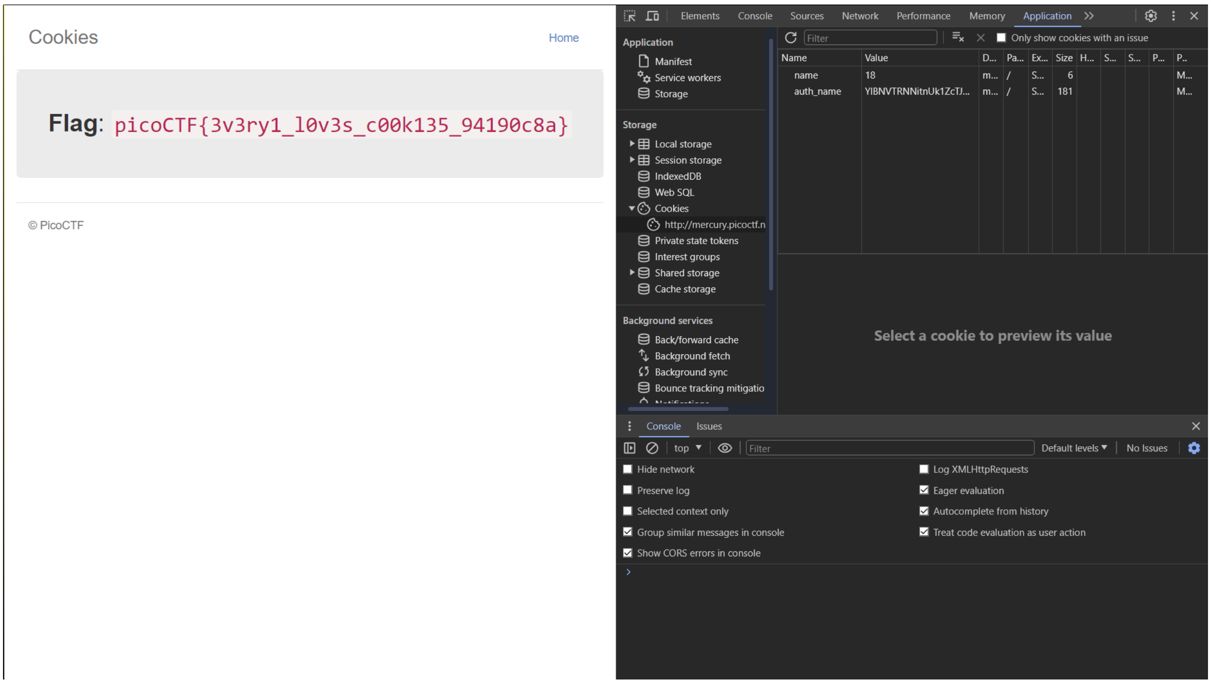
Home Work #2
PicoCTFSolutions

Juan Antonio Romero
00212936

Cookies:

The name of the exercise and the hints suggest I need to go and check for the cookies on this page.I found that had a name so basically when I wrote snickerdoodle the name went to 1 so then I tried modifying this number and I got different types of cookies but the page said it didn't liked that cookie enough so I kept trying until I got to the name number 18 and I got the pico ctf code

`picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}`



Cookies

Flag: picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}

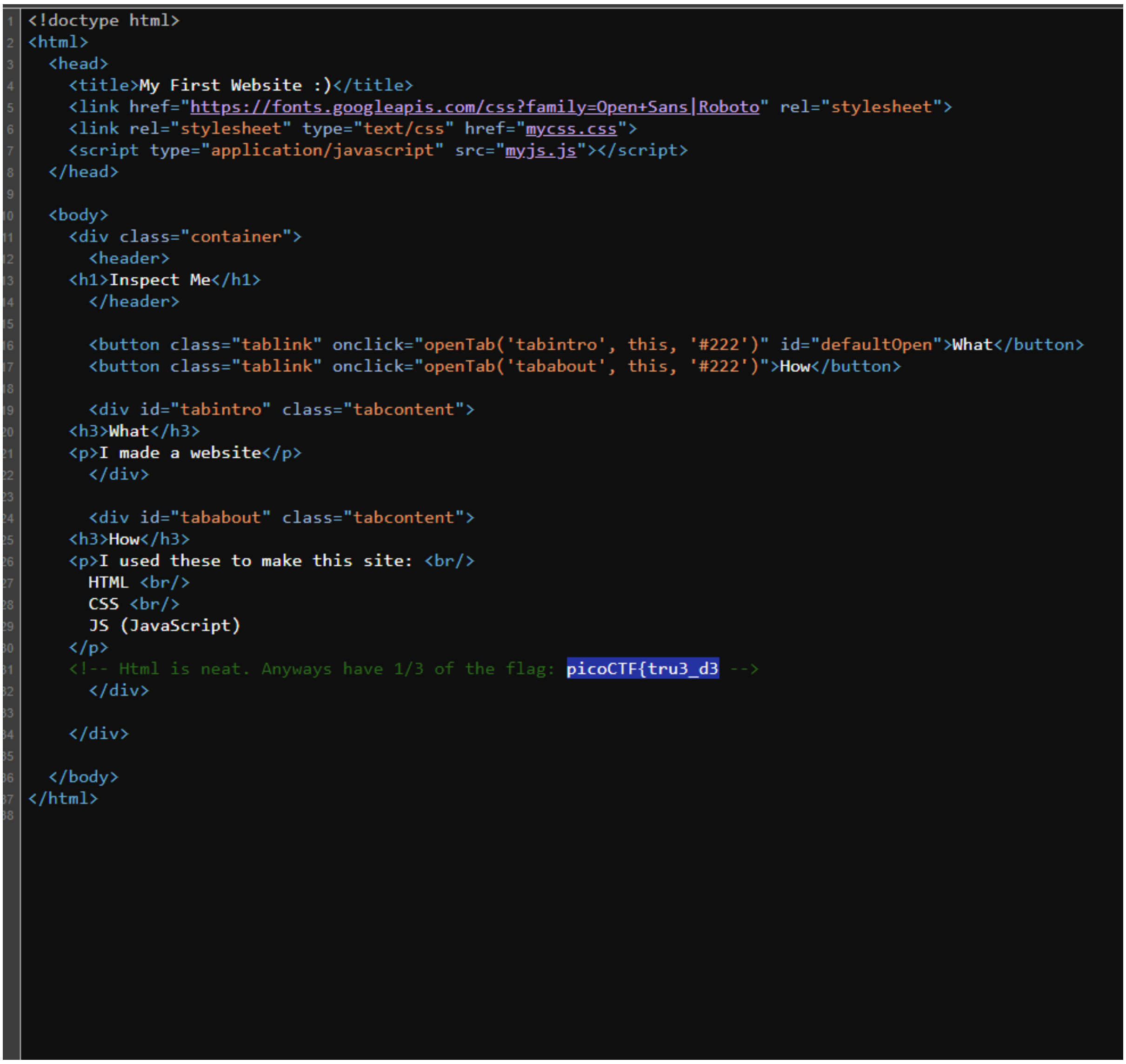
© PicoCTF

Name	Value	D...	Pa...	Ex...	Size	H...	S...	S...	P...	P..
name	18	m...	/	S...	6					M...
auth_name	YIBNVTRNNitnUk1ZcTJ...	m...	/	S...	181					M...

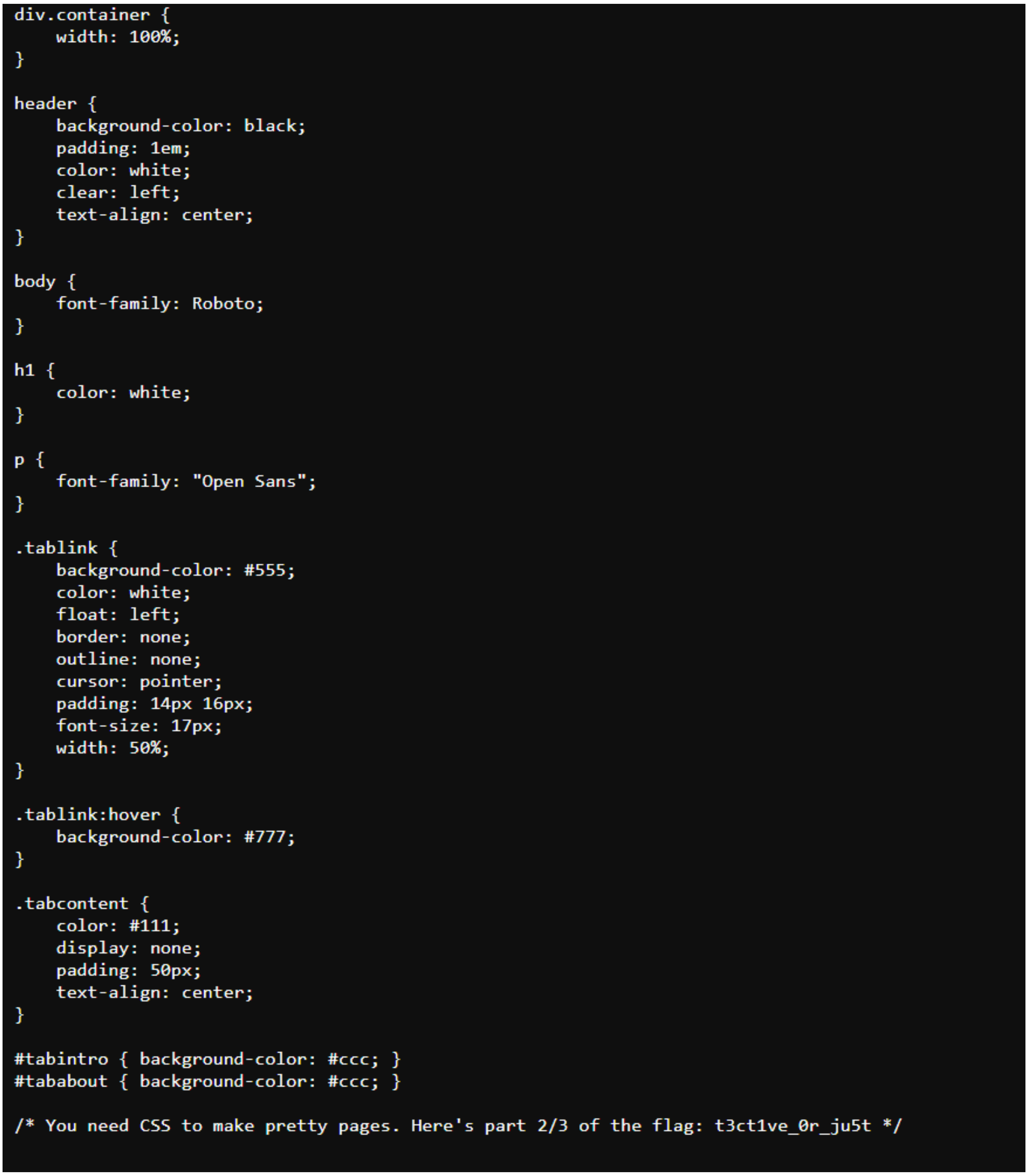
Select a cookie to preview its value

Inp3ct0r:

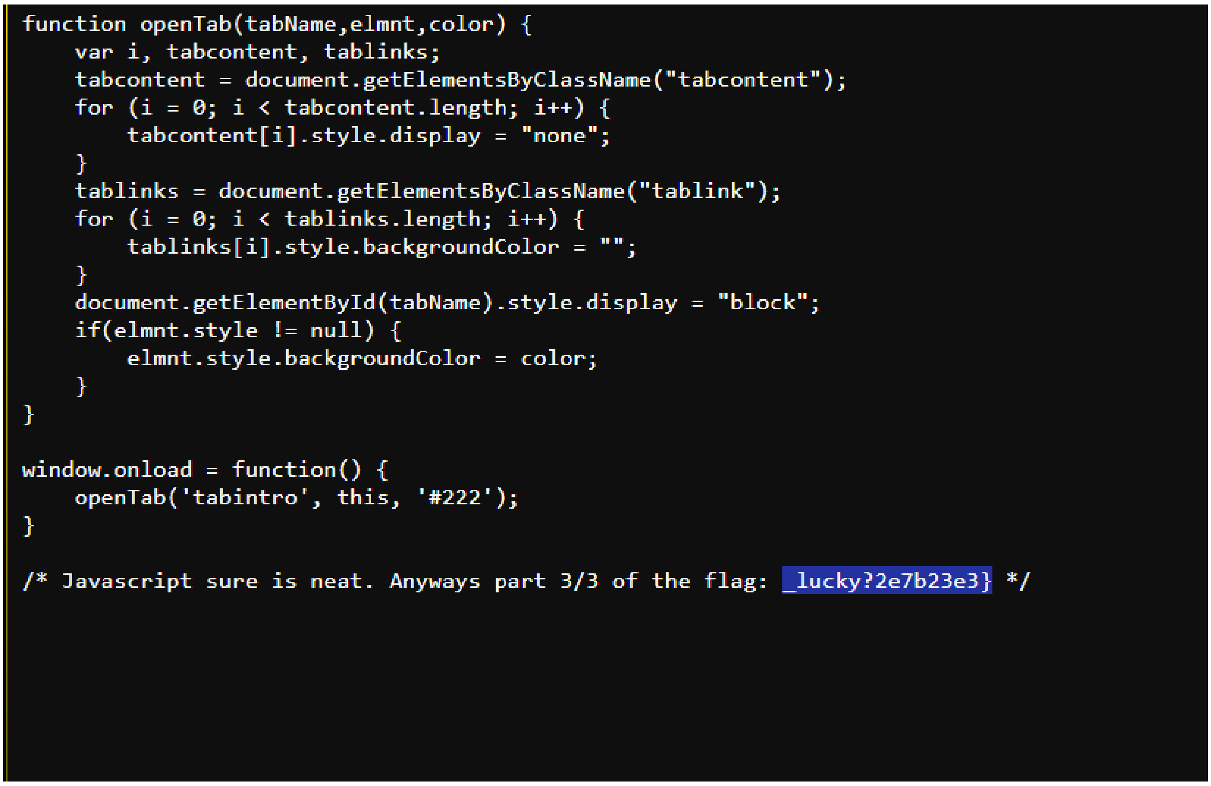
In this problem we basically just need to inspect some web pages and follow some steps. First I inspected the first page and searching I got one part of the code picoCTF{tru3_d3.Then I started opening some archives and I found the second part of the code in the archive mycss that is t3ct1ve_0r_ju5t .In the third archive myjs I found the las part of the code that is _lucky?2e7b23e3}



```
<!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>
    <h1>Inspect Me</h1>
      </header>

      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen">What</button>
      <button class="tablink" onclick="openTab('tababout', this, '#222')">How</button>

      <div id="tabintro" class="tabcontent">
    <h3>What</h3>
    <p>I made a website</p>
      </div>

      <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>

  </body>
</html>
```



```
div.container {
    width: 100%;
}

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; }

/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```



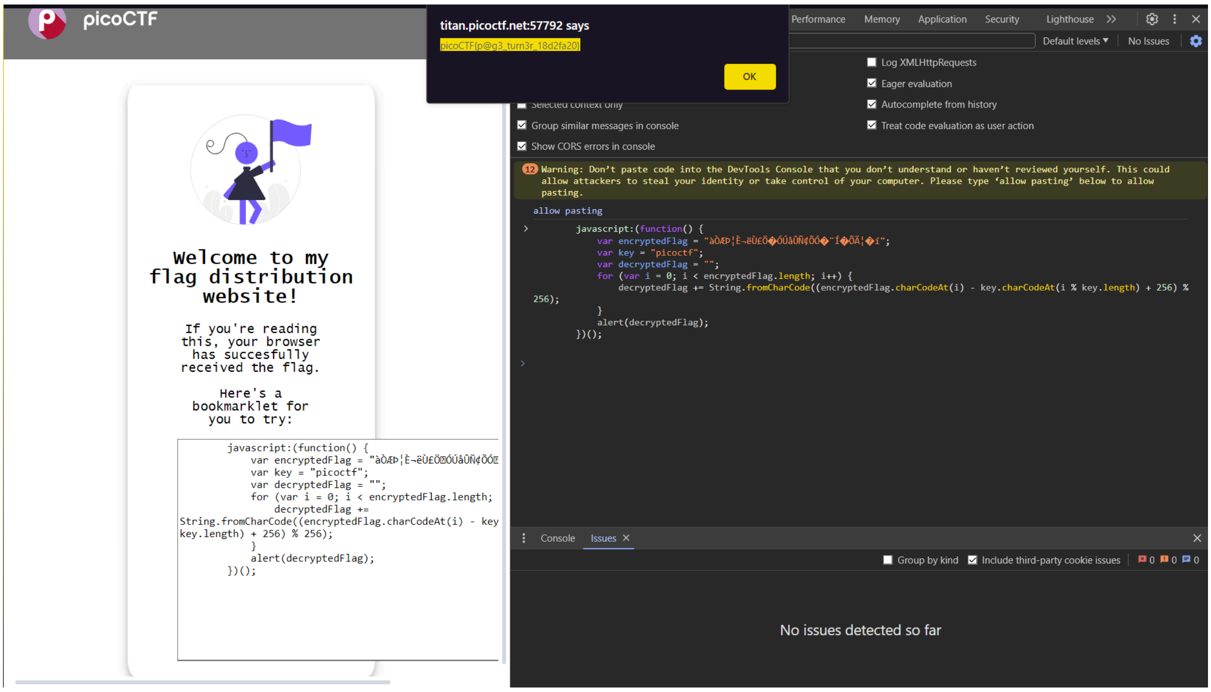
```
function openTab(tabName,elmnt,color) {
    var i, tabcontent, tablinks;
    tabcontent = document.getElementsByClassName("tabcontent");
    for (i = 0; i < tabcontent.length; i++) {
        tabcontent[i].style.display = "none";
    }
    tablinks = document.getElementsByClassName("tablink");
    for (i = 0; i < tablinks.length; i++) {
        tablinks[i].style.backgroundColor = "";
    }
    document.getElementById(tabName).style.display = "block";
    if(elmnt.style != null) {
        elmnt.style.backgroundColor = color;
    }
}

window.onload = function() {
    openTab('tabintro', this, '#222');
}

/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?2e7b23e3} */
```

Scavenger Hunt:

Again this exercise starts by inspecting the page, I got the first part of the flag that is picoCTF{t. Then I went into another archive mycss and got the second part that is h4ts_4_l0. The I opened myjs and got a hint that said that basically I needed to make google quit indexing. So I changed the indexing to none and it gave me the third part t_0f_pl4c. Then I got a hint of an apache archive and when I opened it I got the fourth part that is 3s_2_100k.

BookMarklet:

The first thing I did for this exercise was to inspect the contents. Then I realized that this function copied to the clipboard so what I did was very simple. I just went into the console of my developer tool in the web page and inserted the function. One I inserted the function into the console I got the code that was = picoCTF{p@ge_turn3r_18d2fa20}



Welcome to my flag distribution website!

If you're reading this, your browser has succesfully received the flag.

Here's a bookmarklet for you to try:

```
        javascript:(function() {
            var encryptedFlag = "àÒÆÞ¦È¬ëÙ£ÖΏÓÚåÛÑ¢ÕÓΏ
            var key = "picoctf";
            var decryptedFlag = "";
            for (var i = 0; i < encryptedFlag.length;
                decryptedFlag +=
String.fromCharCode((encryptedFlag.charCodeAt(i) - key
key.length) + 256) % 256);
            }
            alert(decryptedFlag);
        })();
```

titan.picoctf.net:57792 says

picoCTF{p@g3_turn3r_18d2fa20}

□ Log XMLHttpRequests
☑ Eager evaluation
☑ Autocomplete from history
☑ Treat code evaluation as user action
□ Selected context only
☑ Group similar messages in console
☑ Show CORS errors in console

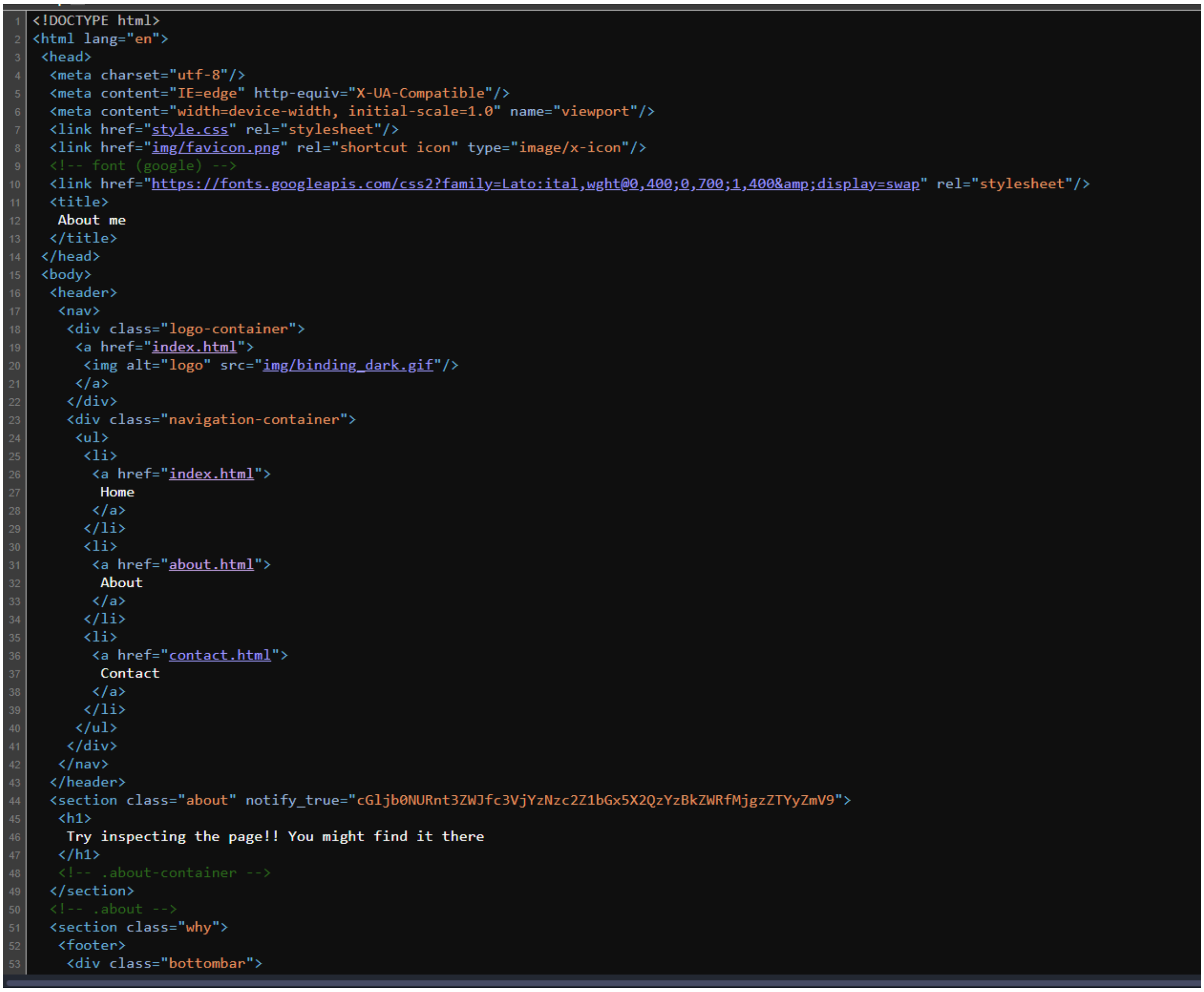
```
12 Warning: Don’t paste code into the DevTools Console that you don’t understand or haven’t reviewed yourself. This could
   allow attackers to steal your identity or take control of your computer. Please type ‘allow pasting’ below to allow
   pasting.
 allow pasting
>        javascript:(function() {
            var encryptedFlag = "àÒÆÞ¦È¬ëÙ£Ö�ÓÚåÛÑ¢ÕÓ�¨Í�ÕÄ¦�í";
            var key = "picoctf";
            var decryptedFlag = "";
            for (var i = 0; i < encryptedFlag.length; i++) {
                decryptedFlag += String.fromCharCode((encryptedFlag.charCodeAt(i) - key.charCodeAt(i % key.length) + 256) %
 256);
            }
            alert(decryptedFlag);
        })();

>
```

□ Group by kind ☑ Include third-party cookie issues 0 0 0

No issues detected so far

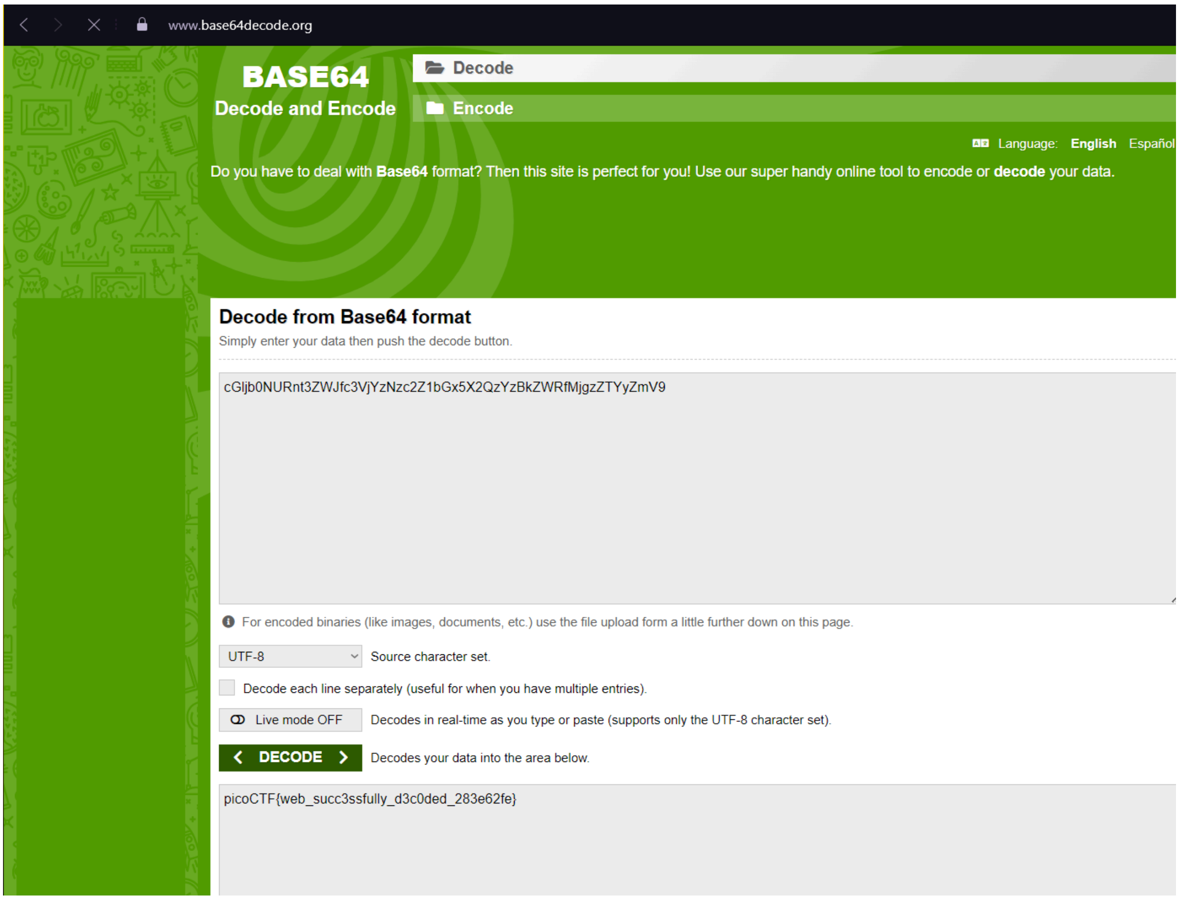
Web Decode:

The first thing I did was to inspect all of the different pages that were available, about, home and the contact page. I didn't found anything in the home and contact page but in the about I found a code.



```html
1  <!DOCTYPE html>
2  <html lang="en">
3   <head>
4    <meta charset="utf-8"/>
5    <meta content="IE=edge" http-equiv="X-UA-Compatible"/>
6    <meta content="width=device-width, initial-scale=1.0" name="viewport"/>
7    <link href="style.css" rel="stylesheet"/>
8    <link href="img/favicon.png" rel="shortcut icon" type="image/x-icon"/>
9    <!-- font (google) -->
10   <link href="https://fonts.googleapis.com/css2?family=Lato:ital,wght@0,400;0,700;1,400&amp;display=swap" rel="stylesheet"/>
11   <title>
12    About me
13   </title>
14  </head>
15  <body>
16   <header>
17    <nav>
18     <div class="logo-container">
19      <a href="index.html">
20       <img alt="logo" src="img/binding_dark.gif"/>
21      </a>
22     </div>
23     <div class="navigation-container">
24      <ul>
25       <li>
26        <a href="index.html">
27         Home
28        </a>
29       </li>
30       <li>
31        <a href="about.html">
32         About
33        </a>
34       </li>
35       <li>
36        <a href="contact.html">
37         Contact
38        </a>
39       </li>
40      </ul>
41     </div>
42    </nav>
43   </header>
44   <section class="about" notify_true="cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfMjgzZTYyZmV9">
45    <h1>
46     Try inspecting the page!! You might find it there
47    </h1>
48    <!-- .about-container -->
49   </section>
50   <!-- .about -->
51   <section class="why">
52    <footer>
53     <div class="bottombar">
```

In line 44 there is the code
cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfMjgzZTYyZmV9
this code needed to be decoded so what I did was search a decoding page for
Base64 format and I got my code that is
picoCTF{web_succ3ssfully_d3c0ded_283e62fe}



Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

```
cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfMjgzZTYyZmV9
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

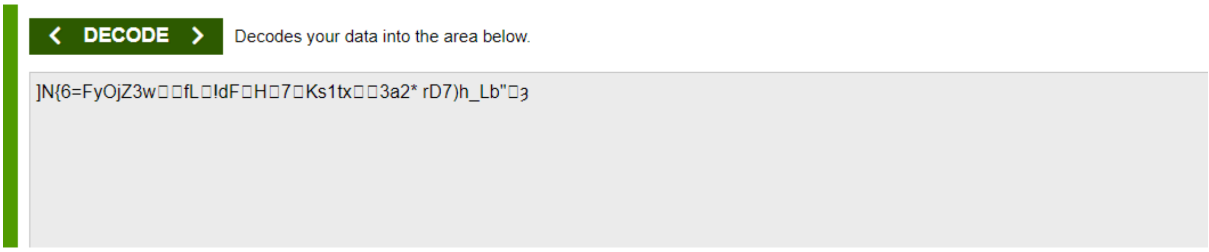
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
picoCTF{web_succ3ssfully_d3c0ded_283e62fe}
```

More Cookies:

For this exercise again I inspected the page and went into the cookies. In the cookies I found a code that looked like a code that needed to be decoded so I entered the code into a decoder and didn't find anything. I rentered it into the decoder and got



< DECODE > Decodes your data into the area below.

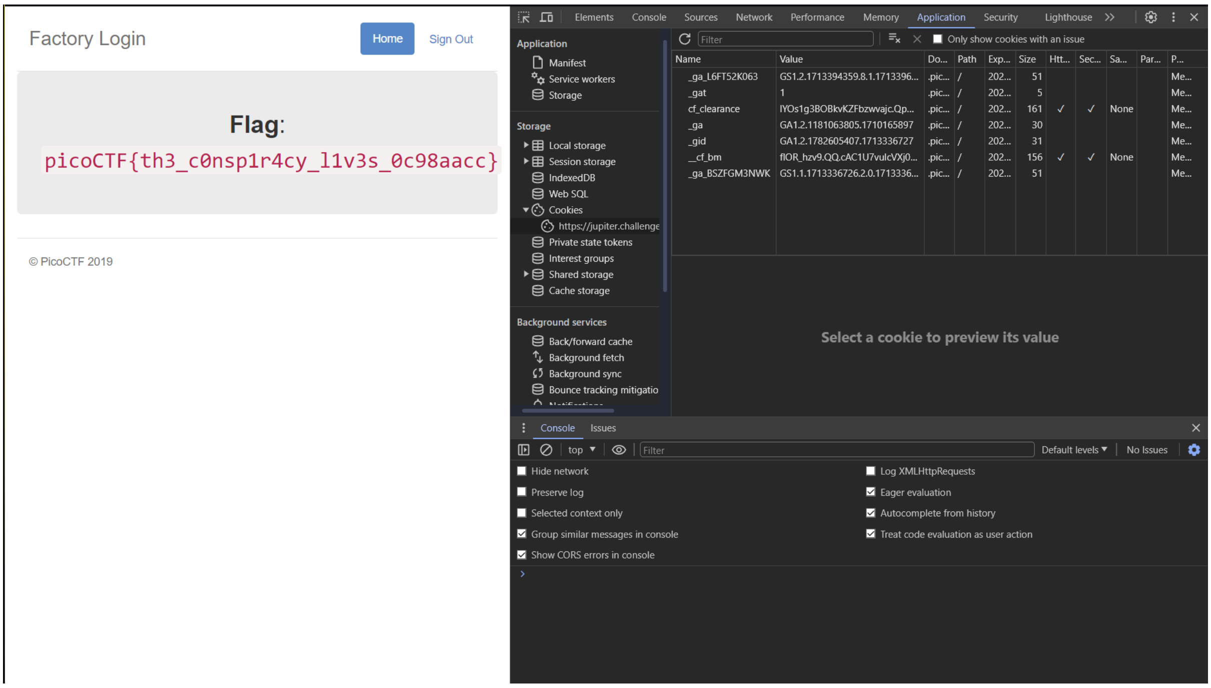
```
]N{6=FyOjZ3w□□fL□!dF□H□7□Ks1tx□□3a2* rD7)h_Lb"□ȝ
```

After getting this code I inserted it into a AES decoder because I investigated about that in the wikipedia link given in the hint and I got: picoCTF{co0ki3s_yum_e491c430}

Logon:

In this exercise again we are set with some username and some password that we need to enter.This one was very hard to find but after trying to login as joe I couldn't find anything until searching in the cookies I found that the admin was appearing meaning that maybe by changing it to true I was going to be able to login as joe and probably sole this and at the end it worked because by putting true it was like if I was the admin now and I had full control.

`picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}`



Flag:
picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}

© PicoCTF 2019

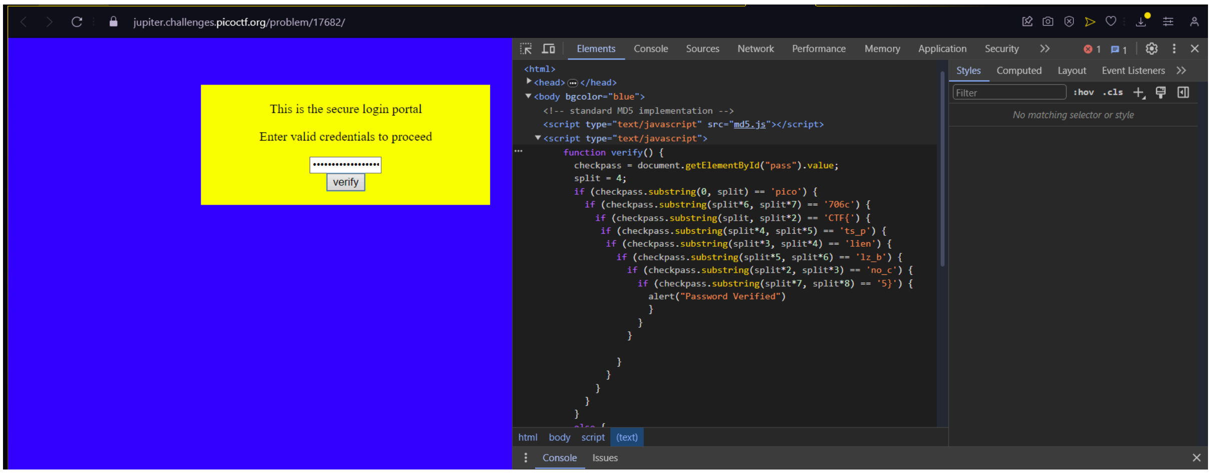
☐ Only show cookies with an issue

Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Par...	P...
_ga_L6FT52K063	GS1.2.1713394359.8.1.1713396...	.pic...	/	202...	51					Me...
_gat	1	.pic...	/	202...	5					Me...
cf_clearance	lYOs1g3BOBkvKZFbzwvajc.Qp...	.pic...	/	202...	161	✓	✓	None		Me...
_ga	GA1.2.1181063805.1710165897	.pic...	/	202...	30					Me...
_gid	GA1.2.1782605407.1713336727	.pic...	/	202...	31					Me...
__cf_bm	fIOR_hzv9.QQ.cAC1U7vulcVXj0...	.pic...	/	202...	156	✓	✓	None		Me...
_ga_BSZFGM3NWK	GS1.1.1713336726.2.0.1713336...	.pic...	/	202...	51					Me...

☐ Hide network
☐ Preserve log
☐ Selected context only
☑ Group similar messages in console
☑ Show CORS errors in console
☐ Log XMLHttpRequests
☑ Eager evaluation
☑ Autocomplete from history
☑ Treat code evaluation as user action

Dont_use_client_side:

This one was really easy, again I inspected the page and I saw in the code that there was a function called verify that checked some substring. I just ordered them and the code was made. picotCTF{no_clients_plz_b706c5}



This is the secure login portal

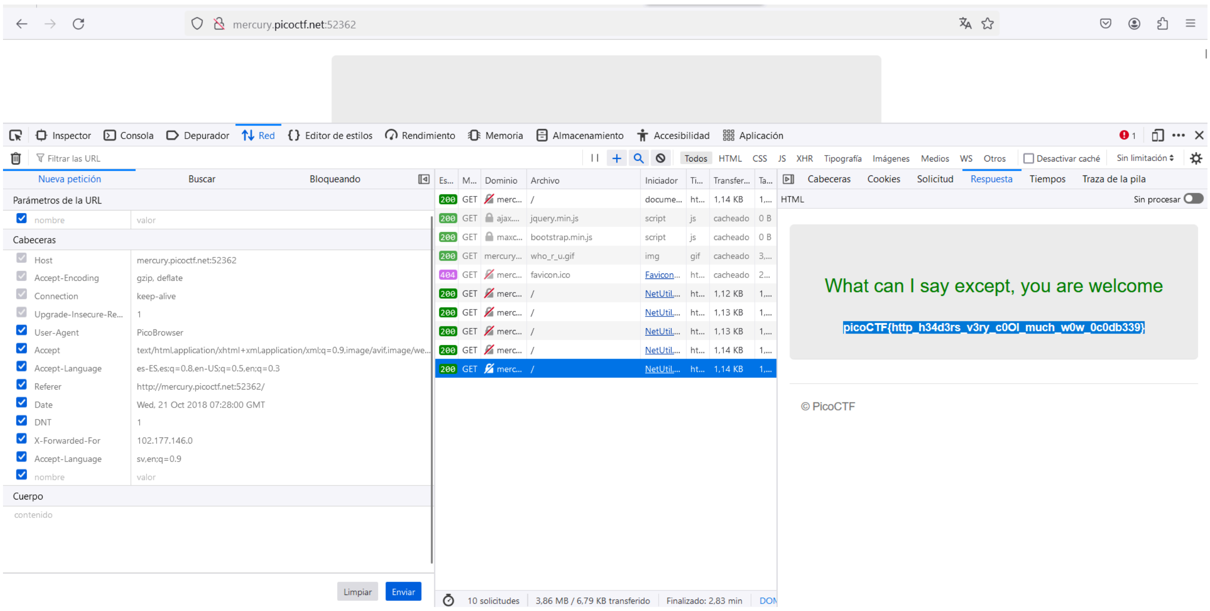
Enter valid credentials to proceed

verify

```
<html>
▶<head>…</head>
▼<body bgcolor="blue">
   <!-- standard MD5 implementation -->
   <script type="text/javascript" src="md5.js"></script>
  ▼<script type="text/javascript">
        function verify() {
          checkpass = document.getElementById("pass").value;
          split = 4;
          if (checkpass.substring(0, split) == 'pico') {
            if (checkpass.substring(split*6, split*7) == '706c') {
              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_b') {
                    if (checkpass.substring(split*2, split*3) == 'no_c') {
                      if (checkpass.substring(split*7, split*8) == '5}') {
                        alert("Password Verified")
                        }
                      }
                    }

                  }
                }
              }
            }
          }
```

Who Are You?:

First as always inspected the document.Second I saw a hint in the page that I can only browse through the PicoBrowser so I investigated and saw that I needed to change the user agent to pico Browser.Then I had to change the date because I got a message that it didn't worked if it wasnt 2018.Then I needed to change the location to Sweden and finally the language to Swedish as well. It was a hard exercise to understand at first but then its just adding headers and investigating what does each header does.



Parámetros de la URL

☑ nombre	valor

Cabeceras

☑ Host	mercury.picoctf.net:52362
☑ Accept-Encoding	gzip, deflate
☑ Connection	keep-alive
☑ Upgrade-Insecure-Re...	1
☑ User-Agent	PicoBrowser
☑ Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we...
☑ Accept-Language	es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
☑ Referer	http://mercury.picoctf.net:52362/
☑ Date	Wed, 21 Oct 2018 07:28:00 GMT
☑ DNT	1
☑ X-Forwarded-For	102.177.146.0
☑ Accept-Language	sv,en;q=0.9
☑ nombre	valor

Cuerpo

contenido

Es...	M...	Dominio	Archivo	Iniciador	Ti...	Transfer...	Ta...
200	GET	merc...	/	docume...	ht...	1,14 KB	1,...
200	GET	ajax....	jquery.min.js	script	js	cacheado	0 B
200	GET	maxc...	bootstrap.min.js	script	js	cacheado	0 B
200	GET	mercury...	who_r_u.gif	img	gif	cacheado	3,...
404	GET	merc...	favicon.ico	Favicon...	ht...	cacheado	2...
200	GET	merc...	/	NetUtil....	ht...	1,12 KB	1,...
200	GET	merc...	/	NetUtil....	ht...	1,13 KB	1,...
200	GET	merc...	/	NetUtil....	ht...	1,13 KB	1,...
200	GET	merc...	/	NetUtil....	ht...	1,14 KB	1,...
200	GET	merc...	/	NetUtil....	ht...	1,14 KB	1,...

10 solicitudes | 3,86 MB / 6,79 KB transferido | Finalizado: 2,83 min | DOM

What can I say except, you are welcome

picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_0c0db339}

© PicoCTF