

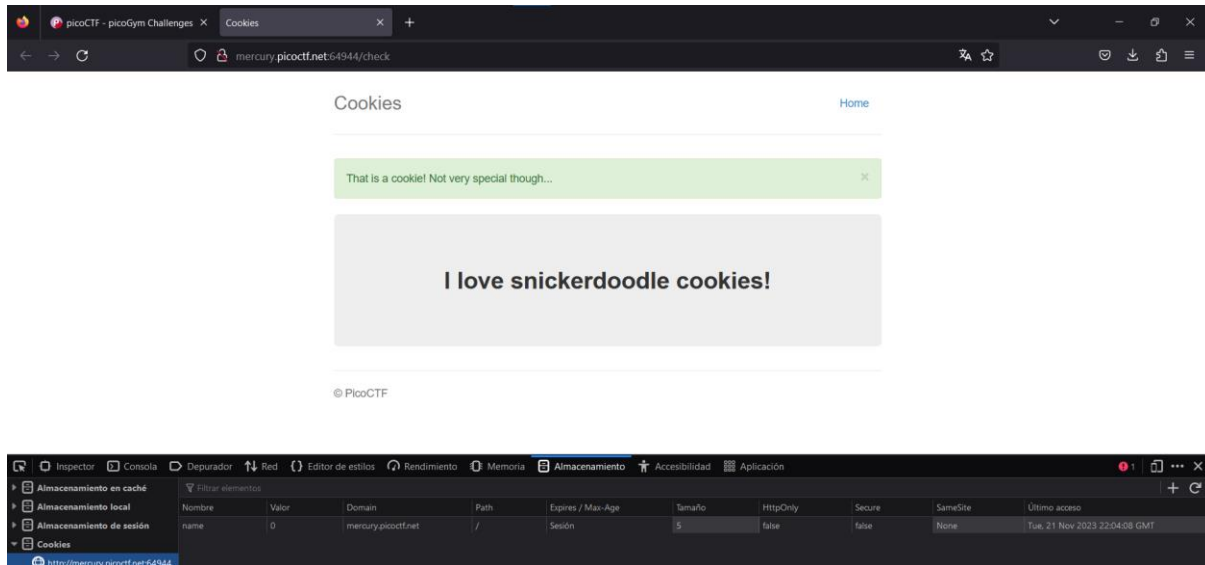
Name: Daniel Silva

Code: 00201725

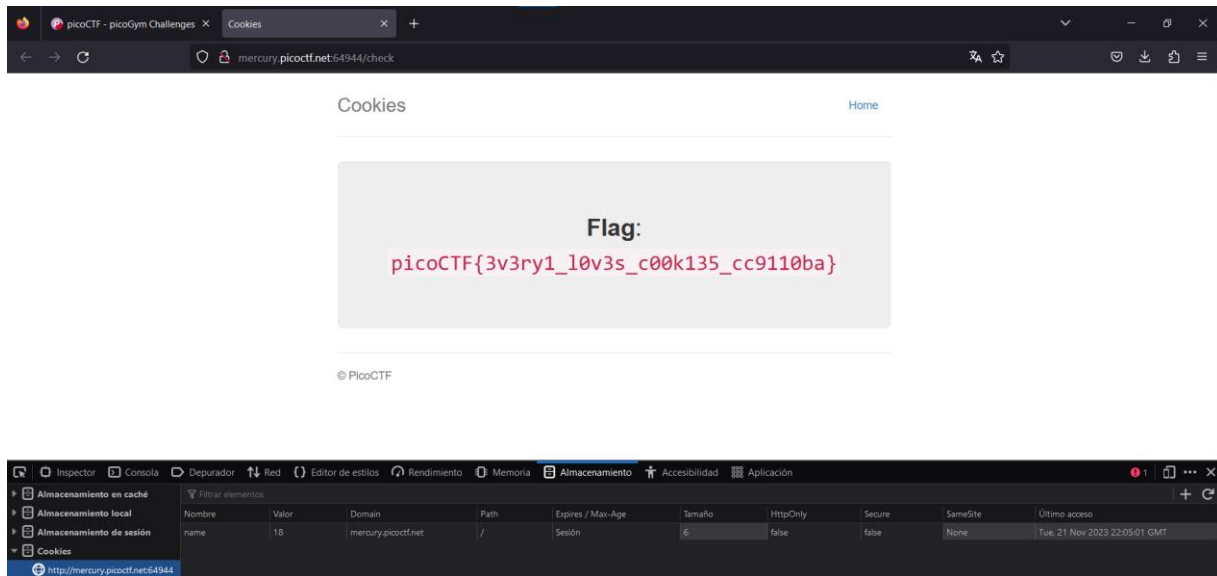
Theme: HMW3.

## 1. Cookies: Who doesn't love cookies? Try to figure out the best one.

For this exercise, the instructions given are followed, so when typing "snickerdoodle", this screen appeared:

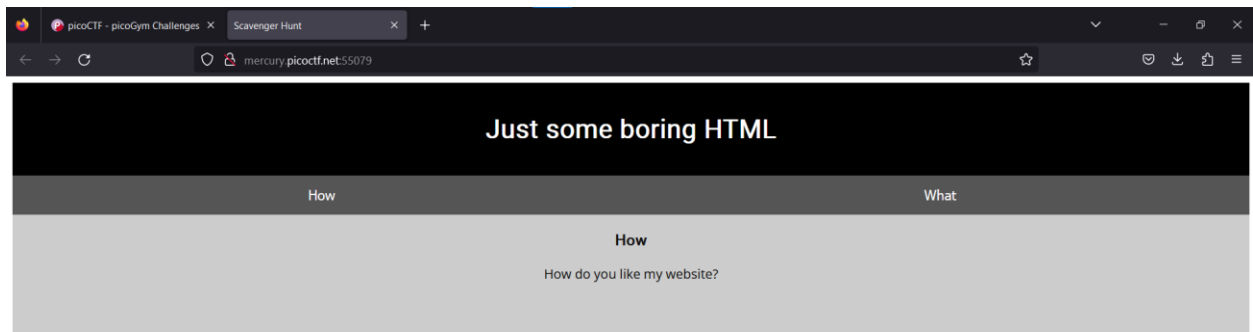


I inspected the page and looked for the cookies. I noticed that the value was 0, so I changed the value and saw that the text was different. Finally, I tried the value one by one, until 18 showed me the flag.



## 2. Scavenger Hunt: There is some interesting information hidden around this site. Can you find it?

For this exercise, the screen we find is the following:



Now to find the flag inspect the web page, and in the code I found this:

```

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

```

Which means that the flag is found in parts.

Then, I continued browsing the files of the page I had access to, and in the CSS file I found the following part of the flag. Also, this gave me clues on how I can find the next part.

```

display: none;
padding: 50px;
text-align: center;
}

#tabintro { background-color: #ccc; }
#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 */

```

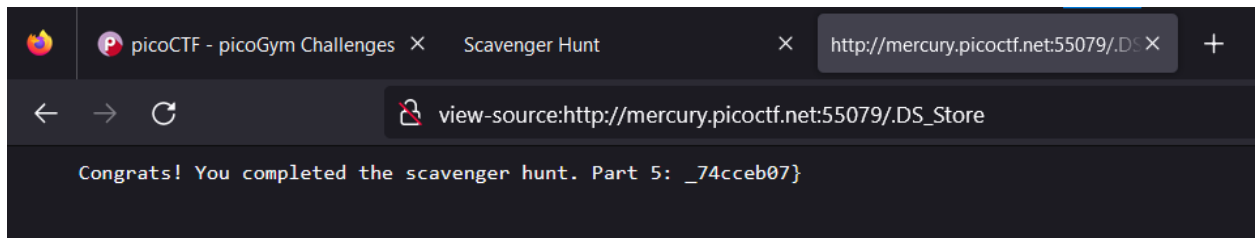
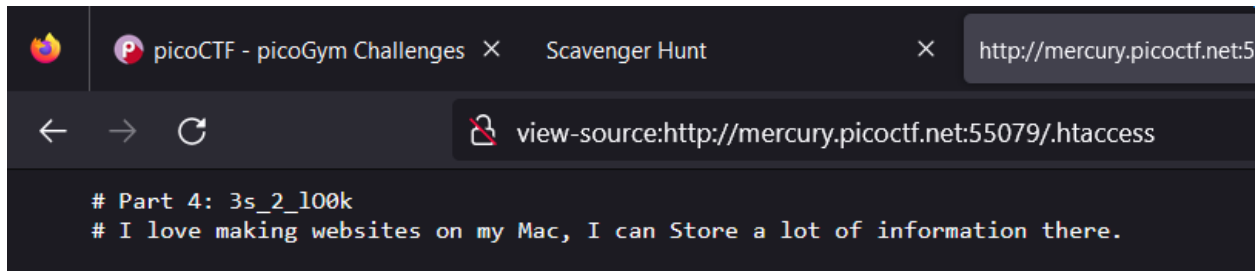
We find the next part when we access robots.txt. And in that same place, it gives me the clue on how to access the last part of the flag.

```

User-agent: *
Disallow: /index.html
# Part 3: t_of_pl4c
# I think this is an apache server... can you Access the next flag?

```

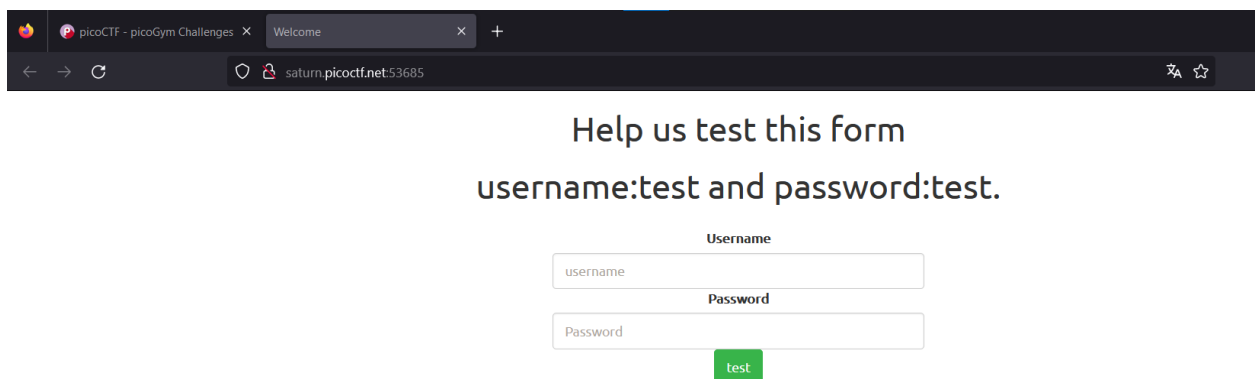
Finally, we follow the track and set out on the route and he gives us the last parts of the flag.



Flag: picoCTF{th4ts\_4\_l0t\_of\_pl4c3s\_2\_100k\_74cceb07}

3. **Findme:** Help us test the form by submitting the username as test and password as test! Additional details will be available after launching your challenge instance.

To start, the service is launched.



Help us test this form

username:test and password:test.

Username

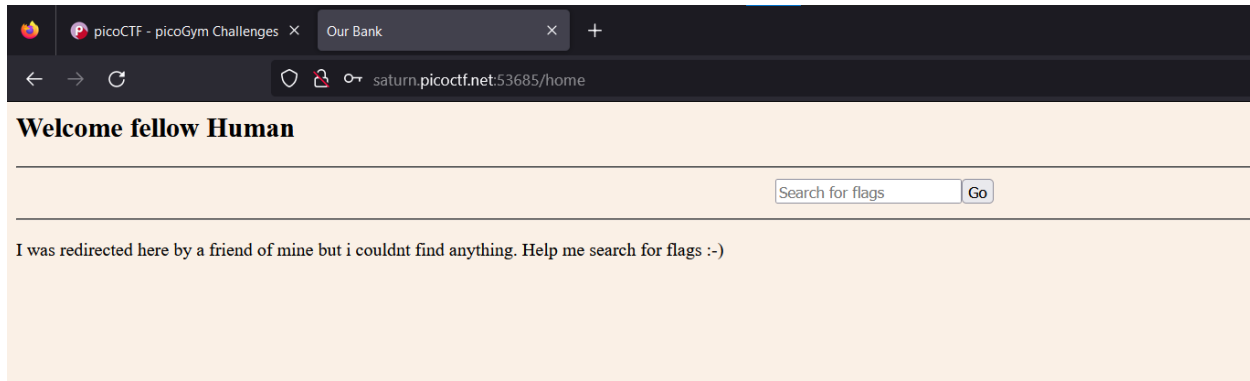
username

Password

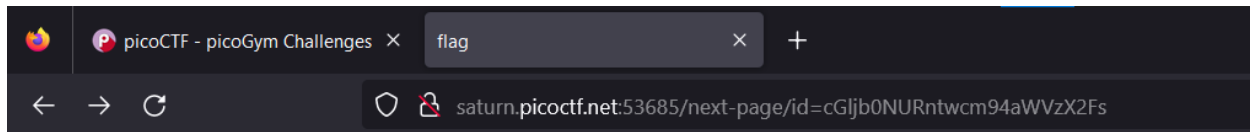
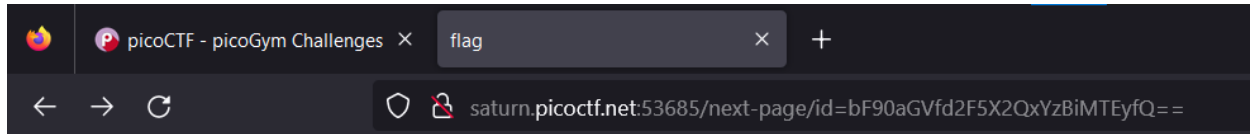
Password

test

We enter the given credentials. Now we have this screen:



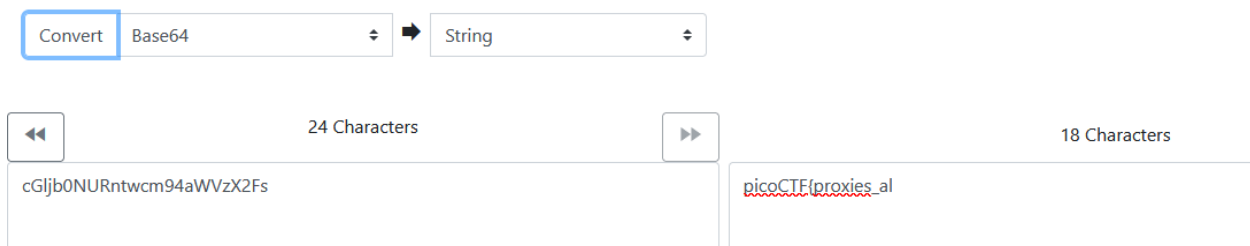
Actually, I did not find functionality on this screen, but when I tried to return to the previous screen, I realized that on the route, it gives me an ID. Additionally, when I return to the previous screen, it gives me a different ID.



I tried to give it a meaning, and I realized that it might be base64 encrypted. So I used a b64 to string calculator. And that's how I found the flag.

## Convert String

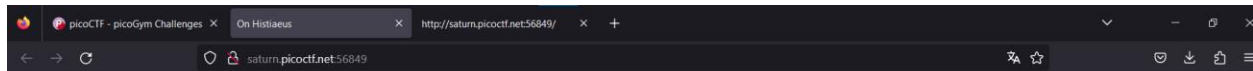
Convert to base64, hex, binary, MD5 or SHA256 hash, AES and 3DES encryption and more



Flag: picoCTF{proxies\_all\_the\_way\_d1c0b112}

## 4. Inspect HTML: Can you get the flag? Go to this website and see what you can discover.

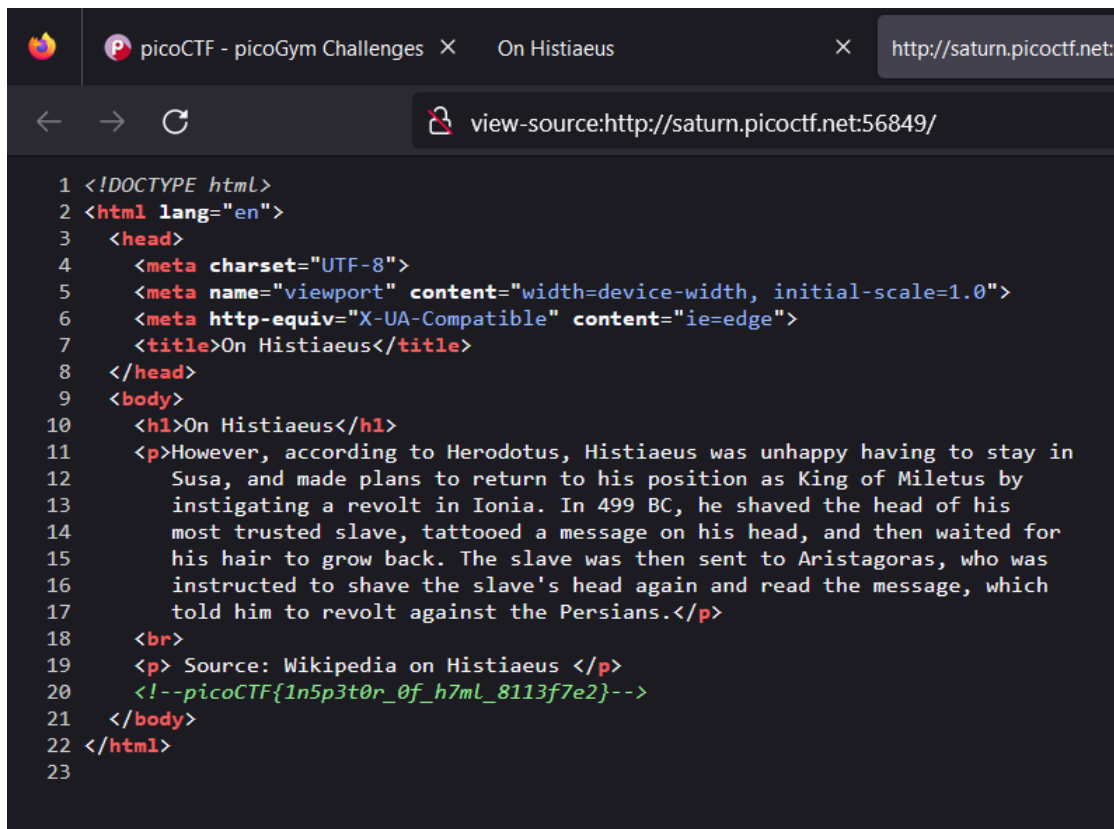
This exercise was simple. When I inspected the source code of the web page, the flag was in a comment.



### On Histiaeus

However, according to Herodotus, Histiaeus was unhappy having to stay in Susa, and made plans to return to his position as King of Miletus by instigating a revolt in Ionia. In 499 BC, he shaved the head of his most trusted slave, tattooed a message on his head, and then waited for his hair to grow back. The slave was then sent to Aristagoras, who was instructed to shave the slave's head again and read the message, which told him to revolt against the Persians.

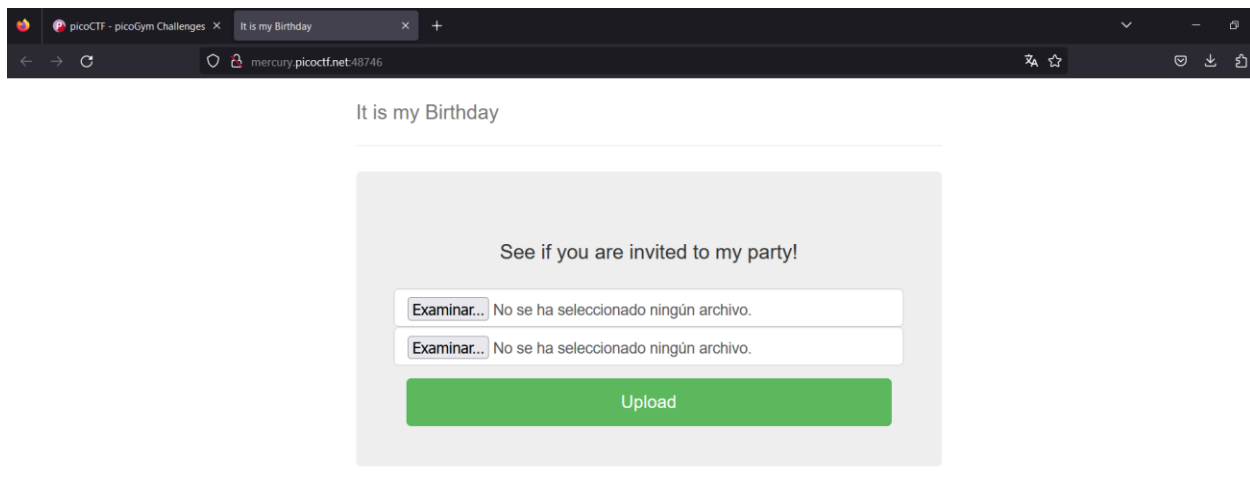
Source: Wikipedia on Histiaeus



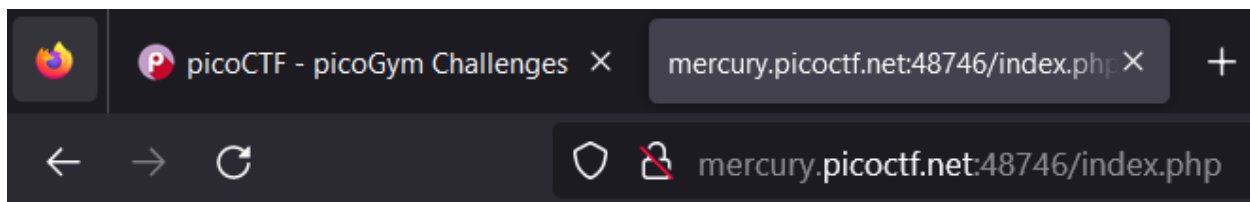
Flag: picoCTF{1n5p3t0r\_0f\_h7ml\_8113f7e2}

5. **It is my Birthday: I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website.**

In this exercise, the instructions given are followed, and two PDFs are uploaded to the website with the characteristics that are indicated.



Then we find this message.



**MD5 hashes do not match!**

Then I was finding information about MD5 collision and I found that it had two hellow files. exe and erase.exe that are used to:

The files were generated by exploiting two facts: the block structure of the MD5 function, and the fact that Wang and Yu's technique works for an arbitrary initialization vector. Therefore, I changed the extension to PDF and it gave me the flag. It gives me the all code.

```
        },
    }
    } 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_aebcbf39}

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

<head>
    <title>It is my Birthday</title>

    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">

    <link href="https://getbootstrap.com/docs/3.3/examples/jumbotron-narrow/jumbotron-narrow.css" rel="style
```

FLAG: picoCTF{c0ngr4ts\_u\_r\_1nv1t3d\_aebcbf39}

## 6. Local Authority: Can you get the flag? Go to this website and see what you can discover.

To start, I inspect the web page and see the code it presents.



```

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     <link rel="stylesheet" href="style.css">
8     <title>Secure Customer Portal</title>
9   </head>
10  <body>
11
12    <h1>Secure Customer Portal</h1>
13
14    <p>Only letters and numbers allowed for username and password.</p>
15
16    <form role="form" action="login.php" method="post">
17      <input type="text" name="username" placeholder="Username" required
18        autofocus></br>
19      <input type="password" name="password" placeholder="Password" required>
20      <button type="submit" name="login">Login</button>
21    </form>
22  </body>
23 </html>
24

```

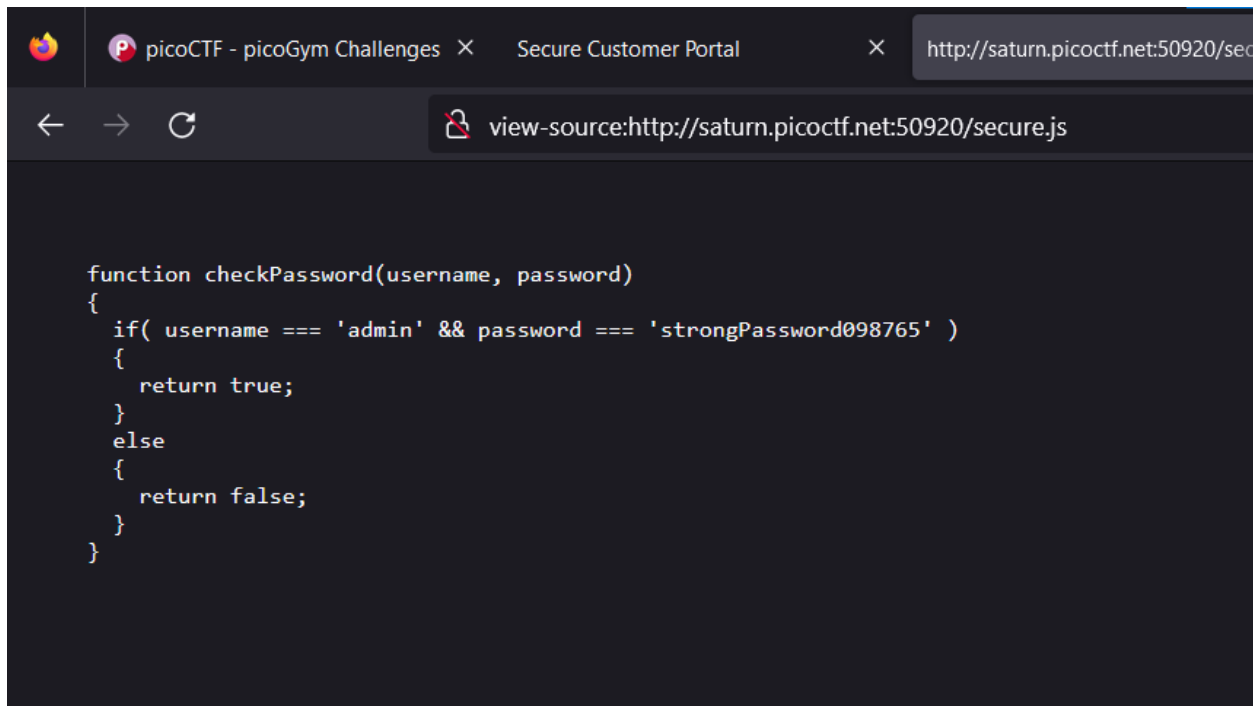
Then, I opened the login.php file

```

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     <link rel="stylesheet" href="style.css">
8     <title>Login Page</title>
9   </head>
10  <body>
11    <script src="secure.js"></script>
12
13    <p id="msg"></p>
14
15    <form hidden action="admin.php" method="post" id="hiddenAdminForm">
16      <input type="text" name="hash" required id="adminFormHash">
17    </form>
18
19    <script type="text/javascript">
20      function filter(string) {
21        filterPassed = true;
22        for (let i = 0; i < string.length; i++){
23          cc = string.charCodeAtAt(i);
24
25          if ( (cc >= 48 && cc <= 57) ||
26              (cc >= 65 && cc <= 90) ||
27              (cc >= 97 && cc <= 122) )
28            {
29              filterPassed = true;

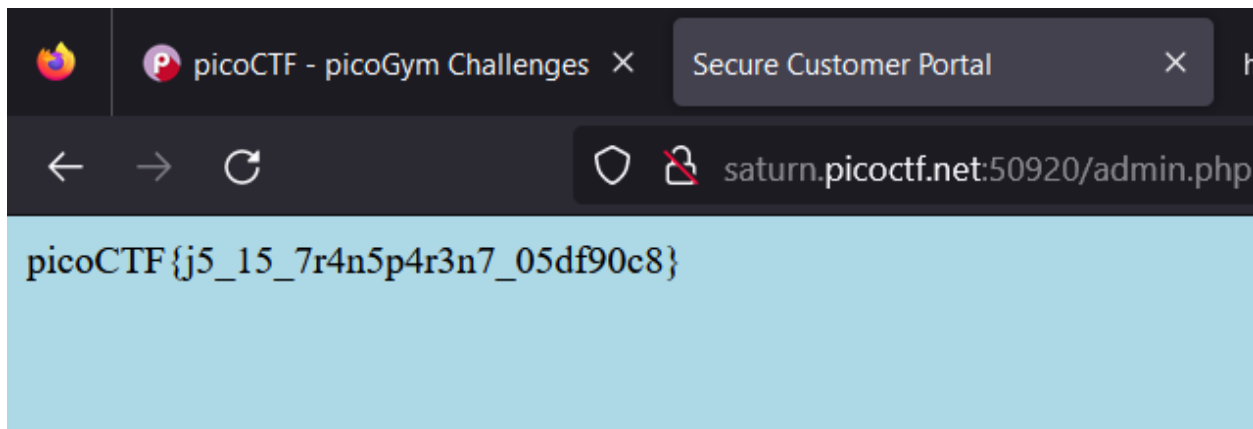
```

In that file I found a secure.js file, where I found the username and password to log in.



```
function checkPassword(username, password)
{
  if( username === 'admin' && password === 'strongPassword098765' )
  {
    return true;
  }
  else
  {
    return false;
  }
}
```

When entering it shows the flag.

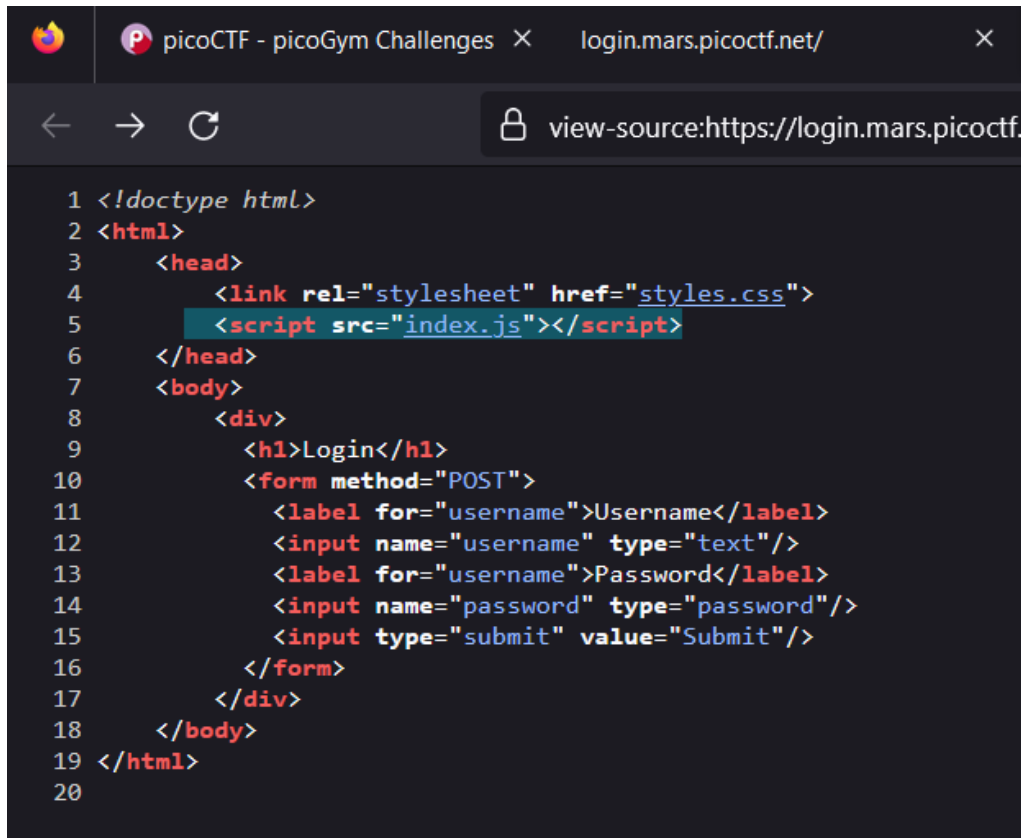


```
picoCTF{j5_15_7r4n5p4r3n7_05df90c8}
```

Flag: picoCTF{j5\_15\_7r4n5p4r3n7\_05df90c8}

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

To start, I inspect the page and found the index.js.



```

1 <!doctype html>
2 <html>
3   <head>
4     <link rel="stylesheet" href="styles.css">
5     <script src="index.js"></script>
6   </head>
7   <body>
8     <div>
9       <h1>Login</h1>
10      <form method="POST">
11        <label for="username">Username</label>
12        <input name="username" type="text"/>
13        <label for="password">Password</label>
14        <input name="password" type="password"/>
15        <input type="submit" value="Submit"/>
16      </form>
17    </div>
18  </body>
19 </html>
20

```

Now, in this file I found a return code after login attempt.



```

current.querySelector(r[e]).value).replace(/</g>""));return"YmItaW4="!t.t.u?alert("Incorrect Username"):"GGI3b0MURos1M332M33fNTNyd3HyXsUzcnYzc1B1M332M33fNTNyd3HyfQ"!=t.p?alert("Incorrect Password");void alert("Correc

```

This code is in B64, so I transformed it to string.

## Convert String

Convert to base64, hex, binary, MD5 or SHA256 hash, AES and 3DES encryption and more

Convert Base64 String

58 Characters 43 Characters

cGljb0NURns1M3J2M3JfNTNyYjNjYXZUcnYzcl81M3J2M3JfNTNyYjNjYfQ

picoCTF{53rv3r\_53rv3r\_53rv3r\_53rv3r\_53rv3r}

Flag: picoCTF{53rv3r\_53rv3r\_53rv3r\_53rv3r\_53rv3r}

### 8. Logon: The factory is hiding things from all of its users. Can you login as Joe and find what they've been looking at?

To start, I tried to log in with any information.

Then, it gave me a message about not having a flag

← → ↻ 🔒 🔑 https://jupiter.challenges.picoctf.org/problem/44573/

Factory Login Home Sign Out

sdf

...

Sign In

I inspected and looked at the cookies and saw that the admin field was set to False, and I manually changed it to True.

Nombre	Valor	Domain
__cf_bm	XEHpXhufvhhhySK.VO0X1znqrBS1cPSj5dsG8ytLkPAk-1700620313-...	.picoctf.org
_ga_BSZF...	GS1.1.1697251701.5.1.1697251748.0.0.0	.picoctf.org
_ga_L6FT...	GS1.2.1700619560.20.1.1700620241.0.0.0	.picoctf.org
_gat	1	.picoctf.org
_ga	GA1.2.1162794626.1693777371	.picoctf.org
_gid	GA1.2.622630720.1700532877	.picoctf.org
admin	False	jupiter.challe...
cf_clearan...	T9PIhCiwBNPvR.Xx.taQ_7GvVuGgwE70yEtu1e.IYs-1700532871-0...	.picoctf.org

I refreshed the page and it gave me the flag.

Factory Login

HomeSign Out

Flag:

picoCTF{th3\_c0nsp1r4cy\_l1v3s\_0c98aacc}

© PicoCTF 2019

Nombre	Valor	Domain	Path	Expires / Max-Age	Tamaño	HttpOnly	Secure	SameSite	Último acceso
__cf_bm	XEHpXhufvhhhySK.VO0X1znqrBS1cPSj5dsG8ytLkPAk-1700620313-0-ATdSHrQxJ+o10O8o8CBH2tEURV0THK058LyNRJm...	.picoctf.org	/	Wed, 22 Nov 2023 0...	152	true	true	None	Wed, 22 Nov 2023 0...
_ga_BSZF...	GS1.1.1697251701.5.1.1697251748.0.0.0	.picoctf.org	/	Mon, 13 Oct 2025 0...	51	false	false	None	Wed, 22 Nov 2023 0...
_ga_L6FT...	GS1.2.1700619560.20.1.1700620241.0.0.0	.picoctf.org	/	Fri, 21 Nov 2025 02...	52	false	false	None	Wed, 22 Nov 2023 0...
_gat	1	.picoctf.org	/	Wed, 22 Nov 2023 0...	5	false	false	None	Wed, 22 Nov 2023 0...
_ga	GA1.2.1162794626.1693777371	.picoctf.org	/	Thu, 20 Nov 2025 02...	30	false	false	None	Wed, 22 Nov 2023 0...
_gid	GA1.2.622630720.1700532877	.picoctf.org	/	Wed, 22 Nov 2023 0...	30	false	false	None	Wed, 22 Nov 2023 0...
cf_clearance	T9PIhCiwBNPvR.Xx.taQ_7GvVuGgwE70yEtu1e.IYs-1700532871-0-1-1e81379a.bca3466.6a7497d8-0.2.1700532871	.picoctf.org	/	Wed, 20 Nov 2024 0...	111	false	true	None	Wed, 22 Nov 2023 0...

Flag: picoCTF{th3\_c0nsp1r4cy\_l1v3s\_0c98aacc}

9. Search source: The developer of this website mistakenly left an important artifact in the website source, can you find it?

To begin, I entered the page and I inspected it.



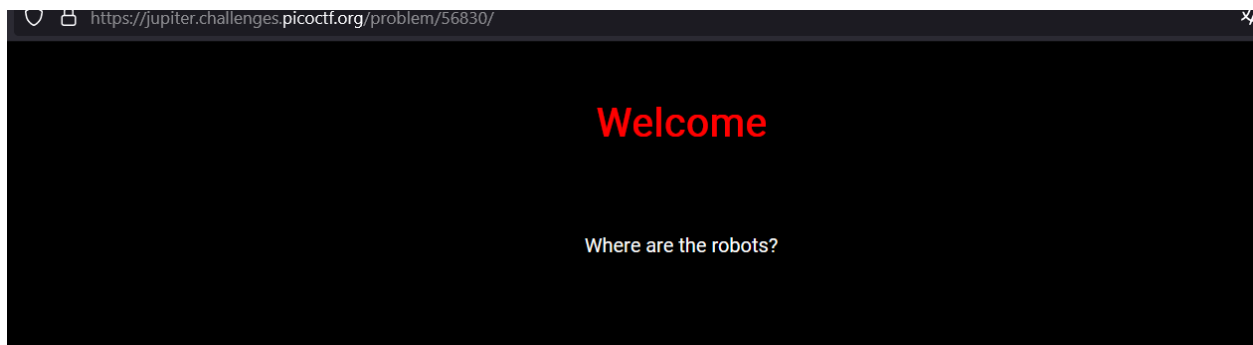
Inside the source code, I found many files and inside the style.css I found the flag.

```
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5   <!-- basic -->
6   <meta charset="utf-8">
7   <meta http-equiv="X-UA-Compatible" content="IE=edge">
8   <!-- mobile metas -->
9   <meta name="viewport" content="width=device-width, initial-scale=1">
10  <meta name="viewport" content="initial-scale=1, maximum-scale=1">
11  <!-- site metas -->
12  <title>flexed</title>
13  <meta name="keywords" content="">
14  <meta name="description" content="">
15  <meta name="author" content="">
16  <!-- bootstrap css -->
17  <link rel="stylesheet" href="css/bootstrap.min.css">
18  <!-- owl css -->
19  <link rel="stylesheet" href="css/owl.carousel.min.css">
20  <!-- style css -->
21  <link rel="stylesheet" href="css/style.css">
22  <!-- responsive -->
23  <link rel="stylesheet" href="css/responsive.css">
24  <!-- awesome fontfamily -->
25  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
```

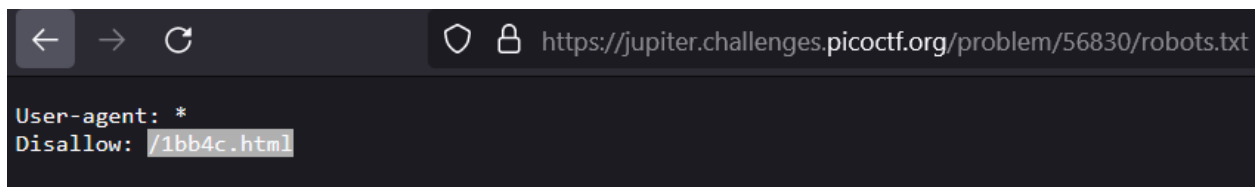
```
color: #000;  
line-height: 18px;  
}  
/** banner_main picoCTF{1nsp3t10n_0f_w3bpag3s_587d12b8} **/  
.carousel-indicators li {  
width: 20px;  
height: 20px;  
border-radius: 11px;  
background-color: #070000;  
}
```

## 10. where are the robots: Can you find the robots?

To begin, we see the initial screen. And it tells us about robots, so by intuition I entered the robots.txt address



When I enter robots.txt it gives me a path to disallow.



I enter the route given above and it gives me the flag.

org/problem/56830/1bb4c.html

Guess you found the robots  
picoCTF{ca1cu1at1ng\_Mach1n3s\_1bb4c}

Flag: picoCTF{ca1cu1at1ng\_Mach1n3s\_1bb4c}