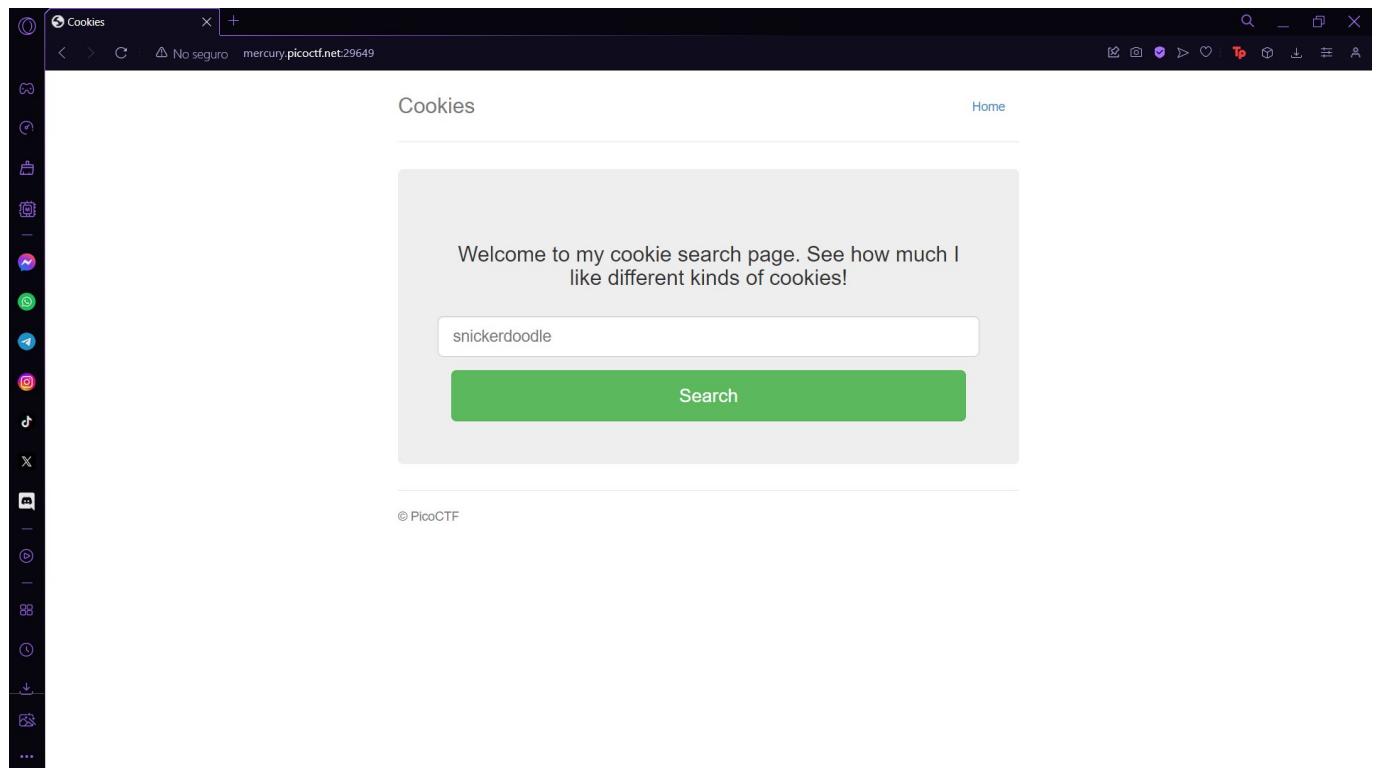


Homework 2

PICO CTF

▼ Cookies

The process involves accessing a redirected page from a link, where we encounter a form. In this form, we input a word as a placeholder. Simultaneously, we receive a default message while changing the value of a cookie in the page inspection window, incrementing from 0 to 17. When reaching the value 18, the PICO flag is revealed.



The screenshot shows a browser window with a message: "That is a cookie! Not very special though...". Below it, a large button says "I love chocolate chip cookies!". The URL is `mercury.picoctf.net:29649/check`. To the right is the Chrome DevTools Application panel, which displays a table of cookies:

Name	Value	D...	P...	E...	S...	H...	S...	P...	P...
name	1	m...	/	S...	5			M...	

A tooltip says "Select a cookie to preview its value". A warning at the bottom of the DevTools panel states: "Warning! This area is for use by developers only. Scammers have been known to encourage people to copy/paste information here to hack accounts. Do not proceed if you are unsure." There is also a link to "Switch DevTools to Spanish".

The screenshot shows a browser window with a message: "Flag: picoCTF{3v3ry1_10v3s_c00k135_a1f5bdb7}". The URL is `mercury.picoctf.net:29649/check`. To the right is the Chrome DevTools Application panel, which displays a table of cookies:

Name	Value	D...	P...	E...	S...	H...	S...	P...	P...
name	18	m...	/	S...	6			M...	

A tooltip says "Select a cookie to preview its value". A warning at the bottom of the DevTools panel states: "Warning! This area is for use by developers only. Scammers have been known to encourage people to copy/paste information here to hack accounts. Do not proceed if you are unsure." There is also a link to "Switch DevTools to Spanish".

▼ Bookmarklet

The screenshot shows a browser window with a picoCTF challenge page. The page features a logo of a person holding a flag and the text "Welcome to my flag distribution website!". It also contains some JavaScript code and a warning about pasting.

In the DevTools console, there is a block of JavaScript code:

```

allow pasting
> javascript:(function() {
  var encryptedFlag = "%D0%E0%O0%D0%E0%C0%E1";
  var key = "picocft";
  var decryptedFlag = "";
  for (var i = 0; i < encryptedFlag.length; i++) {
    decryptedFlag += String.fromCharCode((encryptedFlag.charCodeAt(i) - key.charCodeAt(i)) % key.length + 256);
  }
  alert(decryptedFlag);
})();

<- undefined
> javascript:(function() {
  var encryptedFlag = "%D0%E0%O0%D0%E0%C0%E1";
  var key = "picocft";
  var decryptedFlag = "";
  for (var i = 0; i < encryptedFlag.length; i++) {
    decryptedFlag += String.fromCharCode((encryptedFlag.charCodeAt(i) - key.charCodeAt(i)) % key.length + 256);
  }
  alert(decryptedFlag);
})();

<- undefined
> picocFT{p@g3_turn3r_cebccfde}

```

▼ Insp3ct0r

The screenshot shows a browser window with a challenge page titled "Inspect Me". The page content includes "What" and "How" sections, and a message from the developer: "I made a website".

The DevTools sidebar shows the "Sources" tab is active, displaying the file structure and content of "myjs.js". The code in "myjs.js" is as follows:

```

8   </head>
9
10  <body>
11    <div class="container">
12      <header>
13        <h1>Inspect Me</h1>
14      </header>
15
16      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultTab">What</button>
17      <button class="tablink" onclick="openTab('tababout', this, '#222')">How</button>
18
19      <div id="tabintro" class="tabcontent">
20        <h3>What</h3>
21        <p>I made a website</p>
22      </div>
23
24      <div id="tababout" class="tabcontent">
25        <h3>How</h3>
26        <p>I used these to make this site: <br/>
27          HTML <br/>
28          CSS <br/>
29          JS (JavaScript)
30        </p>
31        <!-- Html is neat. Anyways have 1/3 of the flag: picocTF{tru3_d3} -->
32      </div>
33
34    </div>
35
36  </body>
37  </html>

```

```

myjs.js
1 function openTab(tabName, elmnt, color) {
2     var i, tabcontent, tablinks;
3     tabcontent = document.getElementsByClassName("tabcontent");
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 = "#ccc";
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 /* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399 */
22

```

```

myjs.js
1 function openTab(tabName, elmnt, color) {
2     var i, tabcontent, tablinks;
3     tabcontent = document.getElementsByClassName("tabcontent");
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 = "#ccc";
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 /* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399 */
22

```

Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3}

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

Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399}

- picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?f10be399}

Scavenger Hunt

Two screenshots of a browser developer tools interface showing network requests and element inspection.

Screenshot 1: Network Requests (DevTools)

The browser window shows a request to `mercury.picoctf.net:39698/robots.txt`. The response content is:

```
User-agent: *
Disallow: /index.html
# Part 3: t_0t_p14c
# I think this is an apache server... can you Access the next flag?
```

The DevTools Network tab shows a request to `mercury.picoctf.net:39698/browser.js`. The response content is:

```
;463
;464
;465
;466
;467
;468
;469
;470
;471
;472
;473
;474
;475
;476
;477
;478
;479
;480
;481
;482
```

Screenshot 2: Element Inspection (DevTools)

The browser window shows a request to `mercury.picoctf.net:39698/.htaccess`. The response content is:

```
# Part 4: 3s_2_look
# I love making websites on my Mac, I can Store a lot of information there.
```

The DevTools Elements tab shows the HTML structure:

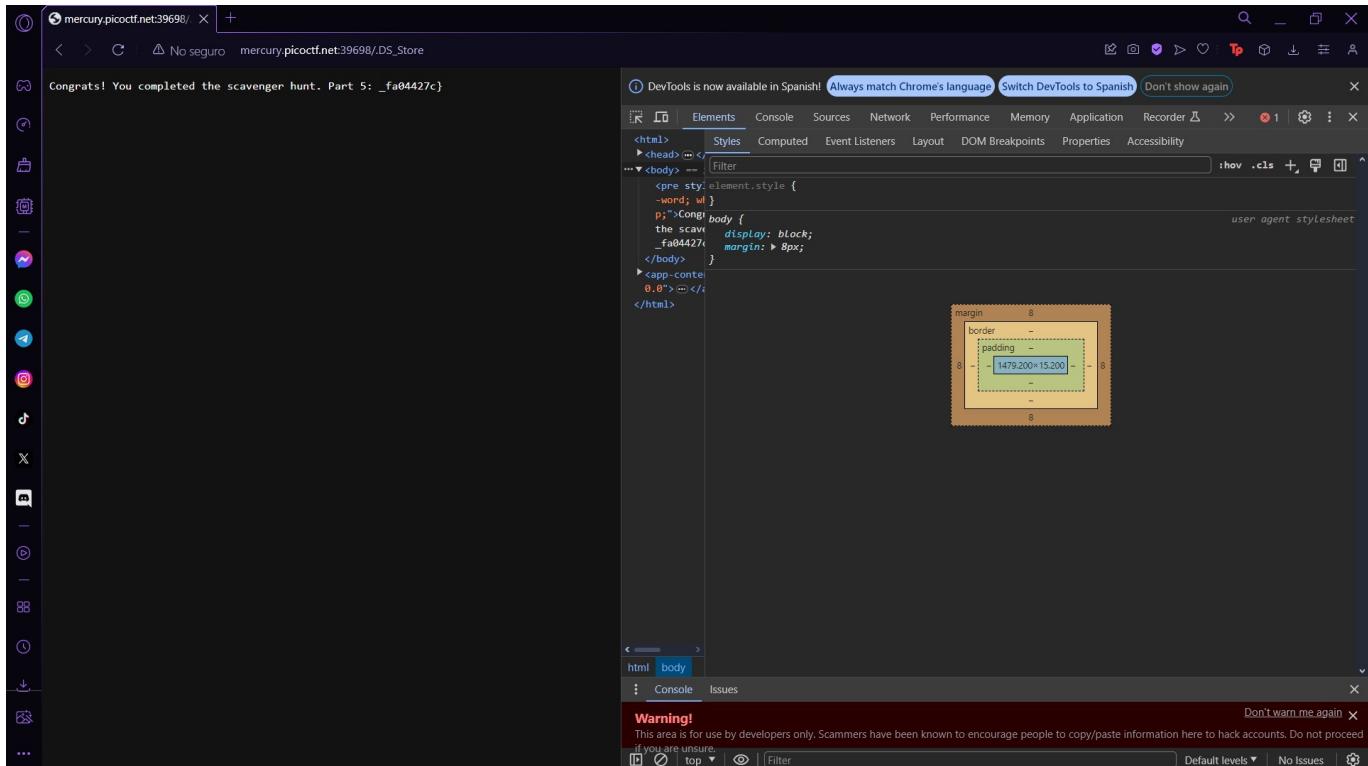
```
<!DOCTYPE html>
<html> == $0
  > <head> == $1
  > <body> == $2
  > <app-content ng-version="16.0.0"> == $3</app-content>
</html>
```

The right panel displays the CSS styles for the `html` element:

```
:root {
  user agent stylesheet
}
  view-transition-name: root;
}

html {
  user agent stylesheet
}
  display: block;
```

A visual representation of the element's bounding box is shown, with dimensions of 652x56400.



Here's the first part of the flag: picoCTF{t

Disallow: /index.html Part 3: t_0f_pl4c I think this is an apache server... can you Access the next flag?

CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0

Part 4: 3s_2_l00k I love making websites on my Mac, I can Store a lot of information there.

Congrats! You completed the scavenger hunt. Part 5: _fa04427c}

- picoCTF{th4ts_4_l0t_0f_pl4c3s_2_l00k_fa04427c}

✓ WebDecode

The screenshot shows a browser window with the URL <https://titan.picoctf.net:58552/about.html>. A large text overlay reads "Try inspecting the page there". The DevTools Elements tab is open, showing the DOM structure of the page. The Console tab displays a warning message:

```
Warning!
This area is for use by developers only. Scammers have been known to encourage people to copy/paste information here to hack accounts. Do not proceed if you are unsure.

Unchecked runtime.lastError: A listener indicated an asynchronous response by returning true, but the message channel closed before a response was received
```

Decode from Base64 format

Simply enter your data then push the decode button.

cG1jb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfZGYwZGE3Mjd9

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_df0da727}

More Cookies

The screenshot shows a browser window with a "More Cookies" search bar. Below it, a message says: "Welcome to my cookie search page. Only the admin can use it!". The DevTools Application tab is open, showing a table of cookies. One cookie is selected:

Name	Value	Do...	Path	Exp...	Size	Htt...	Ses...	Sec...	Part...	Pr...
auth_name	bnNzQ2xNV1VIZJowOHV2eDNOGtwWnoxcnF3aJfSaEhRRXJ6dHNzYjVxSDRuYmxGT1B0cmFR2tYmlHV2pW0tDzbTRSUK1MG40ZC4Q0wzc09qWkpUSC9SJUhsYzNldFdKZDXL2NOR0p8b52C1QRQOEN2QuxmUng3dDlwdfEl=		/		181					Me...
name	-1		/		6					Me...

The DevTools Issues tab shows a warning about an unchecked runtime.lastError message.

9% | 9/96 [00:05<00:53, 1.62it/s] Admin bit found in byte 9 bit 0. Flag:
picoCTF{c00ki3s_yum_e40d16a9}

✓ Dont-use-client-side

The screenshot shows a browser window titled "Secure Login Portal". It displays a yellow box with the text: "This is the secure login portal. Enter valid credentials to proceed." Below the box is a redacted input field and a "verify" button. The DevTools Sources tab is open, showing the "browser.js" file with several conditional statements. A breakpoint is set on line 22, column 20. The DevTools Breakpoints panel shows the current state of the application. The Issues tab shows a failed resource load and an unchecked runtime.lastError message.

```

    <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) == '23c') {
                    if (checkpass.substring(split*4, split*5) == 'CTF') {
                        if (checkpass.substring(split*3, split*4) == 'lien') {
                            if (checkpass.substring(split*2, split*3) == '12.7') {
                                if (checkpass.substring(split*7, split*8) == 'e') {
                                    alert("Password Verified")
                                }
                            }
                        }
                    }
                }
            }
        }
    </script>
  
```

picoCTF{no_clients_plz_7723ce}

✓ logon

The screenshot shows a browser window with the URL <https://jupiter.challenges.picoctf.org/problem/15796/flag>. The main content area displays a "Factory Login" form with a success message: "Success: You logged in! Not sure you'll be able to see the flag though." Below this, a large box says "No flag for you". The footer indicates "© PicoCTF 2019". To the right of the browser is an open DevTools window. The Network tab is selected, showing a list of cookies. One cookie, "password", has its value set to "asdsaw". The DevTools sidebar also lists "Background services" like Back/forward cache, Background fetch, and Bounce tracking.

Name	Value	Dom.	Path	Expir.	Size	Http...	Secure	Same...	Partit...	Prio...
admin	False	jupite...	/	Session	10					Medi...
username	hola	jupite...	/	Session	12					Medi...
password	asdsaw	jupite...	/	Session	14					Medi...
_ga_L6FT52K063	GS1.2.1713412212.16.1.1713414884.0.0.0	picoct...	/	2025...	52					Medi...
cf_clearance	WrpaizNU6zN0SAW0d8sxpAuvbr35...	picoct...	/	2025...	161	✓	✓	None		Medi...
_ga	GAI.2.712295566.1705504730	picoct...	/	2025...	29					Medi...

The screenshot shows the same browser setup. The main content area now displays the flag: "Flag: picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}". The DevTools Network tab shows the same cookie list, but the "password" cookie now has its value set to "picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}".

Name	Value	Dom.	Path	Expir.	Size	Http...	Secure	Same...	Partit...	Prio...
_ct_bm	TEx46927UQHNMyymxz4Yp...	pi...	/	20...	156	✓	✓	No...		Me...
cf_clearance	WrpaizNU6zN0SAW0d8sxpAuvbr35...	pi...	/	20...	161	✓	✓	No...		Me...
_ga_L6FT52K063	GS1.2.1713412212.16.1.1713414884.0.0.0	picoct...	/	20...	52					Me...
_gid	GA1.2.216568032.1713398166	pi...	/	20...	30					Me...
_ga	GA1.2.712295566.1705504730	picoct...	/	20...	29					Me...
_ga_BSZFGM3N...	GS1.1.1706053028.5.1.17060...	pi...	/	20...	51					Me...

✓ Who are you?

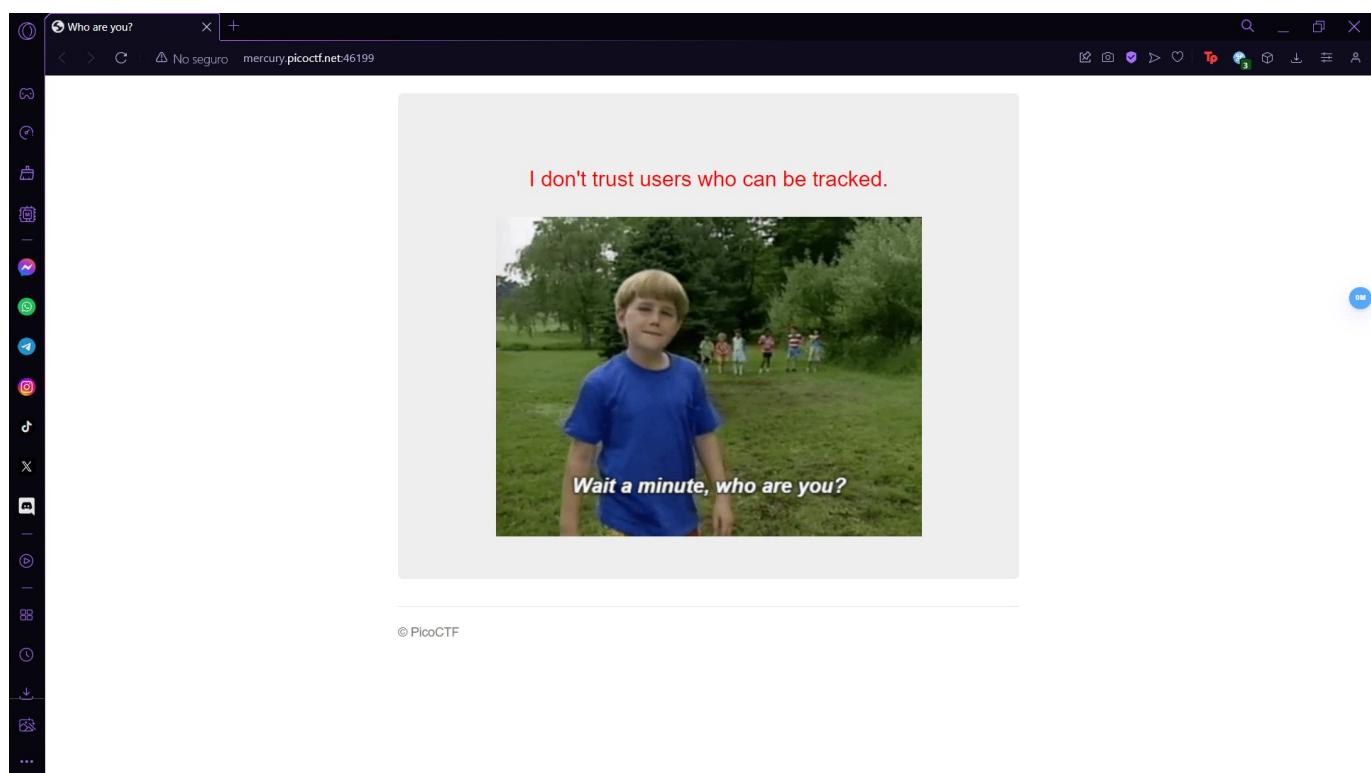
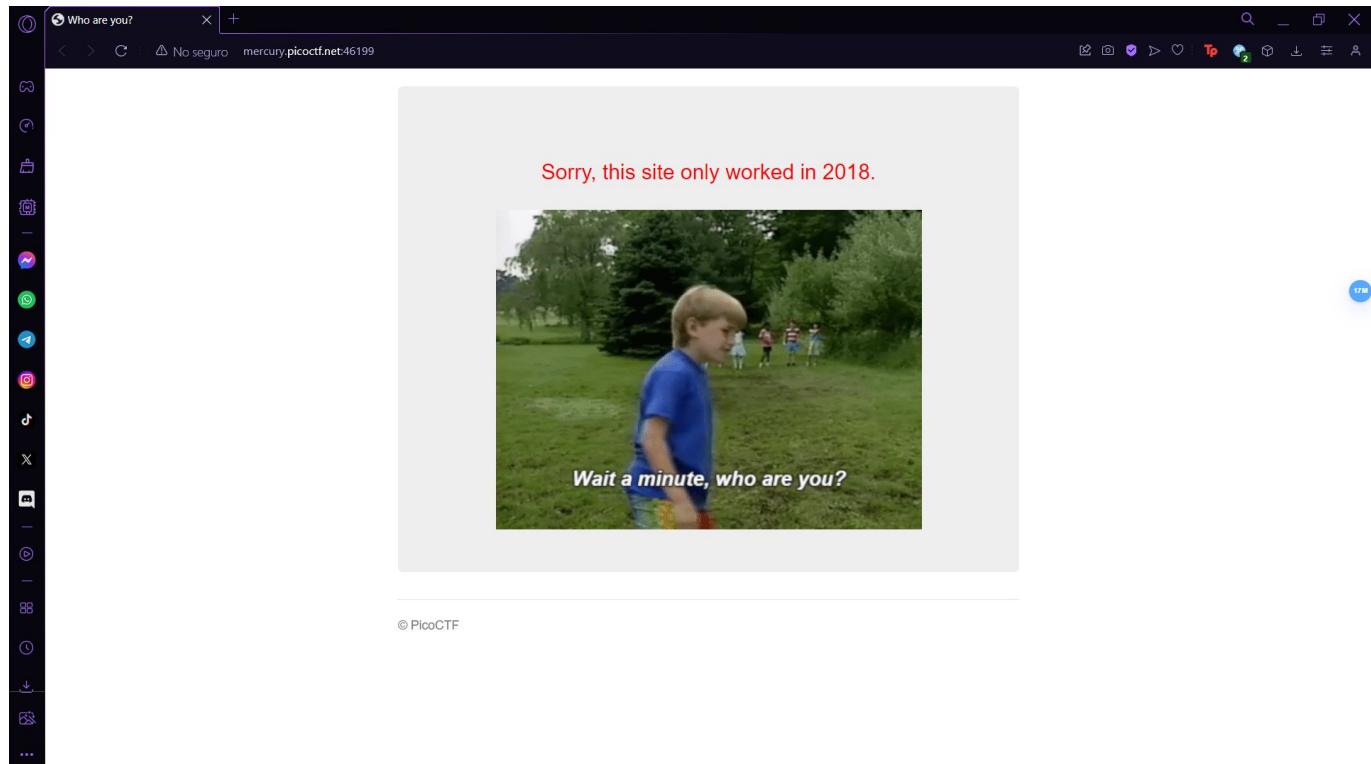
User-Agent: PicoBrowser

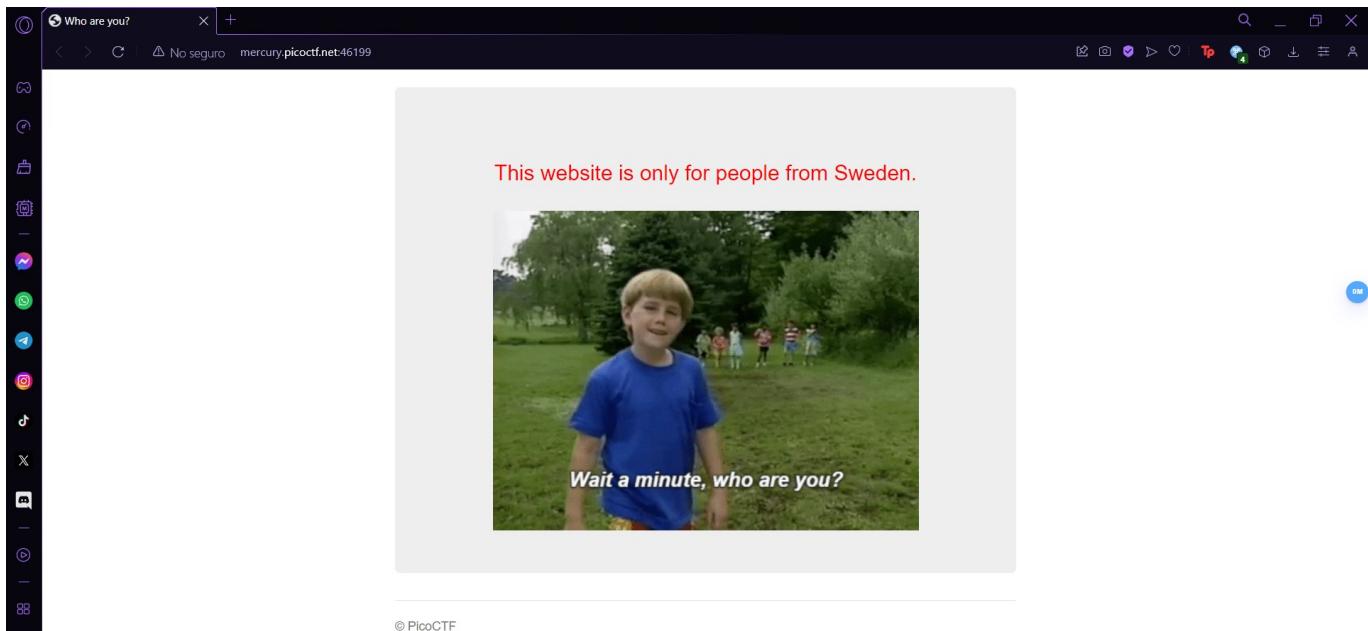
Date: 2018

DNT: 1

X-Forwarded-For: 2.16.66.0

Accept-Language: sv





© PicoCTF