

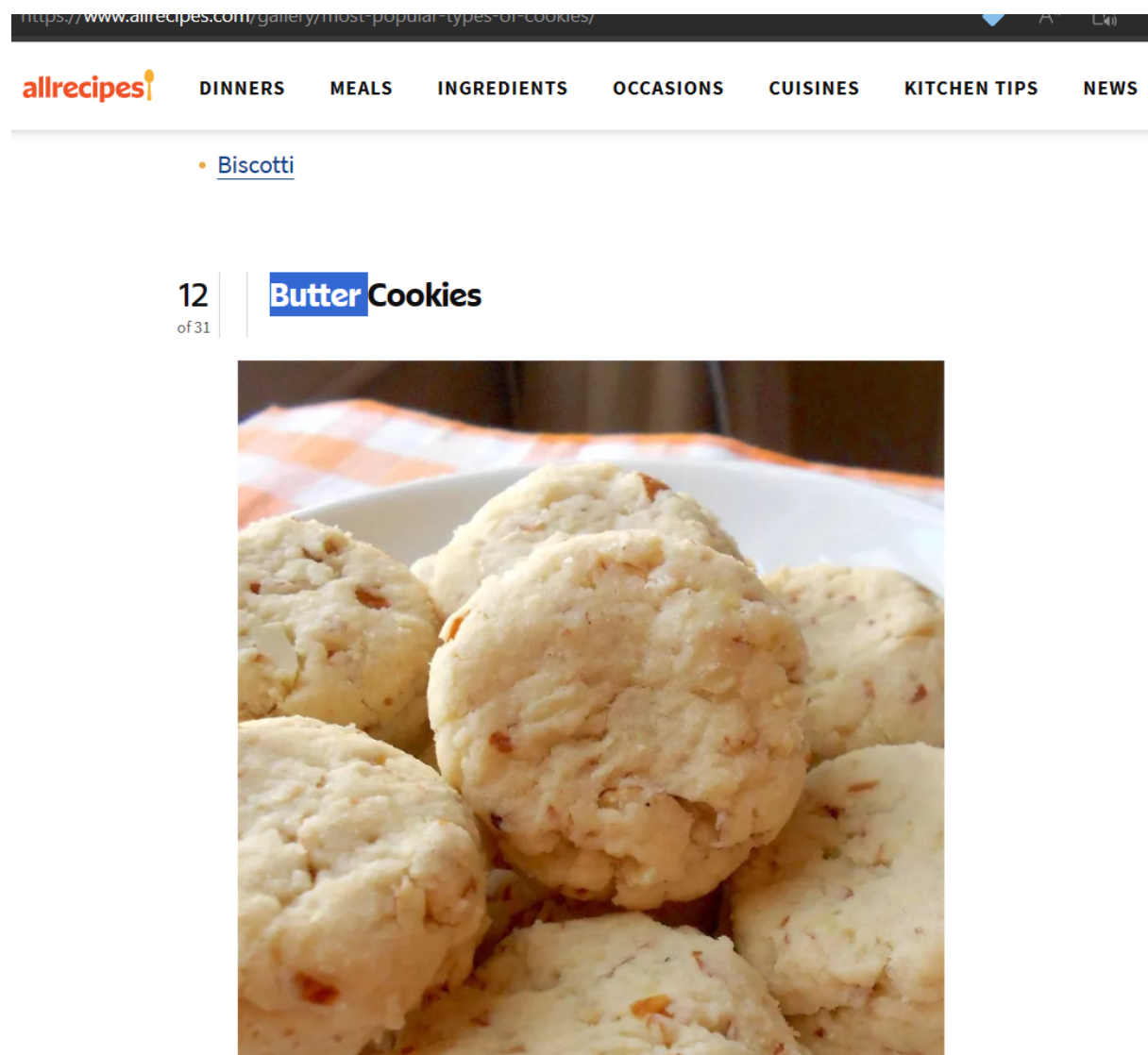
Homework 3

Nicolas Romero

Web Exploitation

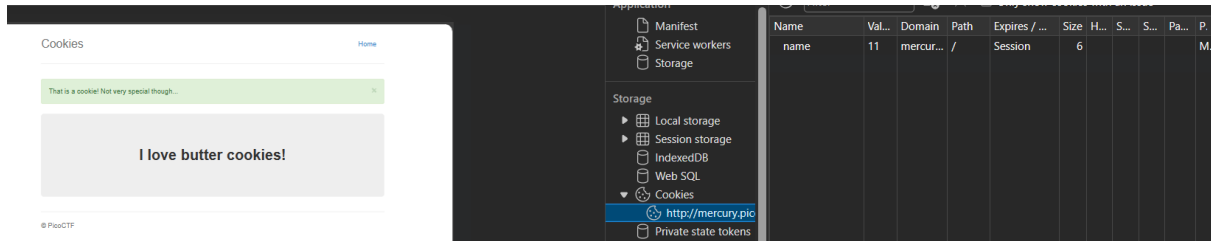
1. Cookies

Snickerdoodle is a real cookie, so i search a top of the best cookies and their names

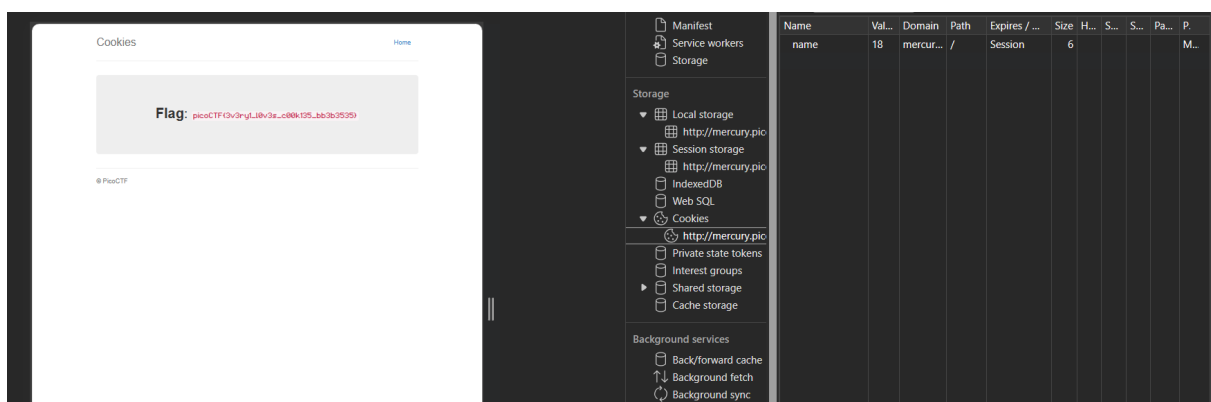


Butter cookies has a value 11, so we can try a max num of cookies, first i put 40 as a value and the page gave me error then 30 and gave me an error, then 25 and gave me a cookie

then the interval is between [25 to 30] trying I find that the final cookie is 28 so we have [0 to 28] = 29 cookies



The trying 1 by 1 value of cookie the number 18 was de flag



Flag: picoCTF{3v3ry1_l0v3s_c00k135_bb3b3535}

2. Scavenger Hunt

We can open the code so we can find the first part of the flag, the wne have a hint that says:

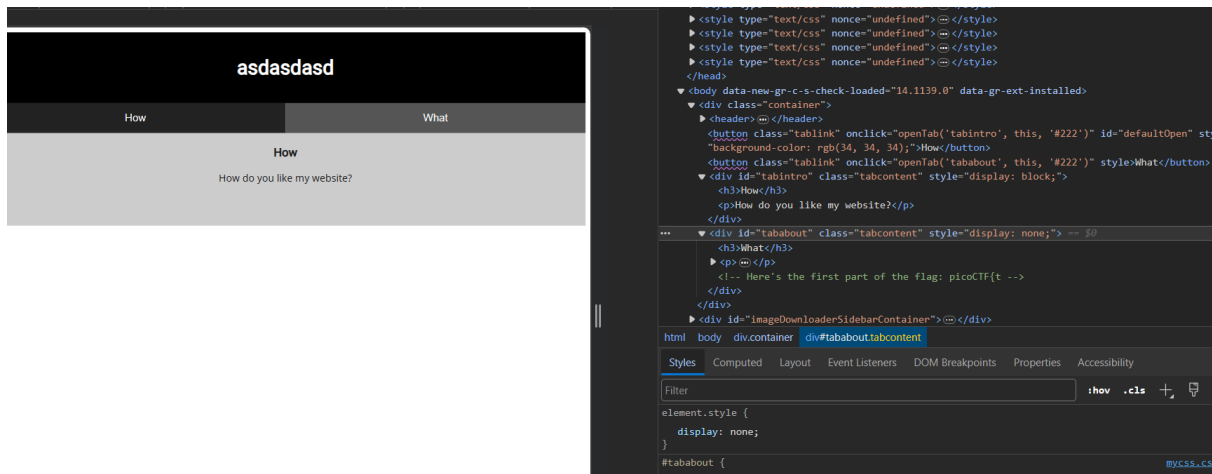
What

I used these to make this site:

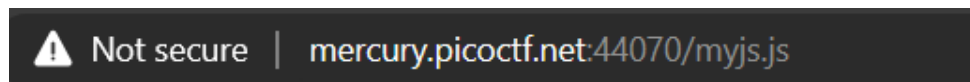
HTML

CSS

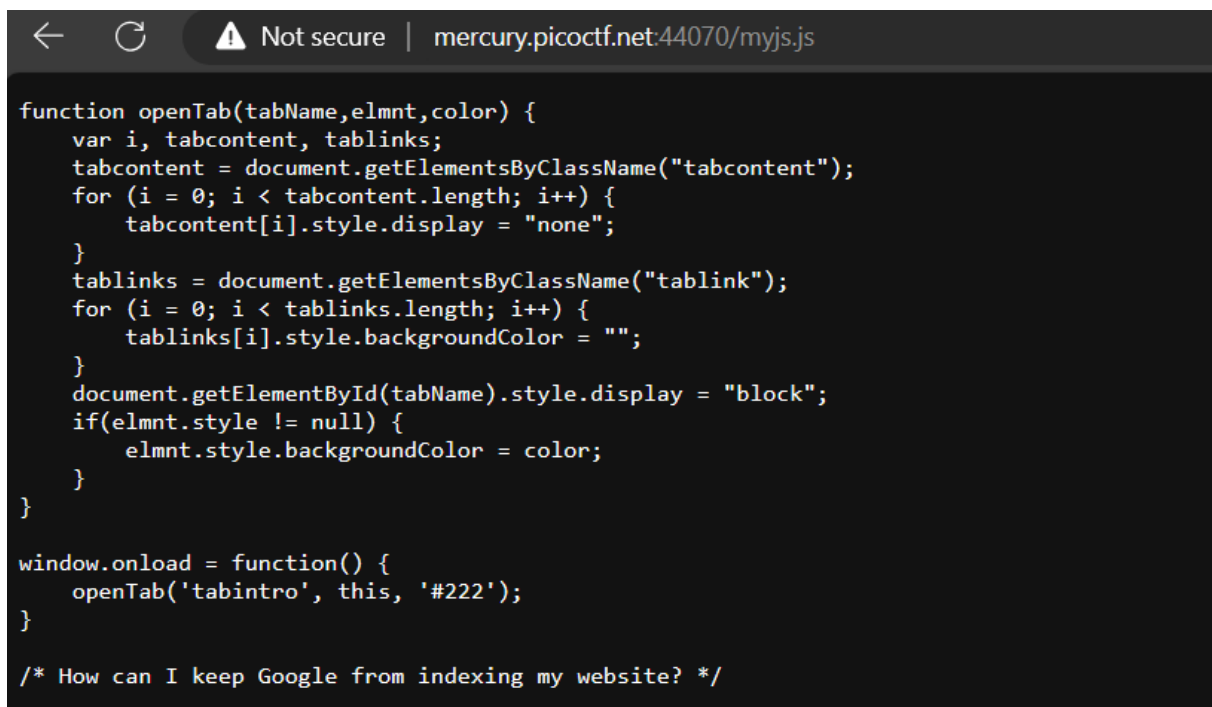
JS (JavaScript)



So we find the first part of the flag in the HTML file, so probably we can find the other parts in the others files of the page



We can change the directory and see the files changing the URL direction so this is the JS content



there's nothing in JS except a hint that says "How can I keep Google from indexing my website"

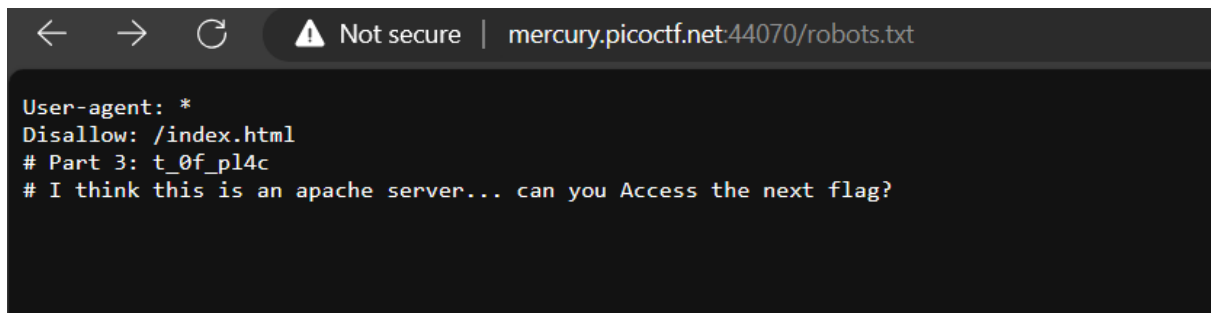
If We know how to positioning a website we can think in two files:

sitemap

robots.txt

The sitemap tell us which pages are part of my website to index this pages together in a search

The robots.txt tell the google scraping bots which parts of the website they can access for indexing content into the web



```
← → ↻ ⚠ Not secure | mercury.picoctf.net:44070/robots.txt

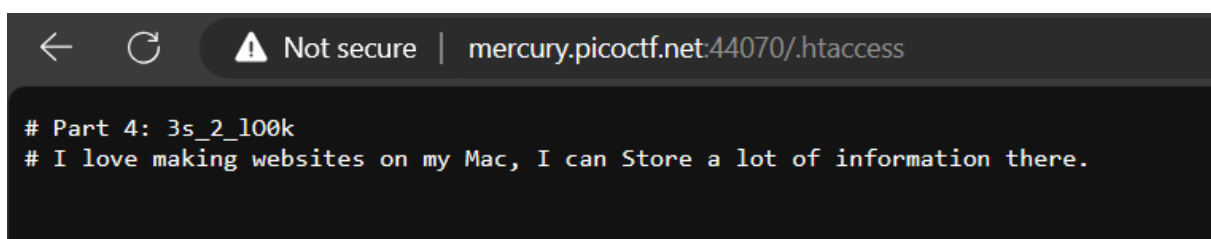
User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

in robots.txt we get the part 3 of the flag

The next hint says that “apache server” “Access” investigating the documentation for apache servers there's a command that we can get into the files using htaccess

Apache .htaccess files allow users to configure directories of the web server they control without modifying the main configuration file.

While this is useful it's important to note that using .htaccess files slows down Apache, so, if you have access to the main server configuration file (which is usually called httpd.conf), you should add this logic there under a Directory block.



```
← ↻ ⚠ Not secure | mercury.picoctf.net:44070/.htaccess

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

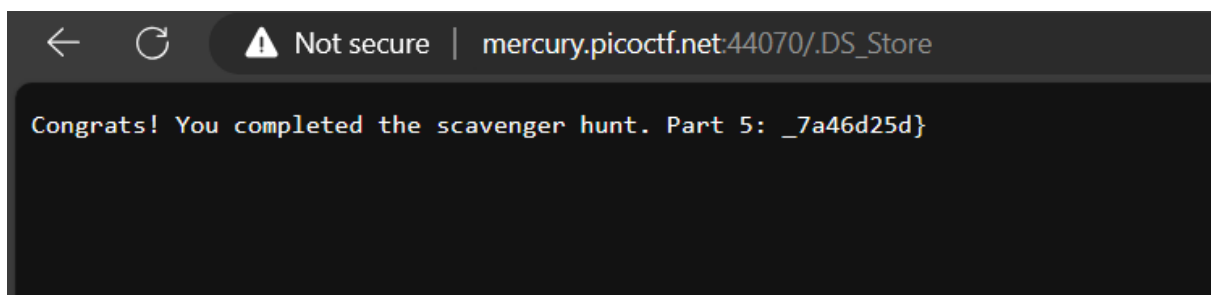
then we get the part 4 of the flag

Now we get the next hint: # I love making websites on my Mac, I can Store a lot of information there.

The **.DS_Store file** you may see in folders on your Mac is generated automatically. It is created by Finder in browser directories on your storage drives. The .DS_Store files contain information about your system's configuration and contain data that tells your Mac how to display the files in those folders.

.DS_Store File on Mac - What is it and How to Delete? - Cyclonis

In MAC there a DS_Store file so we can acces



in this file is the part 5 of the flag, just we need the second part

So now We can open css content

```
← ↻ ⚠ Not secure | mercury.picoctf.net:44070/mycss.css
/*
header {
  background-color: black;
  padding: 1em;
  color: white;
  clear: left;
  text-align: center;
}

body {
  font-family: Roboto;
}

h1 {
  color: white;
}

p {
  font-family: "Open Sans";
}

.tablink {
  background-color: #555;
  color: white;
  float: left;
  border: none;
  outline: none;
  cursor: pointer;
  padding: 14px 16px;
  font-size: 17px;
  width: 50%;
}

.tablink:hover {
  background-color: #777;
}

.tabcontent {
  color: #111;
  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 */

```

In the Css content is the second part of flag

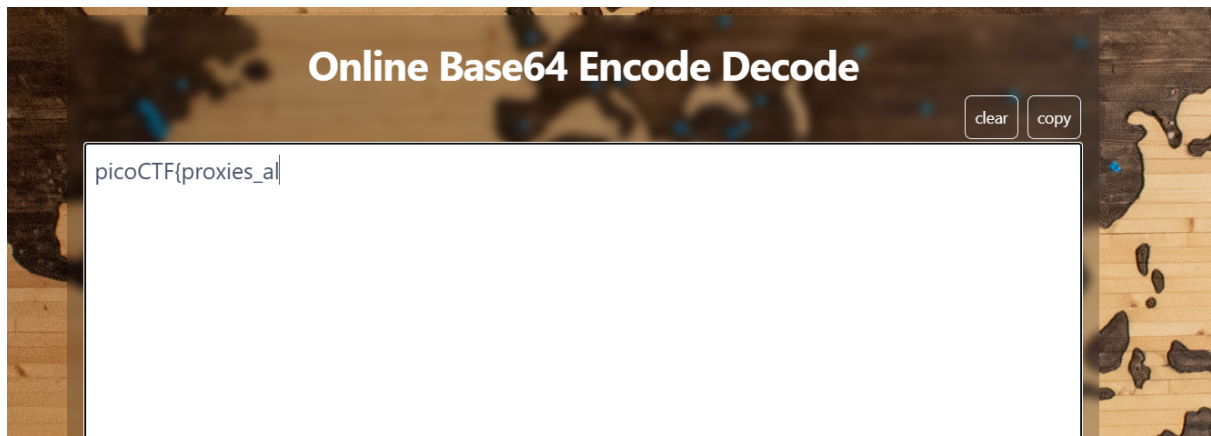
Flag: picoCTF{th4ts_4_l0t_of_pl4c3s_2_l00k_7a46d25d}

3. Find me

If we capture the network from this page we get a file with this id:

<http://saturn.picoctf.net:55629/next-page/id=cGljb0NURntwcm94aWVzX2Fs>

it is encoded so we use a base64 decoder

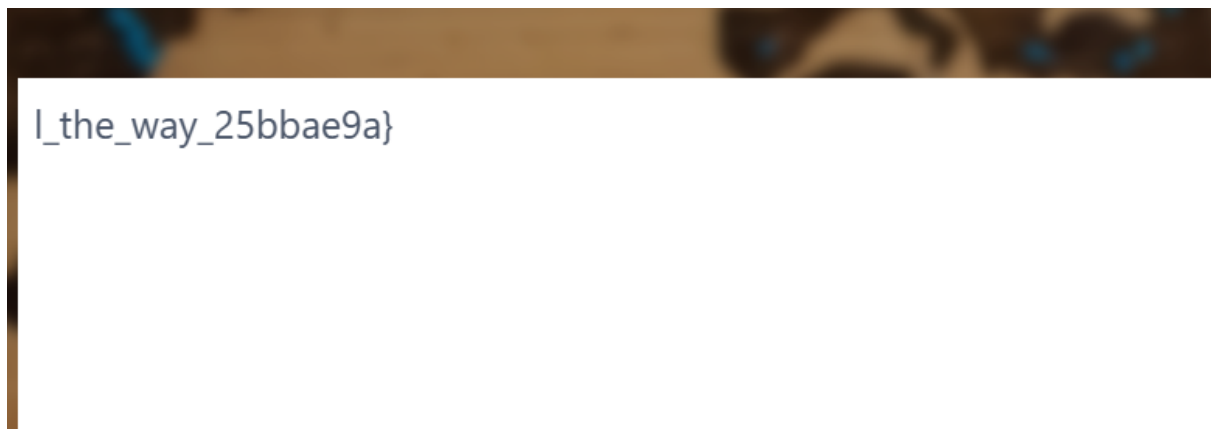


First part: *picoCTF{proxies_al*

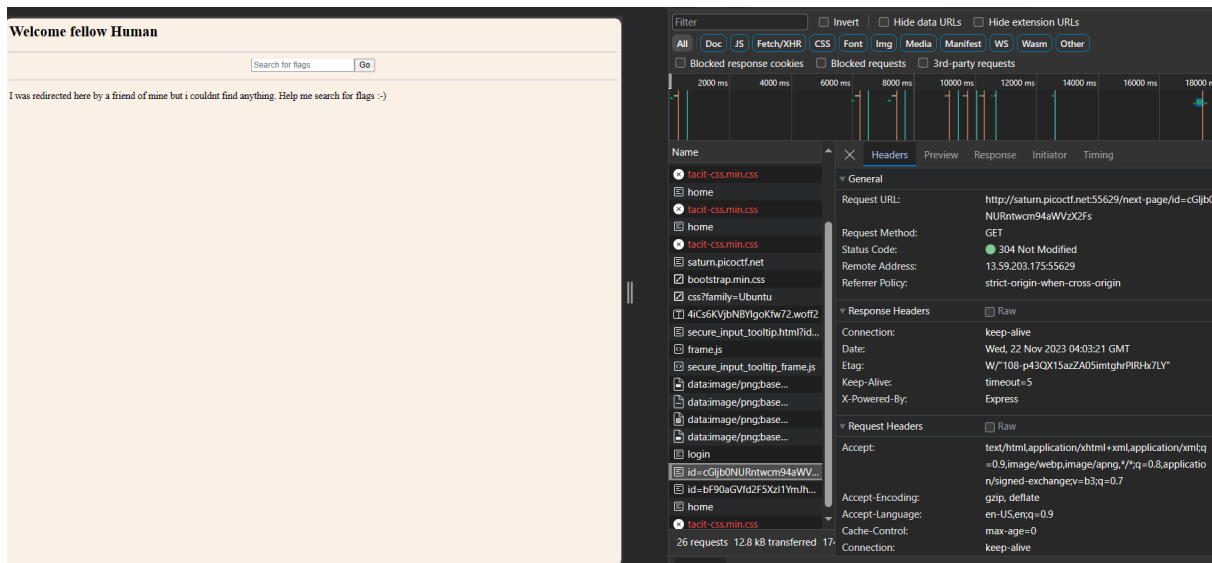
And We get a part of the flag but there is another id page:

<http://saturn.picoctf.net:55629/next-page/id=bF90aGVfd2F5Xzl1YmJhZTlhQ==>

Decoded we got this second part of the flag:



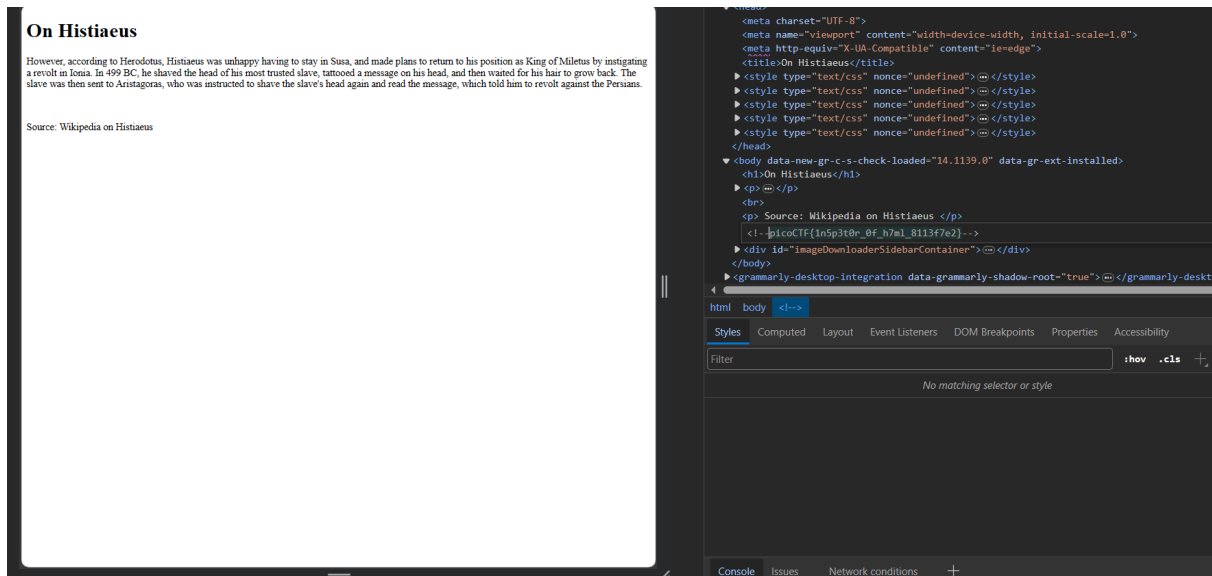
second part: *l_the_way_25bbae9a}*



Flag: picoCTF{proxies_all_the_way_25bbae9a}

4. Inspect HTML

the flag is in an HTML comment



Flag: picoCTF{1n5p3t0r_0f_h7m1_8113f7e2}

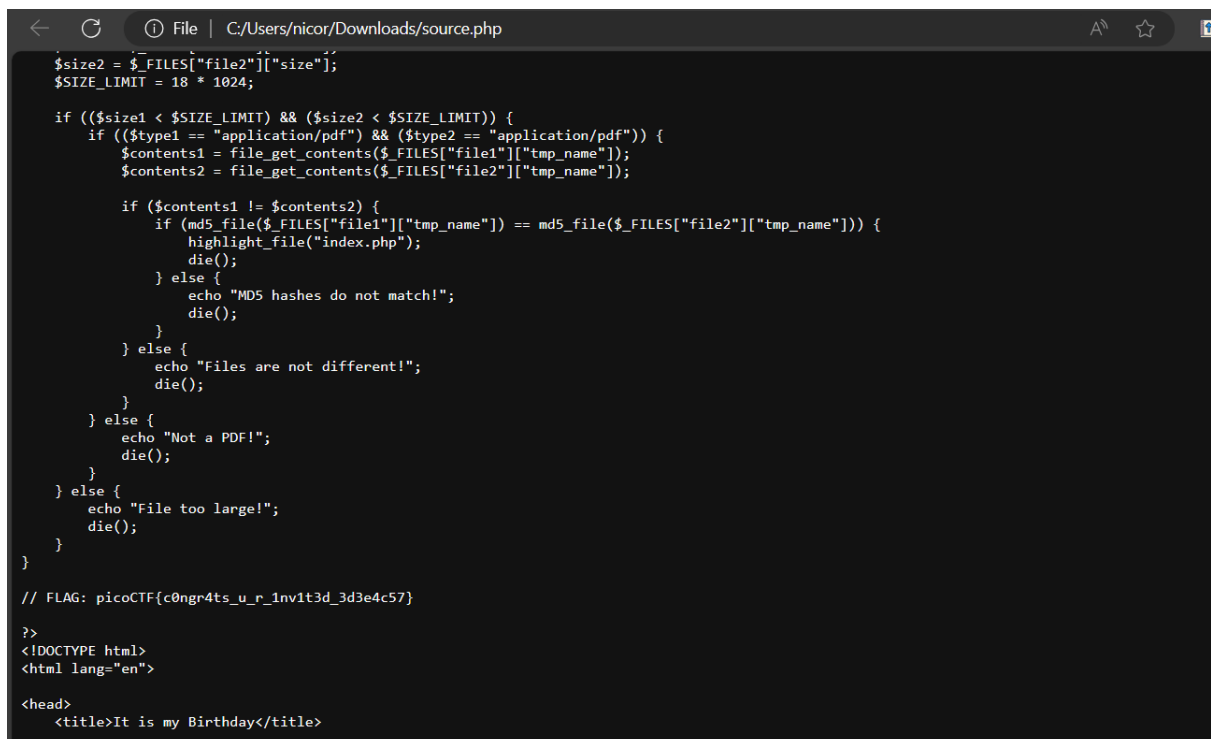
5. It's my birthday

We upload a files and redirect to



but if we download the page with

```
wget --mirror --convert-links --html-extension --wait=2 -o log
```

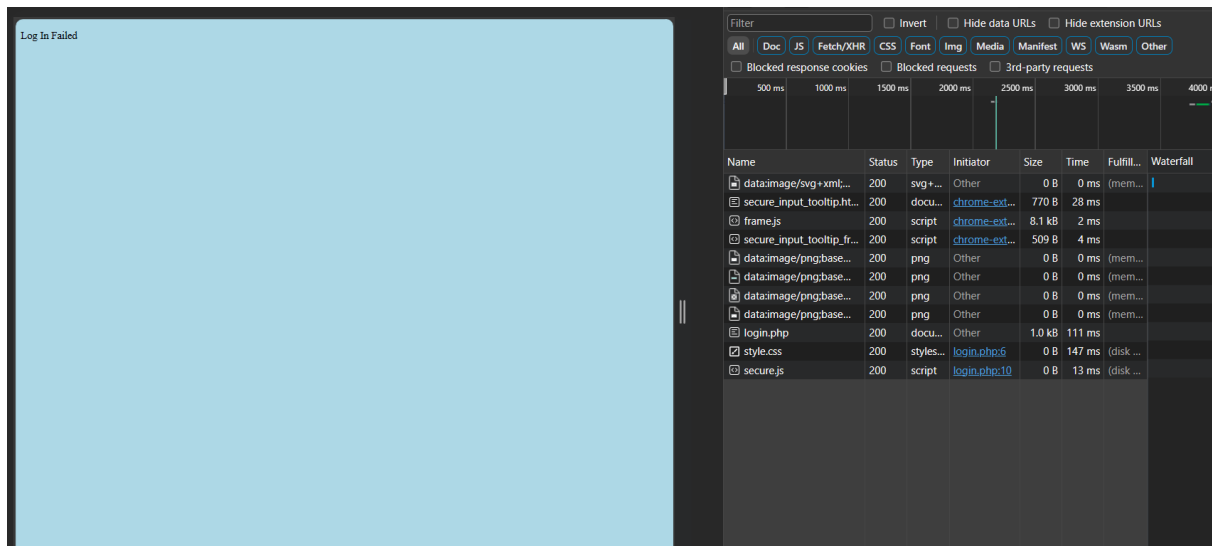


We find the flag at php source

Flag: picoCTF{c0ngr4ts_u_r_1nv1t3d_3d3e4c57}

6. Local Authority

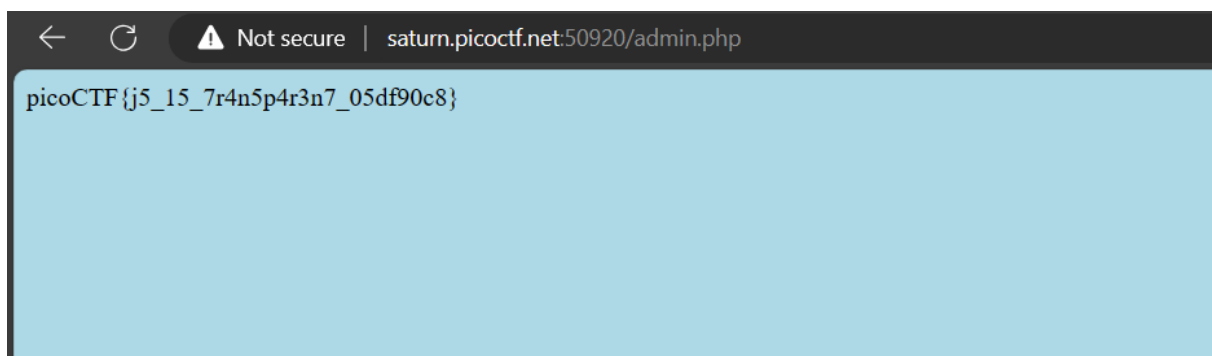
A hint says "How is the password checked on this website?" so if we analyze the network



We can see a file named as secure.js if we open the file



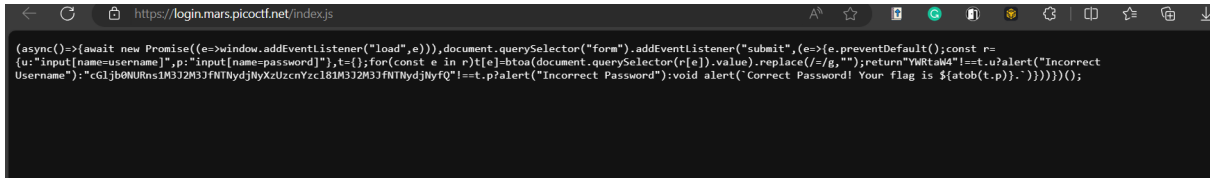
We can see how the page check the password and user in a simple way, so if we log in with that credentials



We find the flag

Flag: picoCTF{j5_15_7r4n5p4r3n7_05df90c8}

7. Login



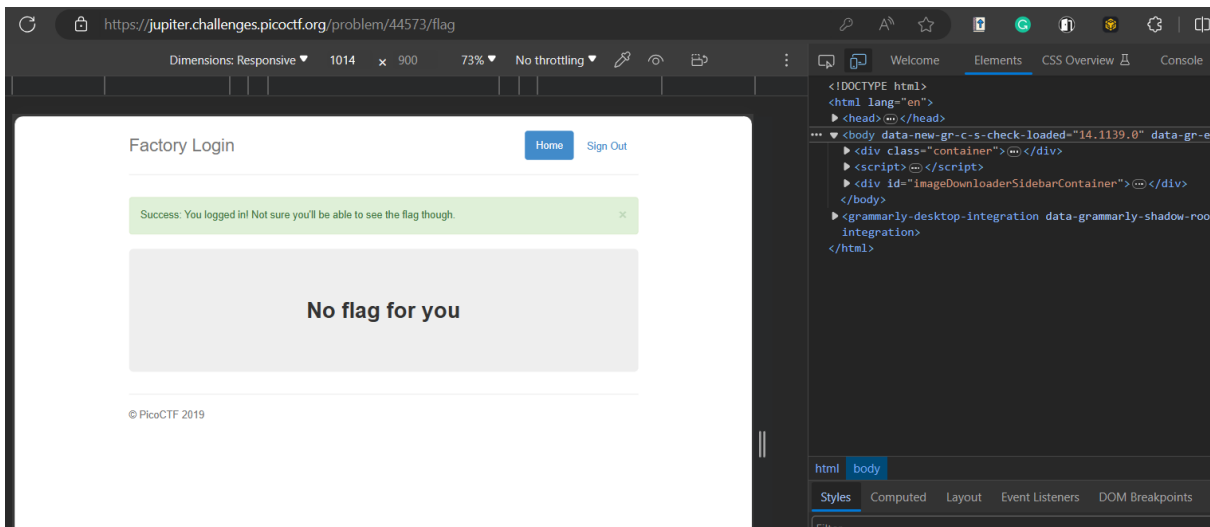
We can see de index.js and see the function atob that is a call for another function in the same code that is btoa and atob is the reverse for the code that te file give us if we decode

cG1jb0NURns1M3J2M3JfNTNyYjNyXzUzcnYzc181M3J2M3JfNTNyYjNyfQ
we get the flag

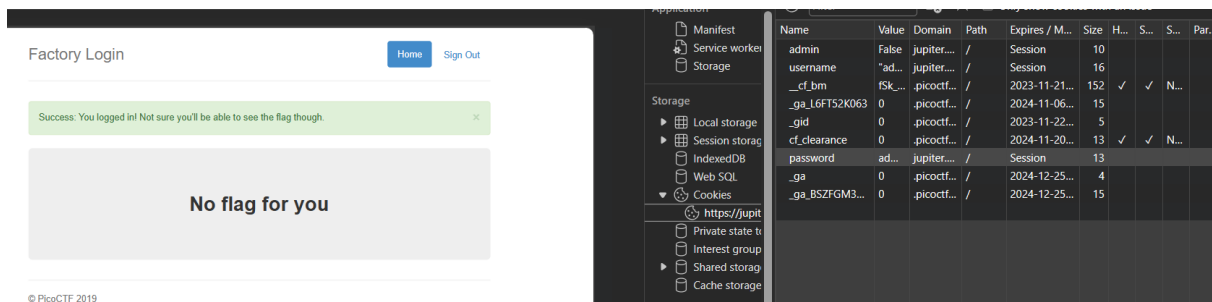
Flag: picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}

8. Logon

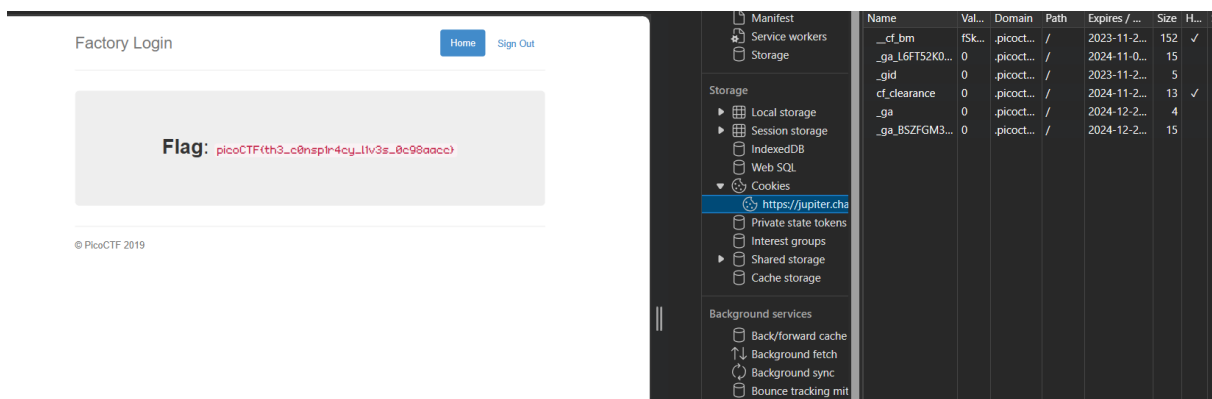
A hint in PicoCTF says that only verify the password for Joe, so If we put Joe as a username we got an error for password but if we log in as another user like: Admin admin we can access to the page



Then if we are inside the site, what happend if we see the cookies that contains the login credentials

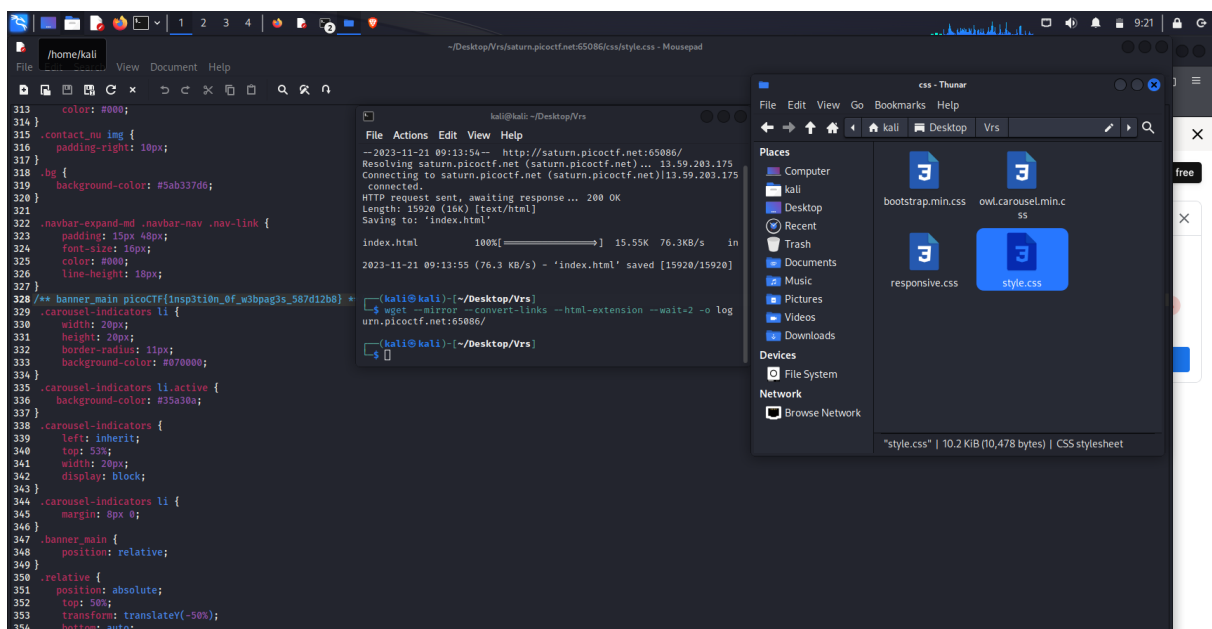


So I can change the user log from Admin to Joe and convert the new User to Admin changing Admin: False → Admin True, recharge the page and we got the flag



Flag: picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}

9. Search source



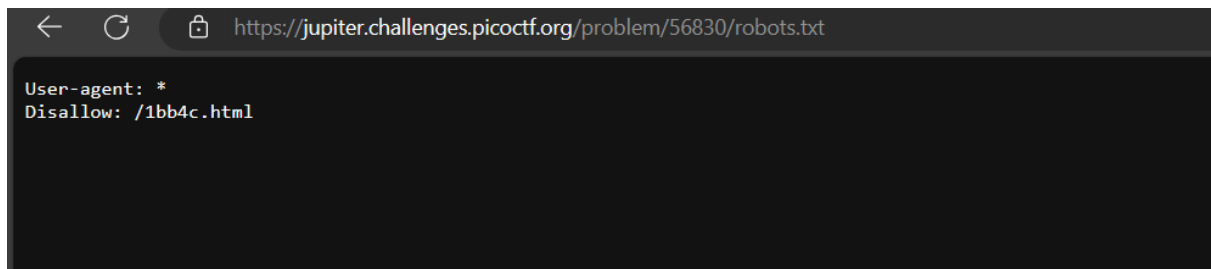
I use Kali linux as a tool to download all the documents and files [mirroring the entire website] to look through the code, in the folder CSS, then in the file style.CSS we can find the flag also, I use the next code to mirror the page into my local machine

```
wget --mirror --convert-links --html-extension --wait=2 -o log http://saturn.picoctf.net:65086/
```

Flag: picoCTF{1nsp3ti0n_of_w3bpag3s_587d12b8}

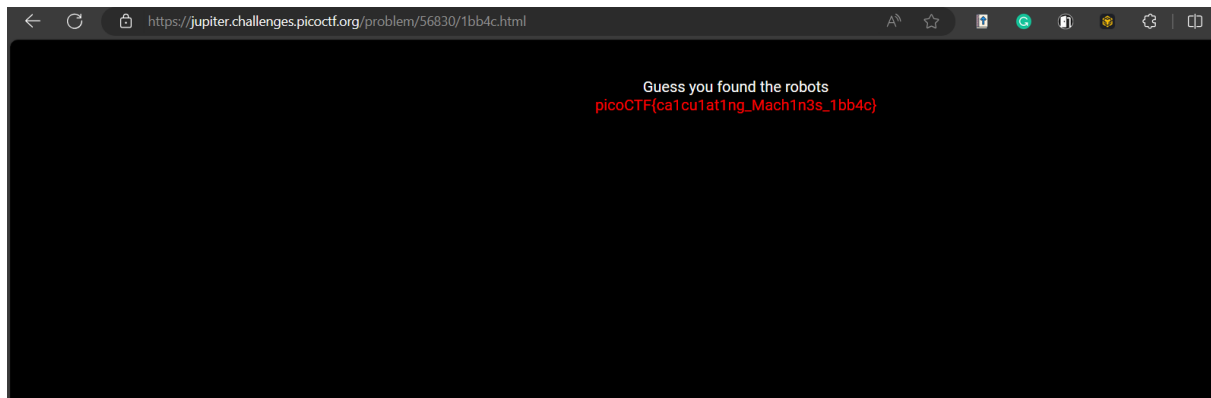
10. Whe are de robots

We have the first hint that says Where are the robots? then We can think in the robots.txt file, so if we go to that redirection



We got that a page is disallow for index so now we can go to

[/1bb4c.html](#)



and finally We find the flag

Flag: picoCTF{ca1cu1at1ng_Mach1n3s_1bb4c}