_Fields.docset/Contents/Resources/Documents/index

HTTP Header Fields Cheat Sheet - Kap… 230 kB

Request

Pretty Raw Hex \n

```
GET / HTTP/1.1
Host: mercury.picoctf.net:1270
Referer: http://mercury.picoctf.net:1270
User-Agent: PicoBrowser
Accept:
text/html,application/xhtml+xml,applic[illegible]n/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Pretty Raw Hex Render


Just "mercury.picoctf.net" didn't work so I had to actually complete the socket

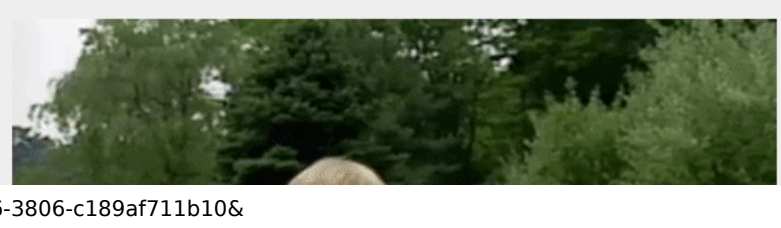
Request

Pretty Raw Hex \n

```
GET / HTTP/1.1
Host: mercury.picoctf.net:1270
Referer: http://mercury.picoctf.net:127[illegible]
Date: Thu, 15 Dec 2018 00:00:00 GMT
User-Agent: PicoBrowser
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Pretty Raw Hex Render

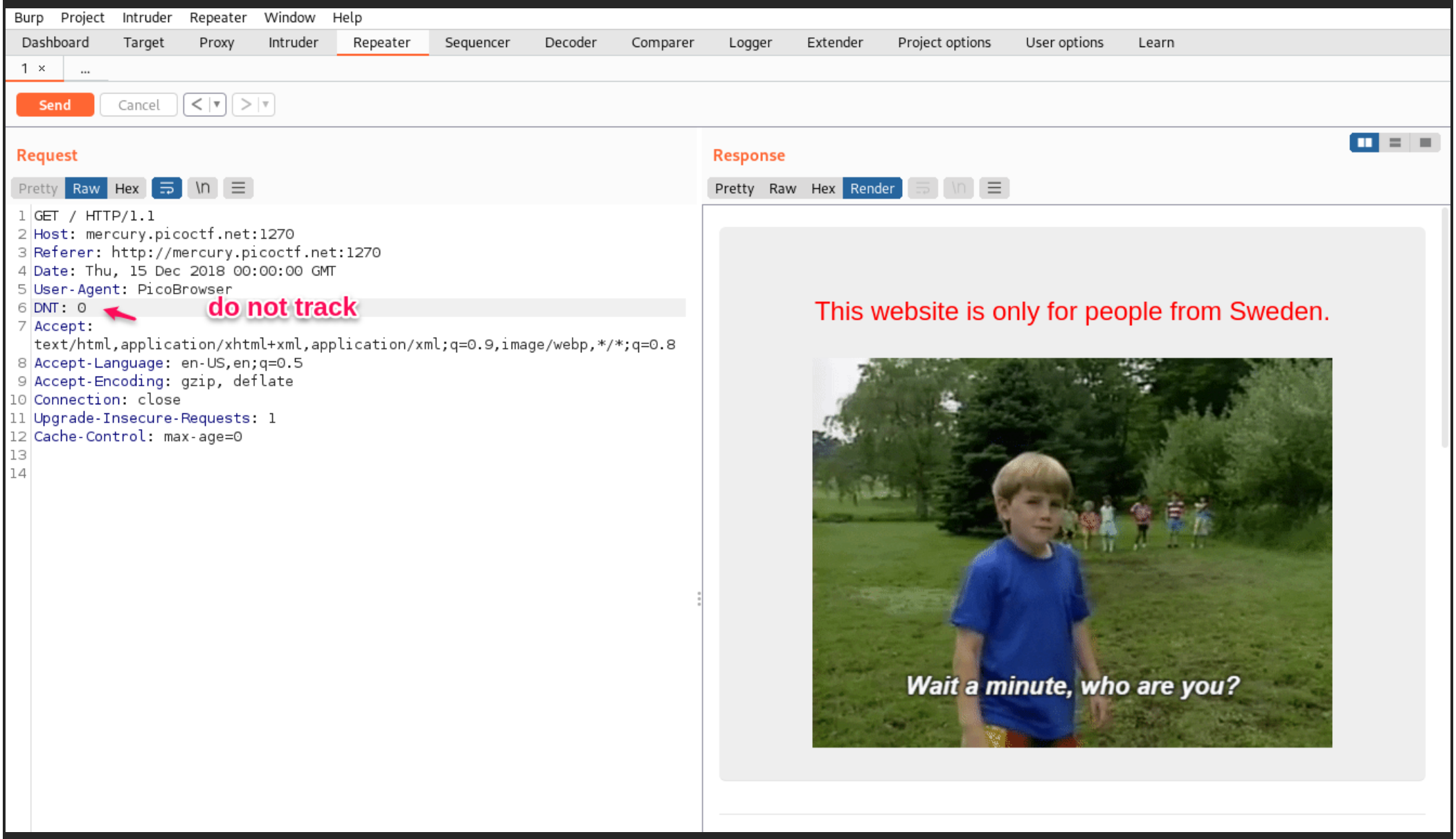



Do not track

https://www.geeksforgeeks.org/http-headers-dnt/

**Syntax:**

```
DNT:0
DNT:1
```




I tried "location" and "origin"; finally, I googled "request header change senders ipaddress"

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-For

15


Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × ...

Send Cancel

**Request**

Pretty Raw Hex \n

```
1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:1270
3 Referer: http://mercury.picoctf.net:1270
4 Date: Thu, 15 Dec 2018 00:00:00 GMT
5 User-Agent: PicoBrowser
6 DNT: 0
7 X-Forwarded-For: 85.226.200.210
8 Accept-Language: sv
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
10 Accept-Language: en-US,en;q=0.5
11 Accept-Encoding: gzip, deflate
12 Connection: close
13 Upgrade-Insecure-Requests: 1
14 Cache-Control: max-age=0
15
16
```

For all my peeps who speak "Svedish"

**Response**

Pretty Raw Hex Render \n

What can I say except, you are welcome

picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_f56f58a5}

© PicoCTF

Apparently, not 'sw' but 'sv'

login | 100 points

Tags: Category: Web Exploitation

AUTHOR: BROWNIEINMOTION

## Description

My dog-sitter's brother made this website but I can't get in; can you help?

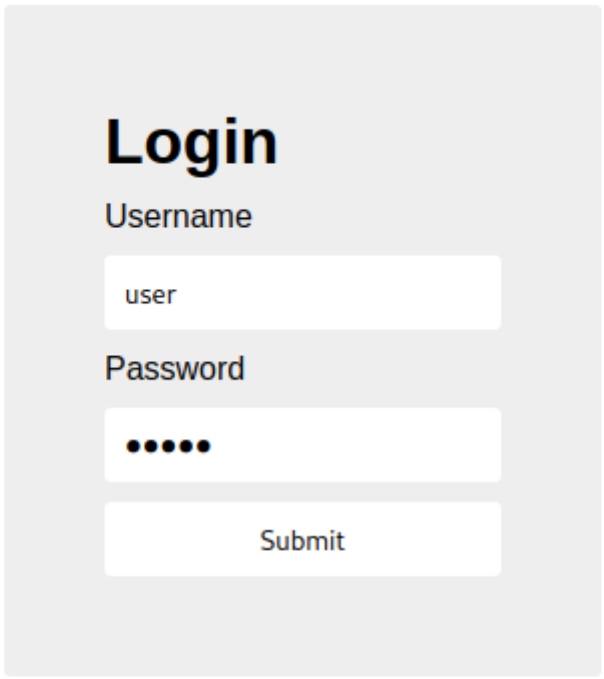
login.mars.picoctf.net

## Hints

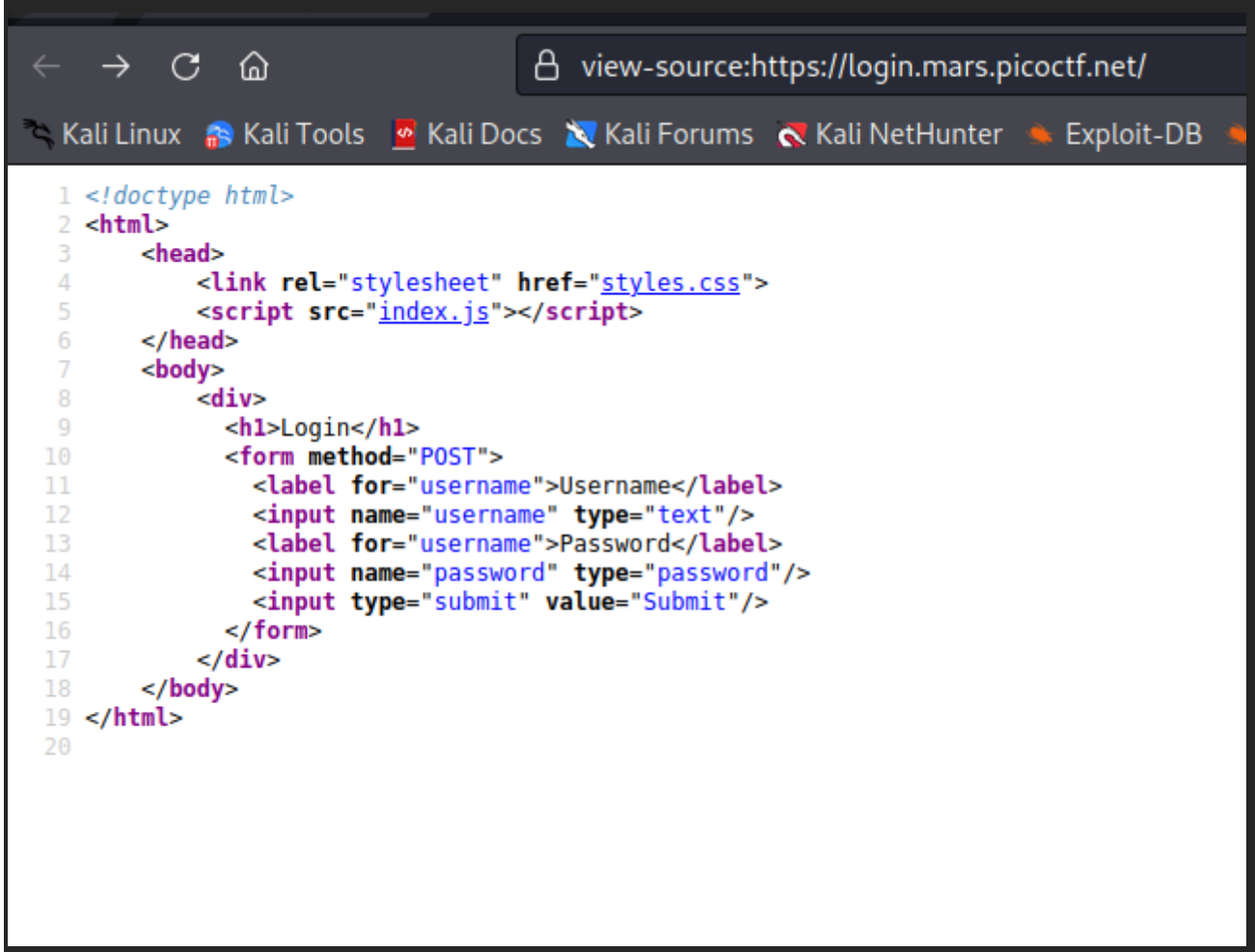
(None)

6,312 solves / 9,809 attempts (64%) 86% Liked

picoCTF{FLAG} Submit Flag




I have Burp Suite open and tried random login but nothing was sent the burp.

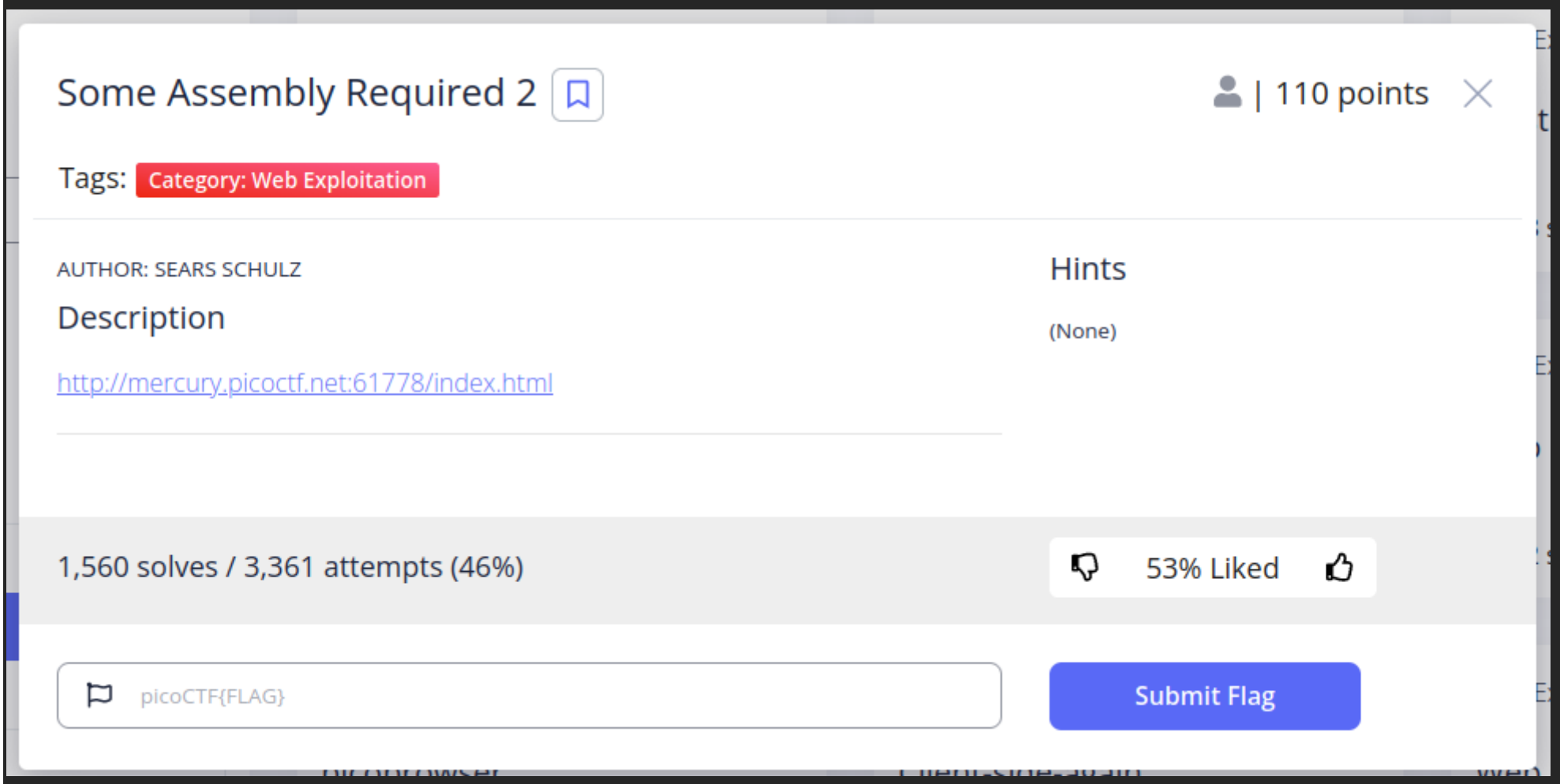


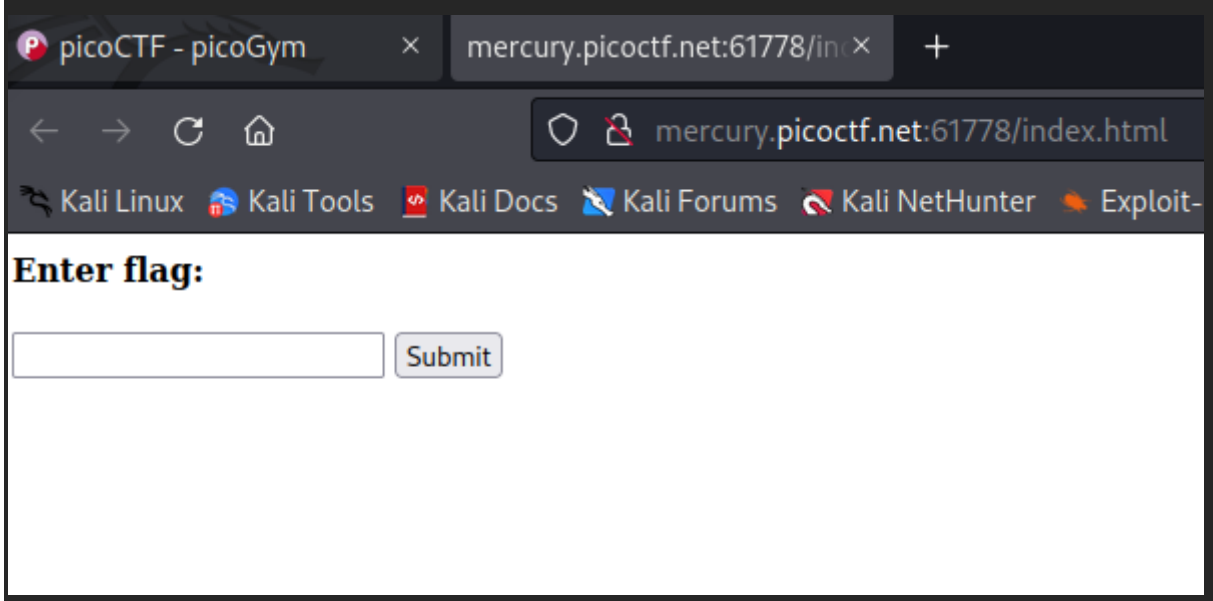

looking at html i see a .js
clicking .js reveal the following

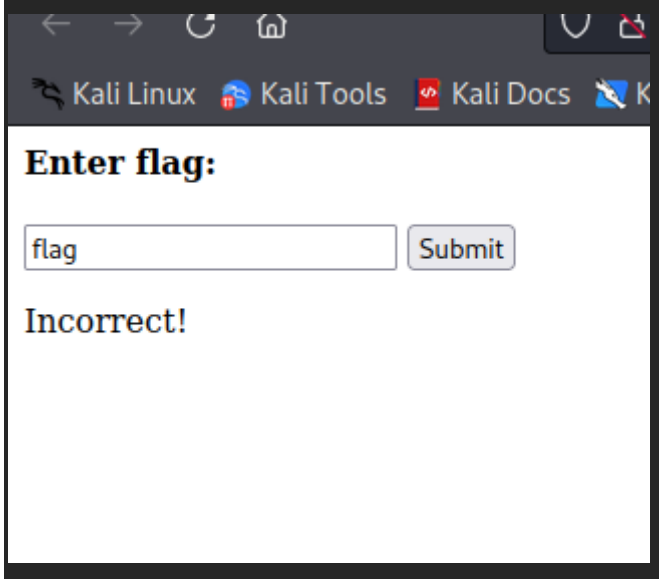
```
(async()=>{await new Promise((e=>window.addEventListener("load",e))),document.querySelector("form").addEventListener("submit",(e=>
{e.preventDefault();const r={u:"input[name=username]",p:"input[name=password]"},t={};for(const e in
r)t[e]=btoa(document.querySelector(r[e]).value).replace(/=/g,"");return"YWRtaW4"!==t.u?alert("Incorrect
Username"):"cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ"!==t.p?alert("Incorrect Password"):void alert(`Correct Password! Your
flag is ${atob(t.p)}.`)}))})();
```

cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ
CyberChef from Base 64 (The magic filter)

| | | |
|---|---|---|
| | _53rv3r} | Entropy: 3.16 |
| -Za-z0-9_.',true) | picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r} | Valid UTF8<br>Entropy: 3.16 |
| | cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ | Matching ops: Fr<br>Valid UTF8<br>Entropy: 4.40 |

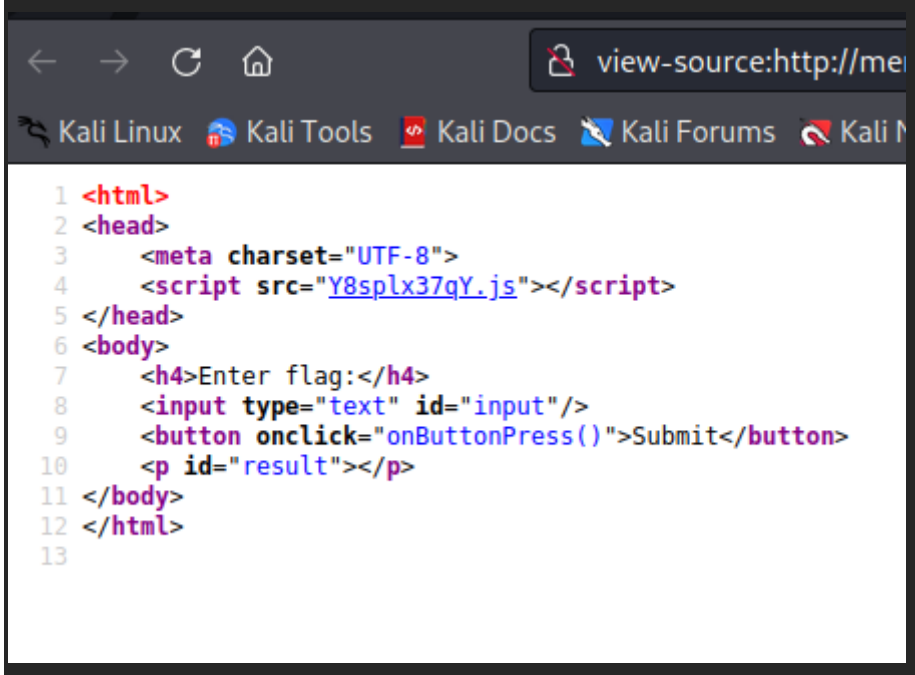



Entering "flag" does not work. haha!

While dirsearch is running i look at html

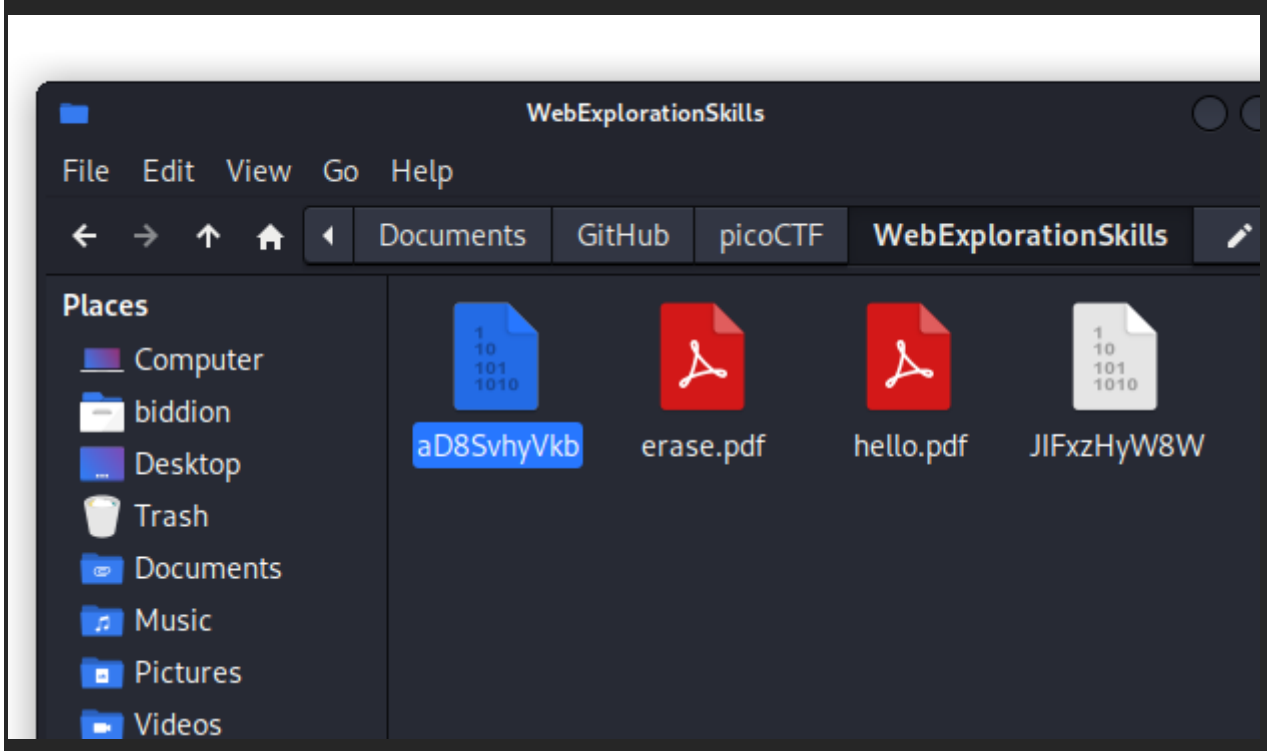



and find .js

```
const _0x6d8f=
['copy_char','value','207aLjBod','1301420SaUSqf','233ZRpipt','2224QffgXU','check_flag','408533hsoVYx','instance','278338GVFUrH','Correct!','54
9933ZVjkwI','innerHTML','charCodeAt','./aD8SvhyVkb','result','977AzKzwq','Incorrect!','exports','length','getElementById','1jIrMBu','input','6
15361geljRK'];const _0x5c00=function(_0x58505a,_0x4d6e6c){_0x58505a=_0x58505a-0xc3;let _0x6d8fc4=_0x6d8f[_0x58505a];return _0x6d8fc4;};
(function(_0x12fd07,_0x4e9d05){const _0x4f7b75=_0x5c00;while(!![]){try{const _0x1bb902=-parseInt(_0x4f7b75(0xc8))*-parseInt(_0x4f7b75(0xc9))+-
parseInt(_0x4f7b75(0xcd))+parseInt(_0x4f7b75(0xcf))+parseInt(_0x4f7b75(0xc3))+-
parseInt(_0x4f7b75(0xc6))*parseInt(_0x4f7b75(0xd4))+parseInt(_0x4f7b75(0xcb))+-
parseInt(_0x4f7b75(0xd9))*parseInt(_0x4f7b75(0xc7));if(_0x1bb902===_0x4e9d05)break;else _0x12fd07['push'](_0x12fd07['shift']
());}catch(_0x4f8a){_0x12fd07['push'](_0x12fd07['shift']());}}}(_0x6d8f,0x4bb06));let exports;(async()=>{const _0x835967=_0x5c00;let
_0x1adb5f=await fetch(_0x835967(0xd2)),_0x355961=await WebAssembly['instantiate'](await _0x1adb5f['arrayBuffer']
()),_0x5c0ffa=_0x355961[_0x835967(0xcc)];exports=_0x5c0ffa[_0x835967(0xd6)];})();function onButtonPress(){const _0x50ea62=_0x5c00;let
_0x5f4170=document[_0x50ea62(0xd8)](_0x50ea62(0xda))[_0x50ea62(0xc5)];for(let _0x19d3ca=0x0;_0x19d3ca<_0x5f4170['length'];_0x19d3ca++)
{exports[_0x50ea62(0xc4)](_0x5f4170[_0x50ea62(0xd1)](_0x19d3ca),_0x19d3ca);}exports['copy_char']
(0x0,_0x5f4170[_0x50ea62(0xd7)]),exports[_0x50ea62(0xca)]()==0x1?document['getElementById'](_0x50ea62(0xd3))
[_0x50ea62(0xd0)]=_0x50ea62(0xce):document[_0x50ea62(0xd8)](_0x50ea62(0xd3))['innerHTML']=_0x50ea62(0xd5);}
```

These two look interesting
'278338GVFUrH','Correct!'
'./aD8SvhyVkb'

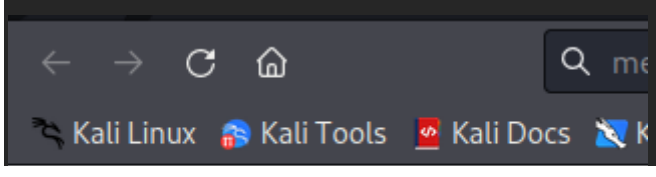
I download the file

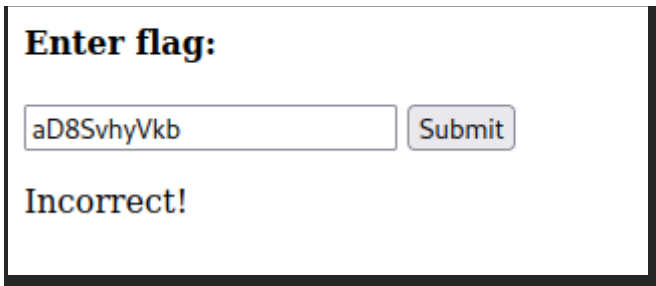



```
┌──(biddion㉿kali)-[~/Documents/GitHub/picoCTF/WebExplorationSkills]
└─$ file aD8SvhyVkb
aD8SvhyVkb: WebAssembly (wasm) binary module version 0x1 (MVP)
```

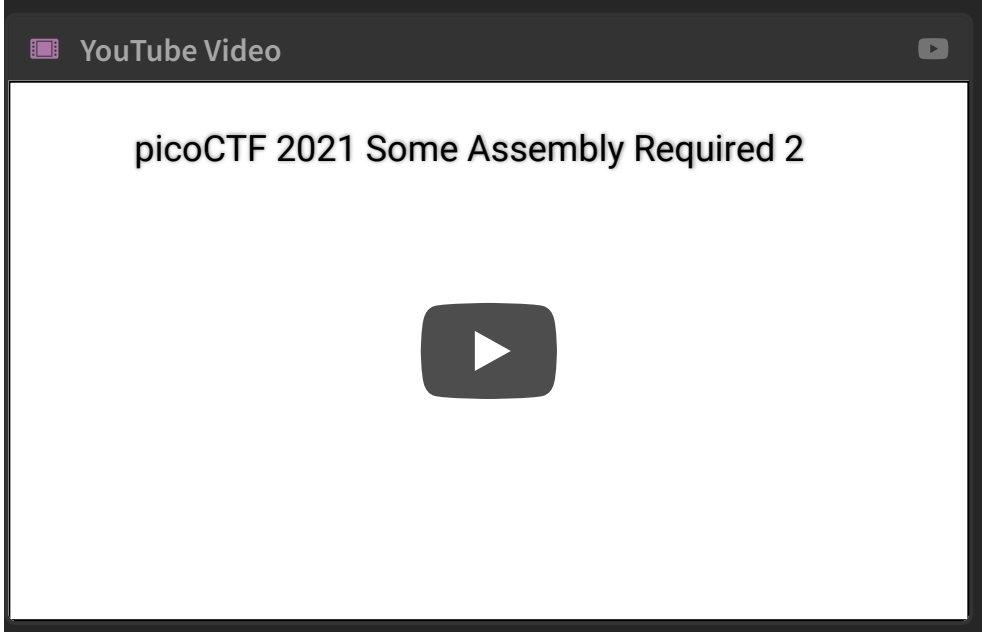
both running this and cat'ing it doesn't bear fruit nor flag.

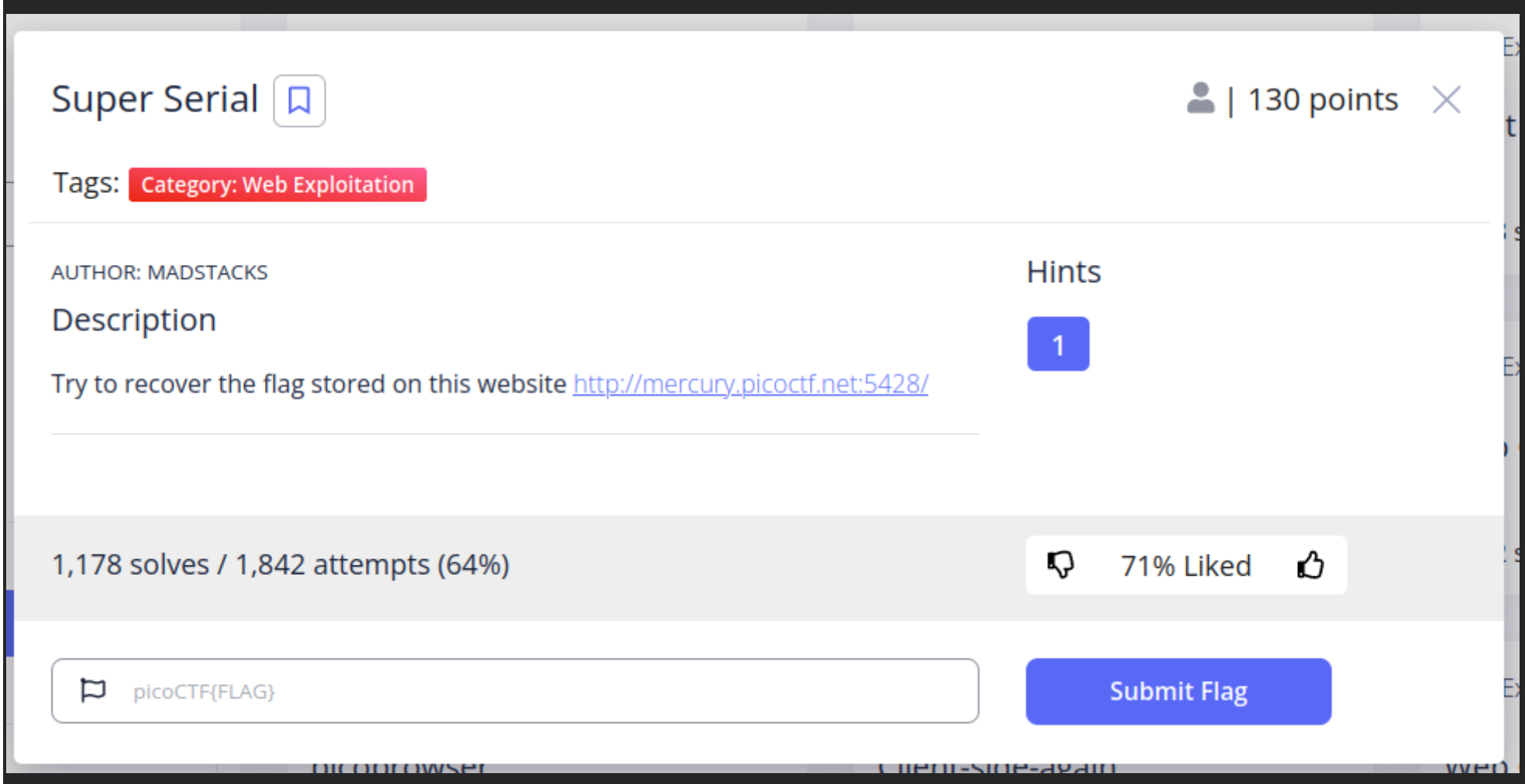
copy 278338GVFUrH into the box doesn't work nor does aD8SvhyVkb

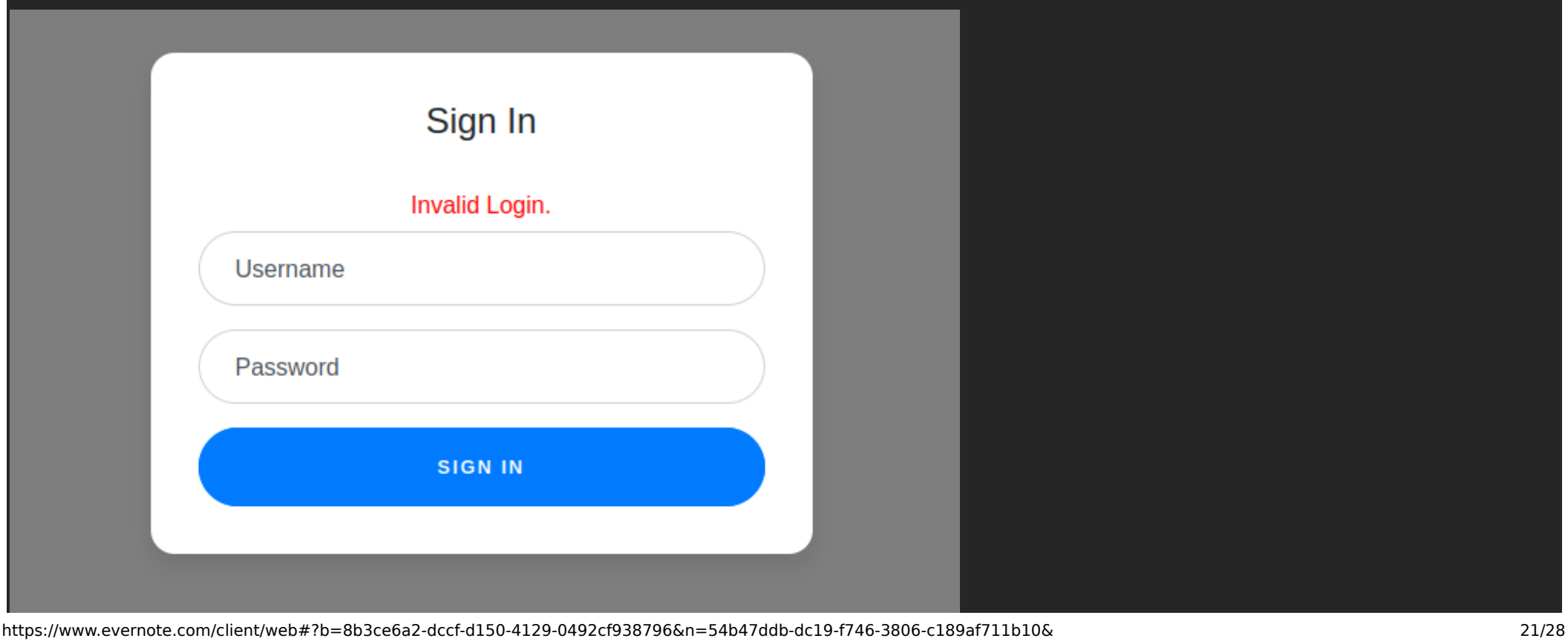





Being stumped, I looked up a writeup and found I need to know about webassembly/debugging



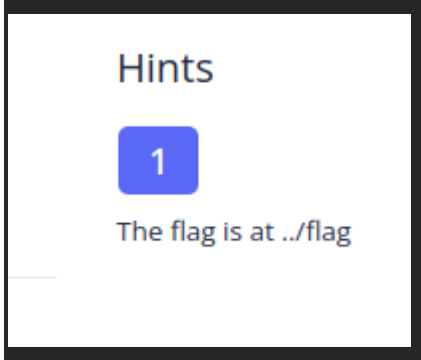



view-source:http://mercury.picoctf.net:5428/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
<!DOCTYPE html>
<html>
<head>
<link href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<link href="style.css" rel="stylesheet">
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>
</head>
    <body>
        <div class="container">
            <div class="row">
                <div class="col-sm-9 col-md-7 col-lg-5 mx-auto">
                    <div class="card card-signin my-5">
                        <div class="card-body">
                            <h5 class="card-title text-center">Sign In</h5>
                            <h6 class="text-center" style="color:red">Invalid Login.</h6>                        <form class="form-signin" action="index.php" method="post">
                                <div class="form-label-group">
                                    <input type="text" id="user" name="user" class="form-control" placeholder="Username" required autofocus>
                                    <label for="user">Username</label>
                                </div>

                                <div class="form-label-group">
                                    <input type="password" id="pass" name="pass" class="form-control" placeholder="Password" required>
                                    <label for="pass">Password</label>
                                </div>

                                <button class="btn btn-lg btn-primary btn-block text-uppercase" type="submit">Sign in</button>
                            </form>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </body>
</html>
```

The .js which is too massive to be of any use to me.

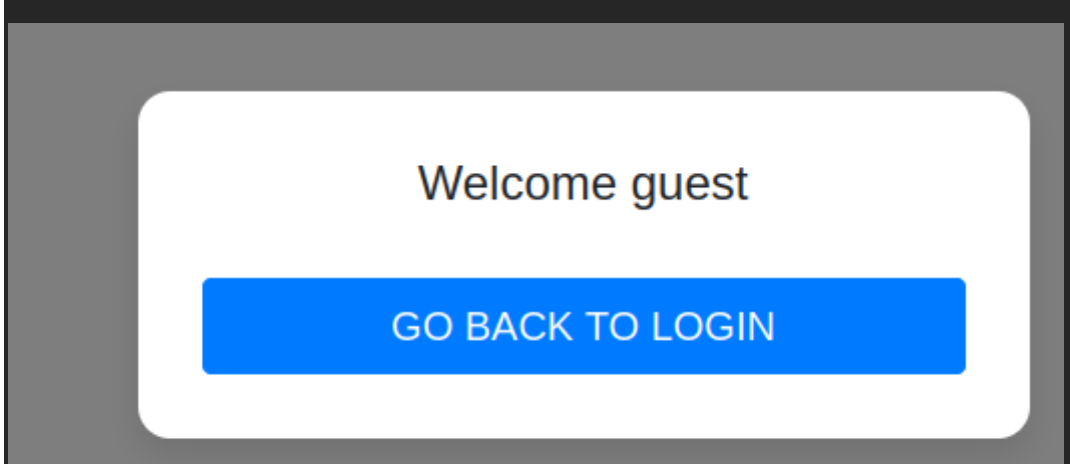



```
 _|. _ _  _  _  _ _|_    v0.4.2
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method

Output File: /home/biddion/.dirsearch/reports/merc

Error Log: /home/biddion/.dirsearch/logs/errors-22

Target: http://mercury.picoctf.net:5428/

[14:35:30] Starting:
[14:36:08] 200 -    0B  - /access.log
[14:36:34] 200 -    1KB - /authentication.php
[14:36:46] 200 -    0B  - /cookie.php
[14:37:03] 200 -    1KB - /index.php
[14:37:03] 200 -    1KB - /index.php/login/
[14:37:32] 200 -   36B  - /robots.txt

Task Completed
```

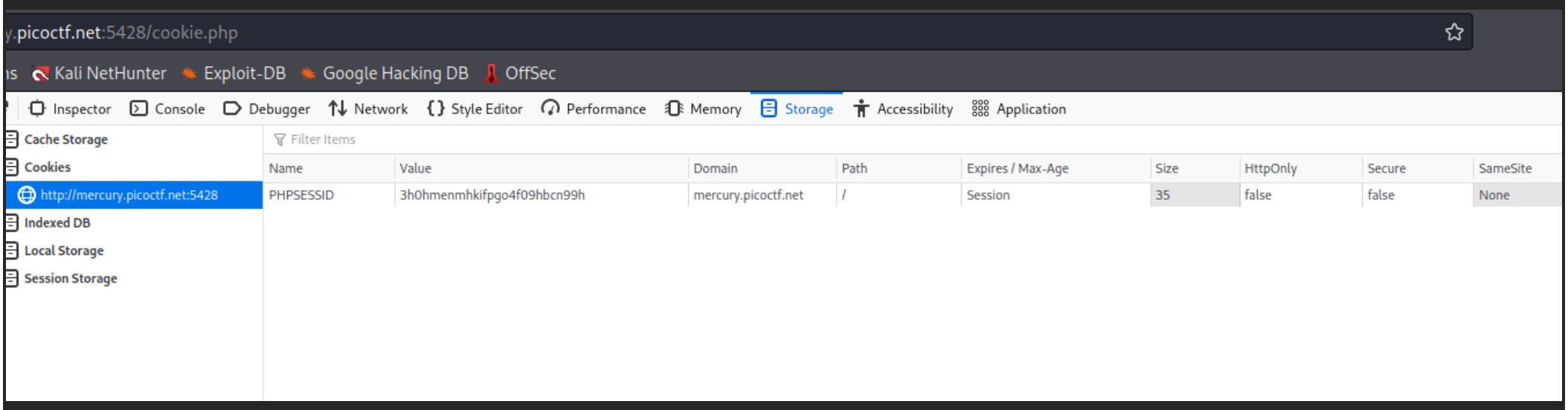
I'll try each of the above

/access.log is just as it says; but it's empty

/authentication.php

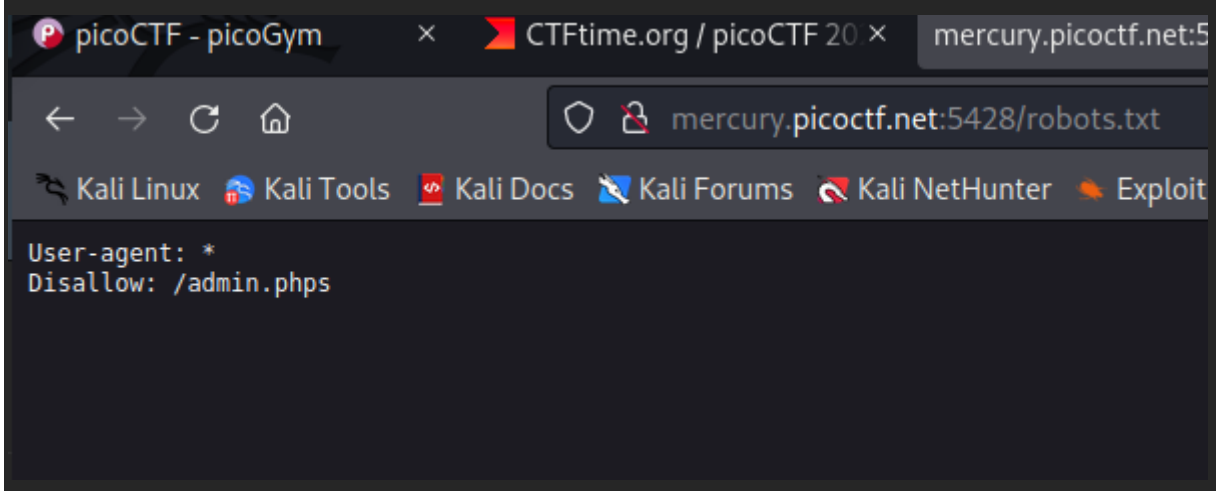


/cookie.php



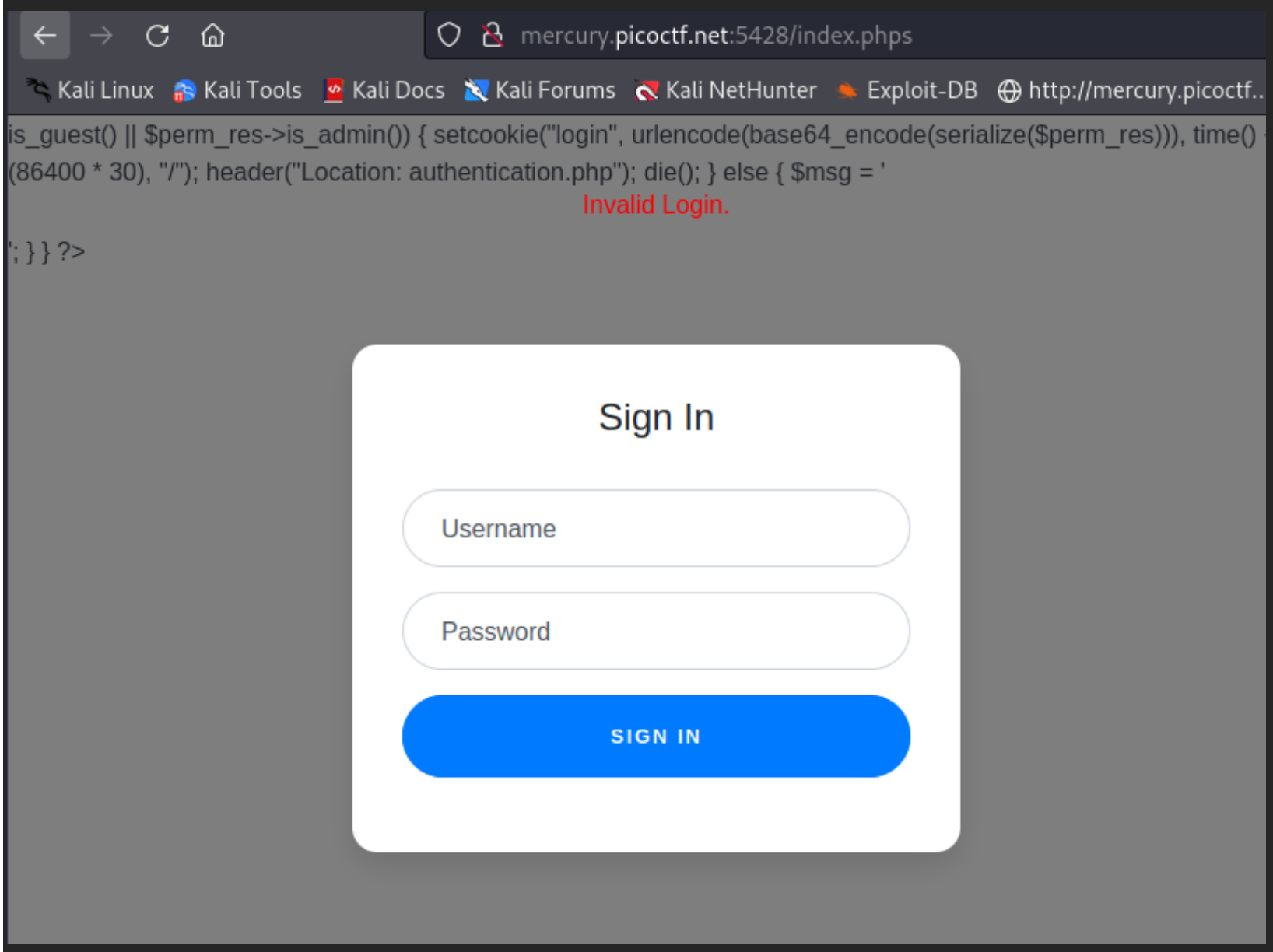

Hmmmm "3h0hmenmhkifpgo4f09hbcn99h"?

/robots.txt

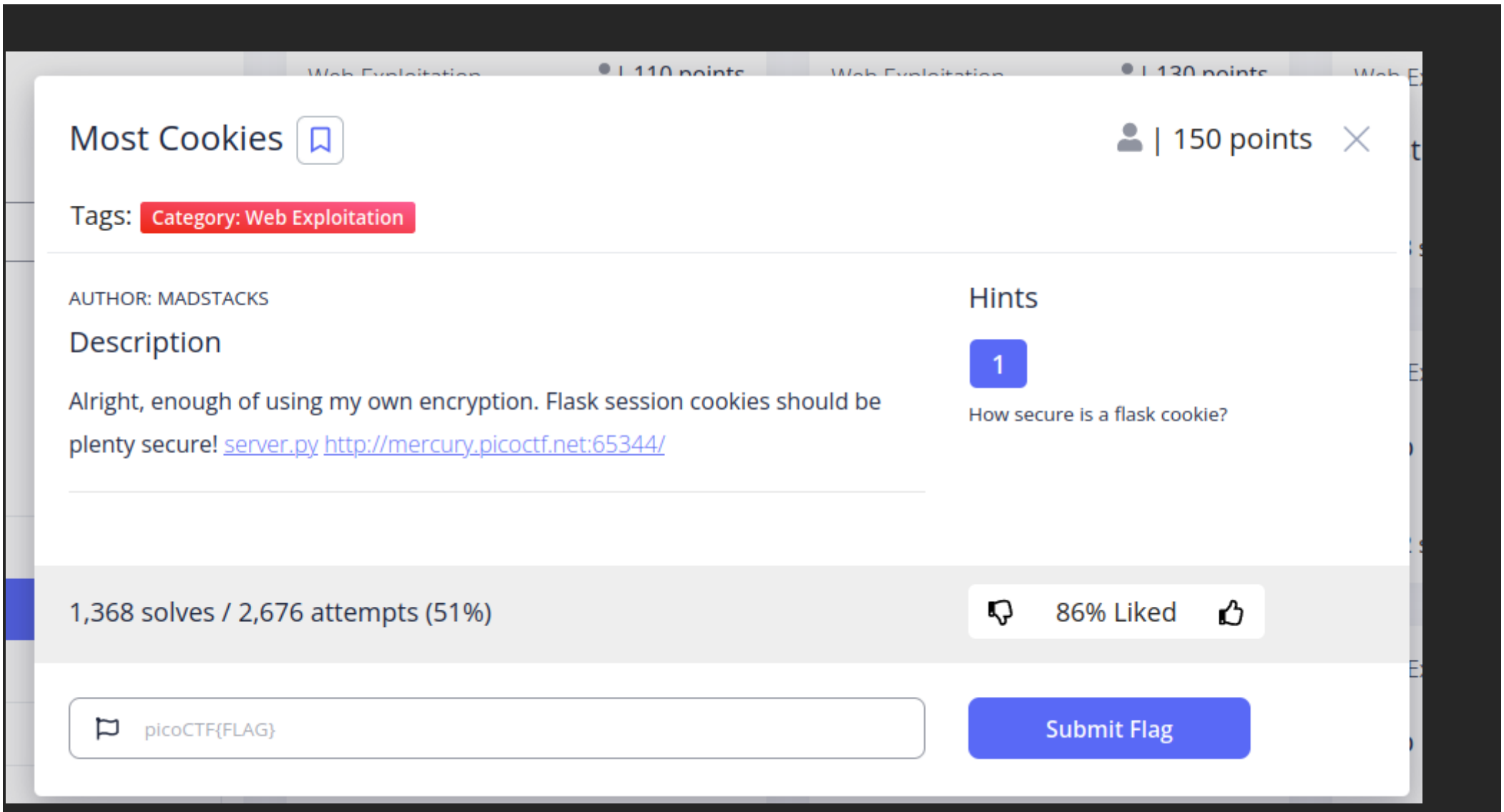



/admin.phps? _ not found nor is .php an option
Let's try SQLi via Burp's Intruder.--Doesn't look fruitful
I looked up more about what is .phps
https://filext.com/file-extension/PHPS

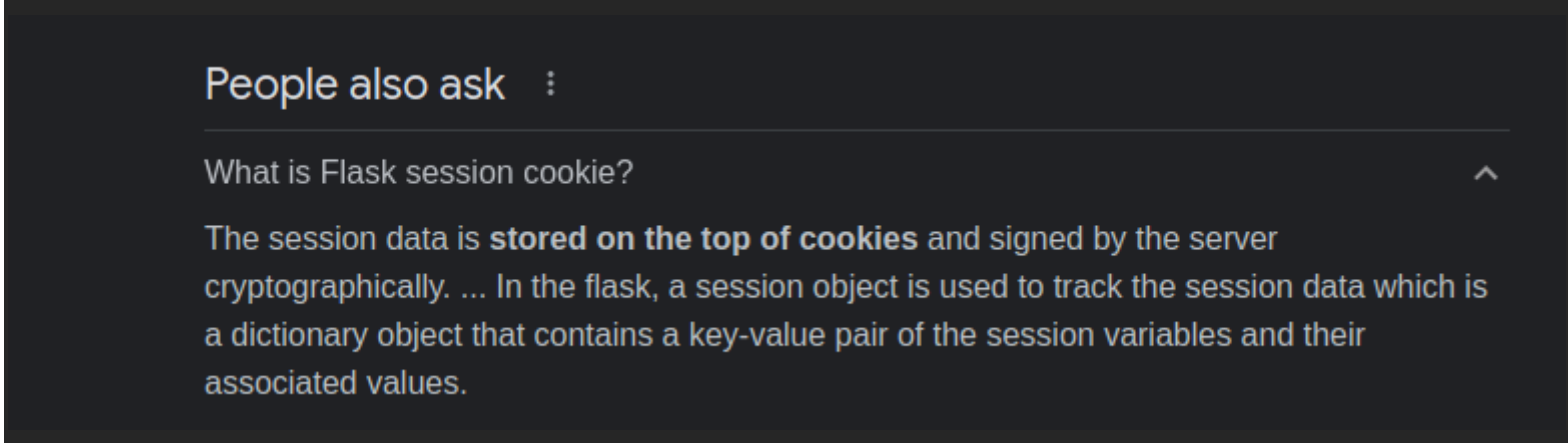
The text in BG is a bit weird




I'm not sure what to do here. I don't know much about how websites work.__I have to quit here.




First I need to learn what is a flask 'session' cookie




## Setting a Cookie

In Flask, we use `set_cookie()` method of the response object to set cookies. The syntax of `set_cookie()` method is as follows:

```
set_cookie(key, value="", max_age=None)
```

The `key` is a required argument and refers to the name of the cookie. The `value` is data you want to store in the cookie and it defaults to empty string. The `max_age` refers to the expiration time of the cookie in seconds, if not set the cookie will cease to exist when the user closes the browser.

Open `main2.py` and add the following code just after the `contact()` view function:

**flask_app/main2.py**

```
from flask import Flask, render_template, request, redirect, url_for, flash, make_res
#...
@app.route('/cookie/')
def cookie():
    res = make_response("Setting a cookie")
    res.set_cookie('foo', 'bar', max_age=60*60*24*365*2)
    return res
#...
```

Here we are creating a cookie named `foo` with the value `bar` that will last for 2 years.

Start the server and visit http://localhost:5000/cookie/. You should see a page with "Setting a

Looking at the .py that was supplied

```
        return resp
    else:
        message = "That doesn't appear to be a valid cookie."
        category = "danger"
        flash(message, category)
        resp = make_response(redirect("/"))
        session["very_auth"] = "blank"
        return resp

@app.route("/reset")
def reset():
    resp = make_response(redirect("/"))
    session.pop("very_auth", None)
    return resp

@app.route("/display", methods=["GET"])
def flag():
    if session.get("very_auth"):
        check = session["very_auth"]
        if check == "admin":
            resp = make_response(render_template("flag.html", value=flag_value, title=title))
            return resp
        flash("That is a cookie! Not very special though...", "success")
        return render_template("not-flag.html", title=title, cookie_name=session["very_auth"])
    else:
        resp = make_response(redirect("/"))
        session["very_auth"] = "blank"
        return resp

if __name__ == "__main__":
    app.run()
```

Does this mean I need to have 'admin' cookie?

I learned about cookie encryption

https://jwt.io

picobrowser | 200 points

Tags: Category: Web Exploitation

AUTHOR: ARCHIT

Description

This website can be rendered only by **picobrowser**, go and catch the flag!

https://jupiter.challenges.picoctf.org/problem/26704/ (link) or

http://jupiter.challenges.picoctf.org:26704

Hints

1

You don't need to download a new web browser

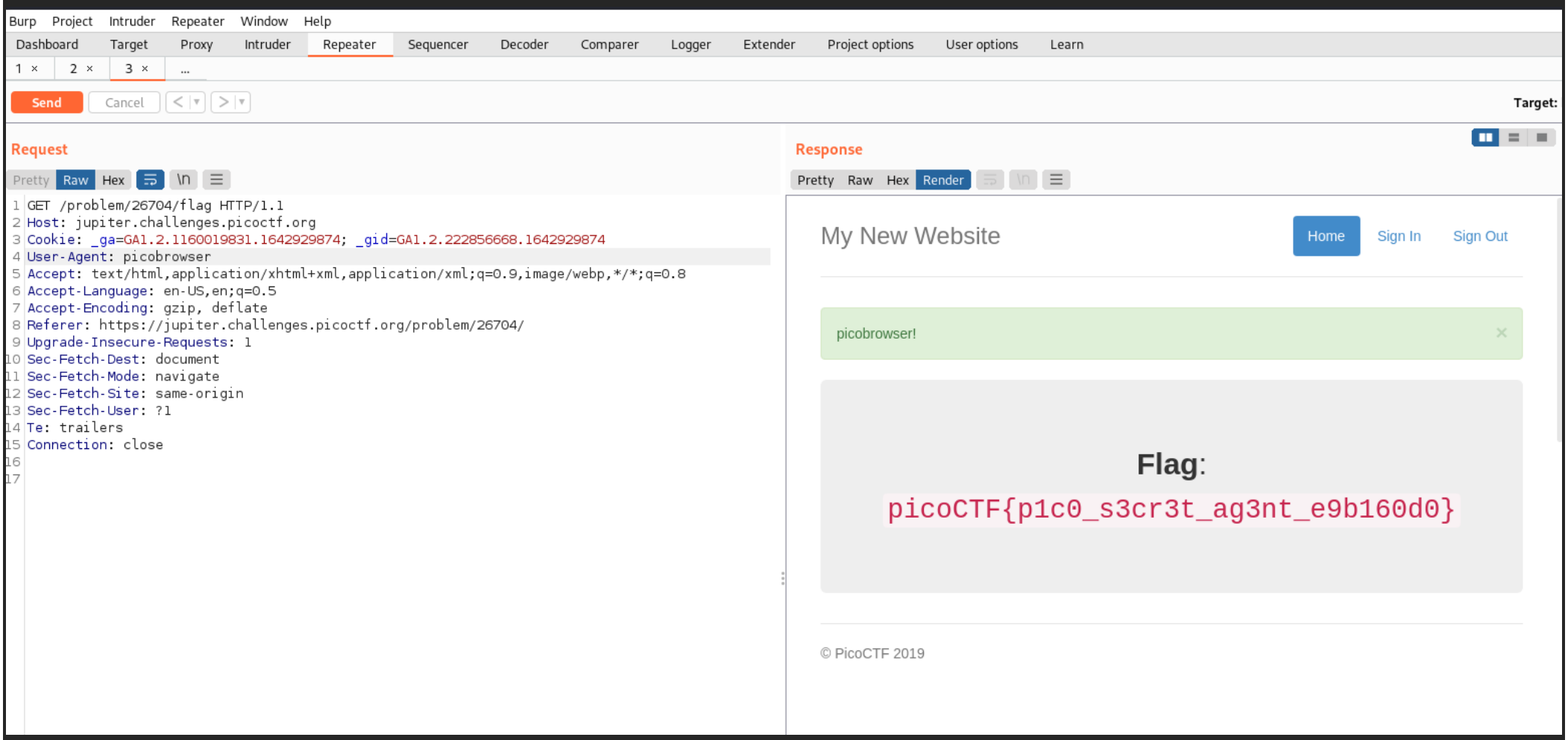
12,808 solves / 17,542 attempts (73%)

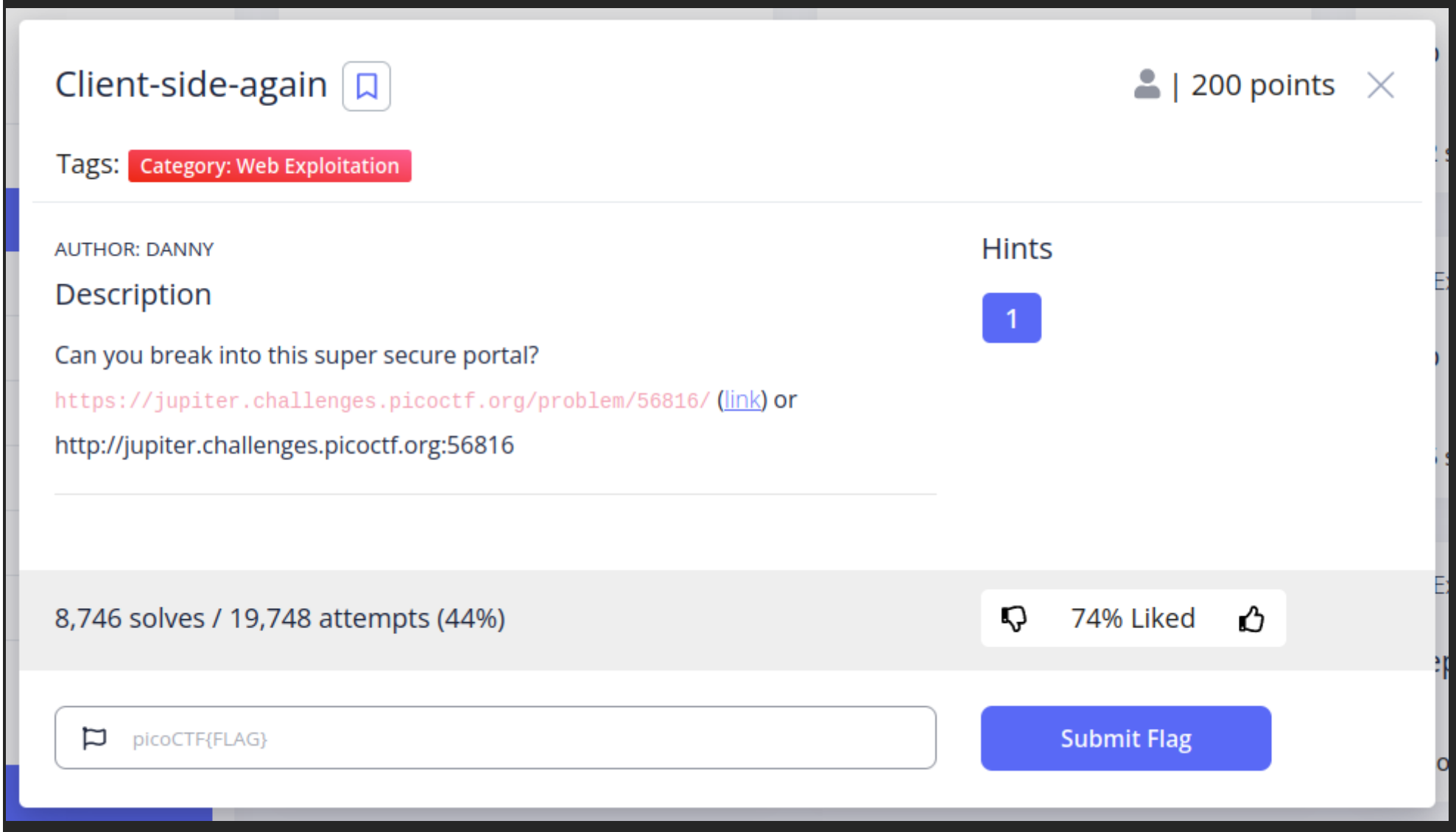
89% Liked

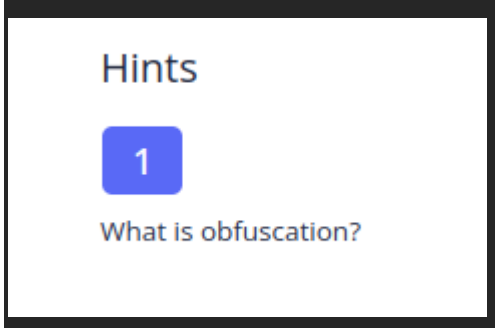
picoCTF{FLAG}

Submit Flag

This was easy with Burp

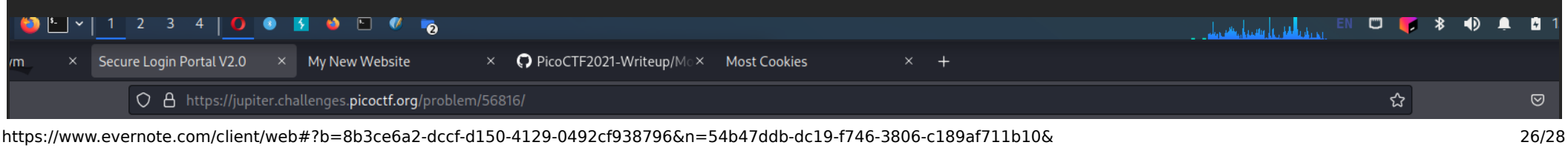


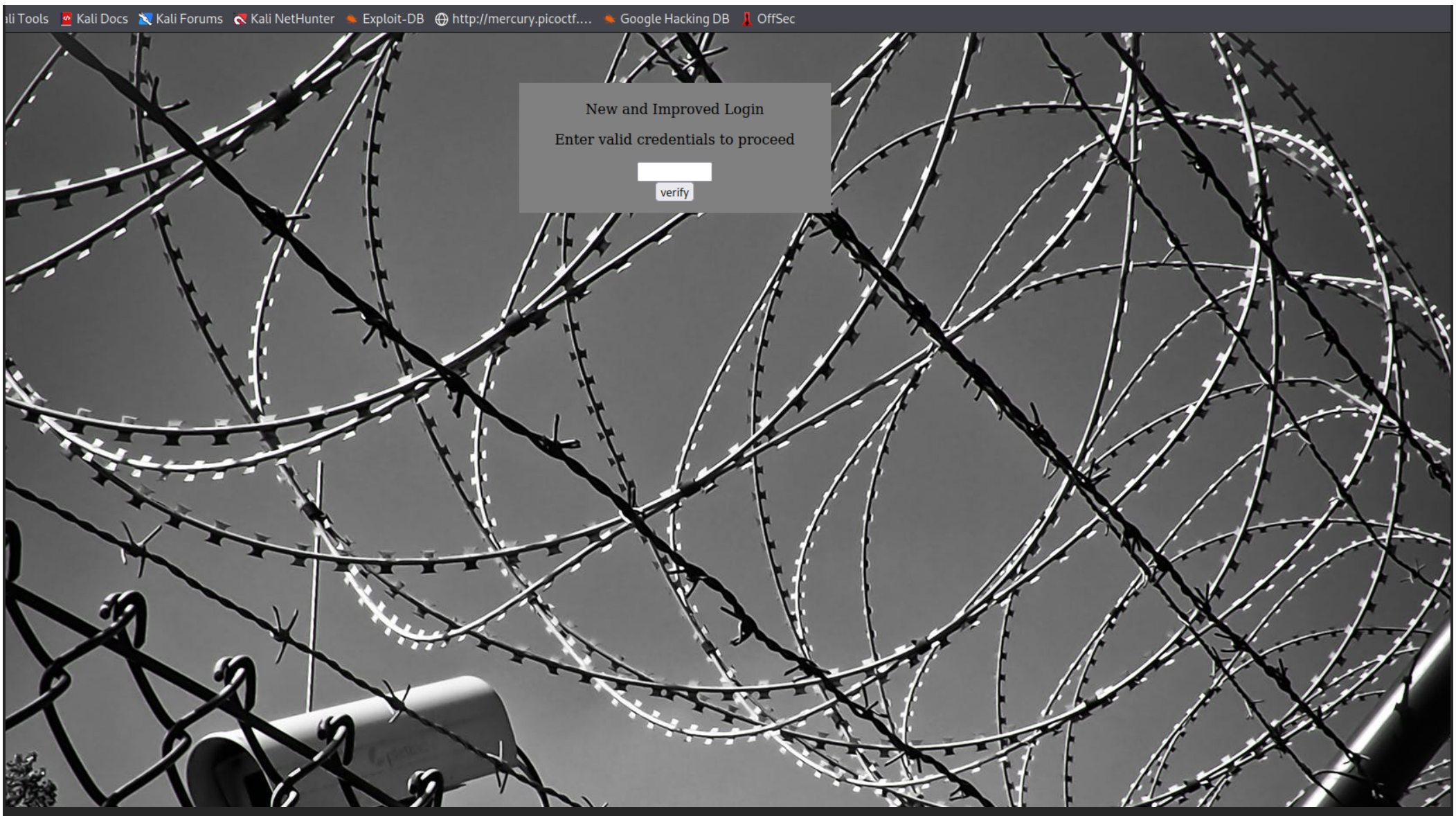



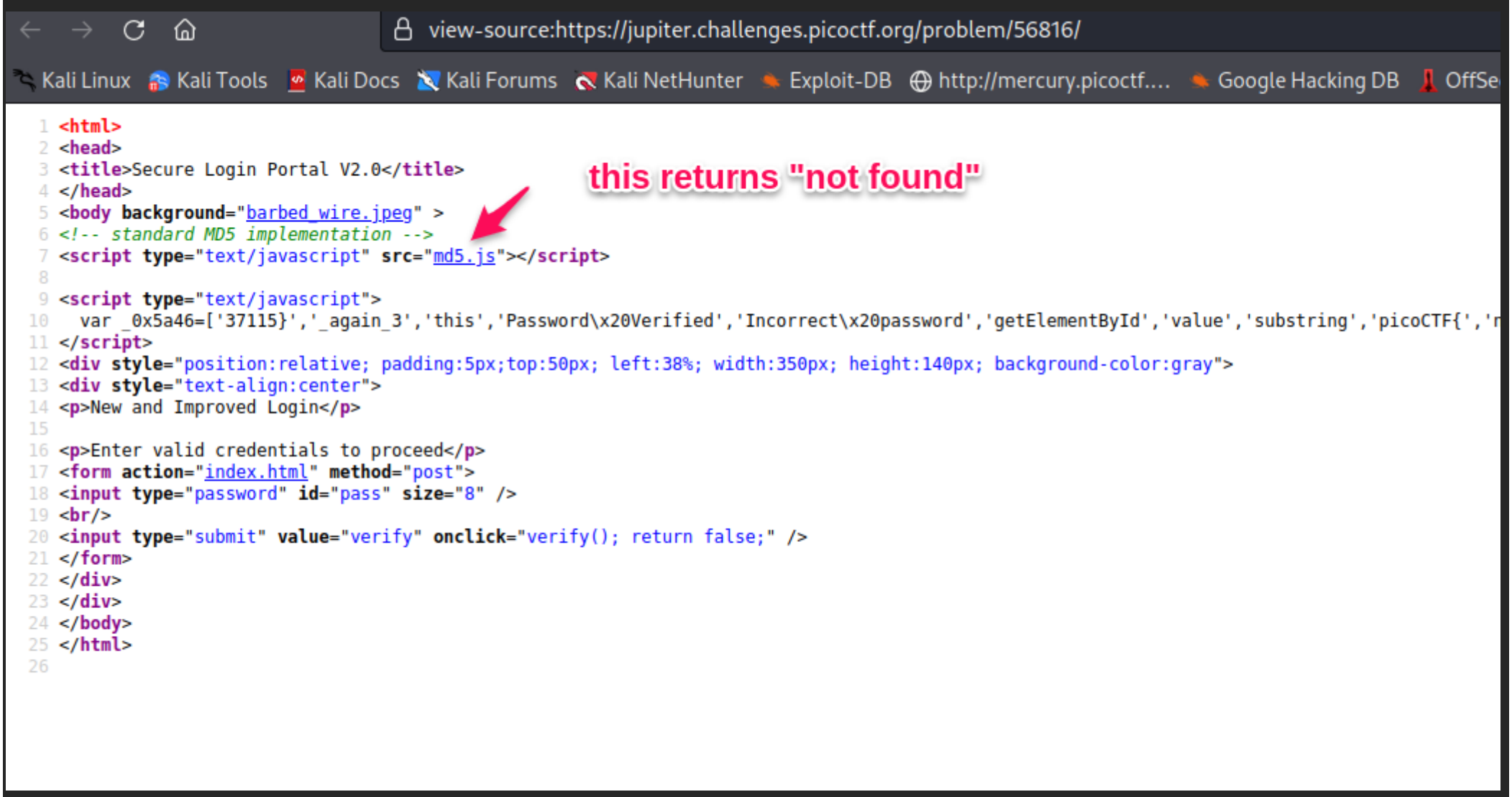




https://www.quora.com/Is-code-obfuscation-a-common-practice-to-protect-the-client-side-code-in-web-applications

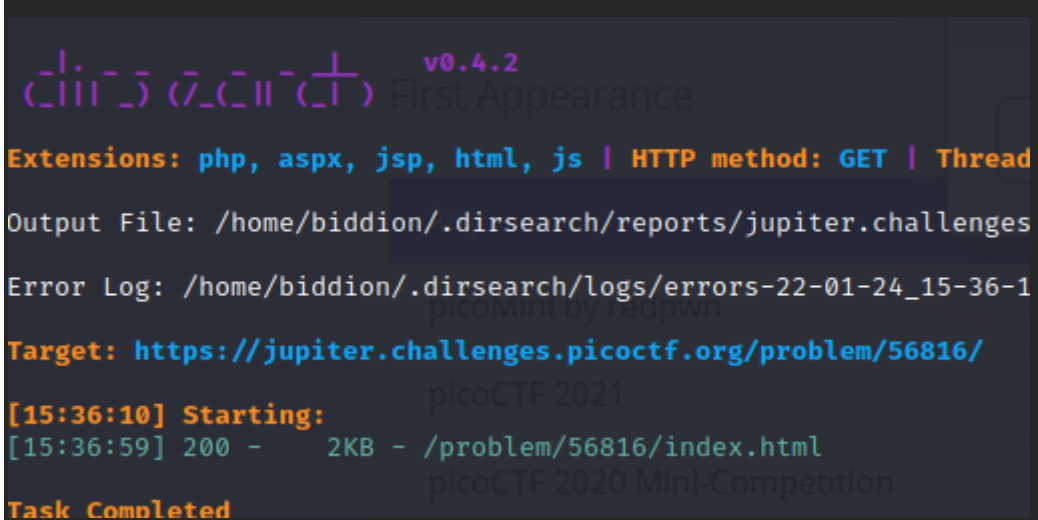
Various build tools are available to developers to perform obfuscation, with a few of the most prominent being the JavaScript Obfuscator, Google Closure Compiler, YUI Compressor, and UglifyJS. Arguably, these processors are just **minifiers with added optimizations to mangle code**.






Not much here



These problems are only getting harder. Maybe I'll come back next year.

The End!--for now