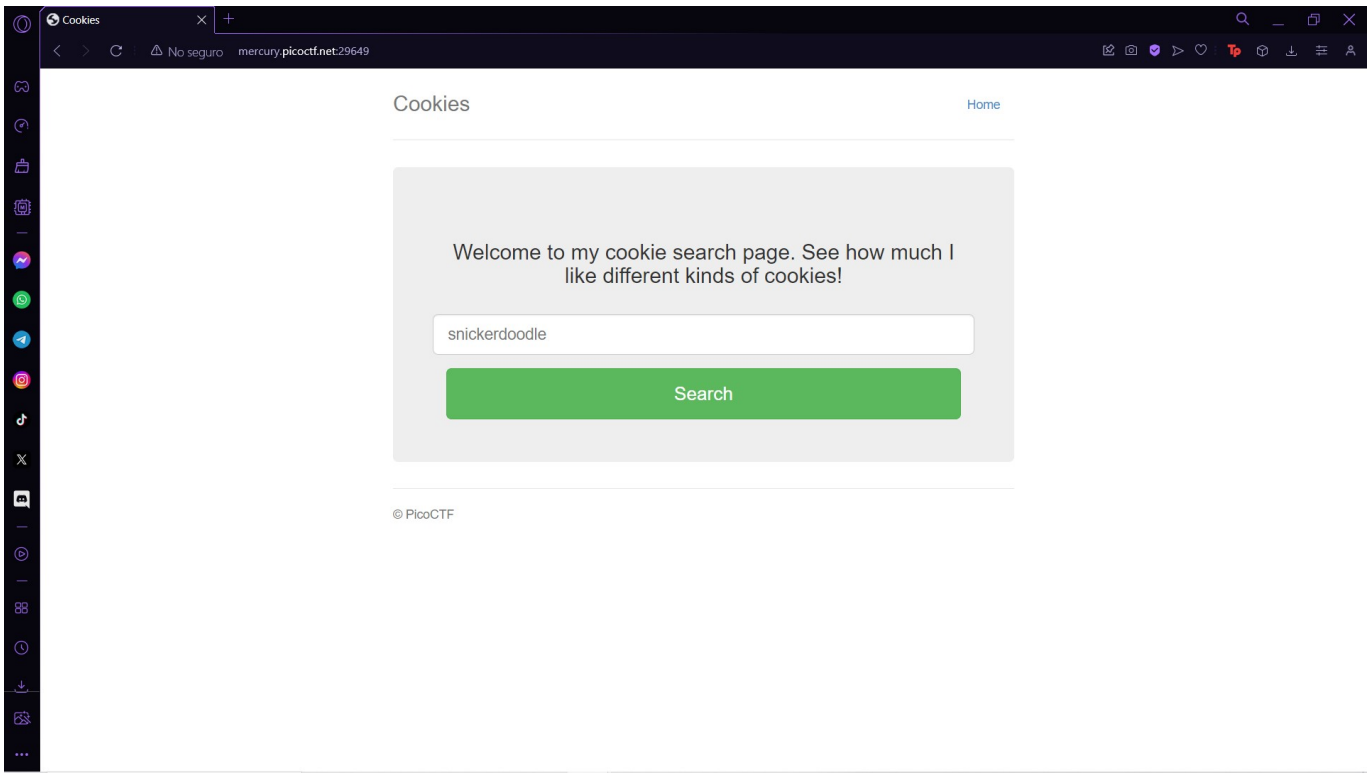
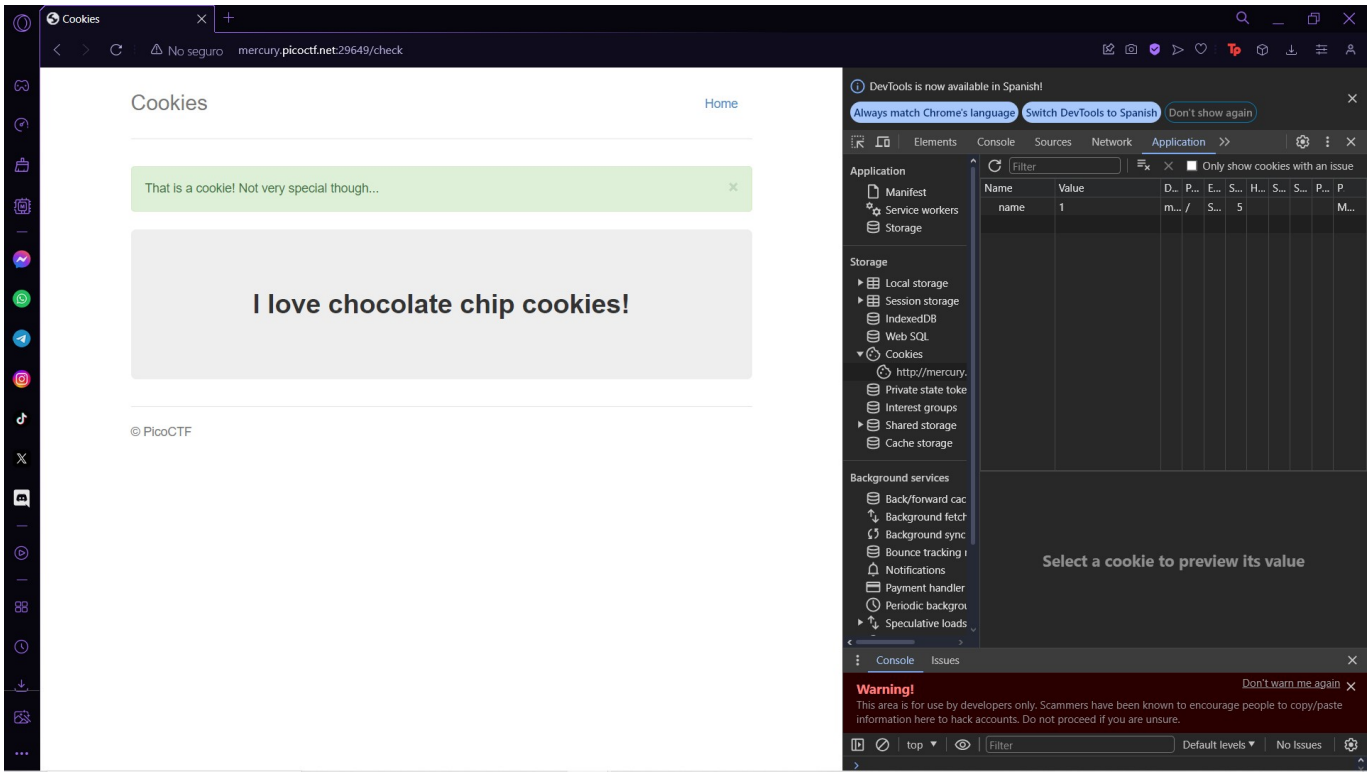
Homework 2

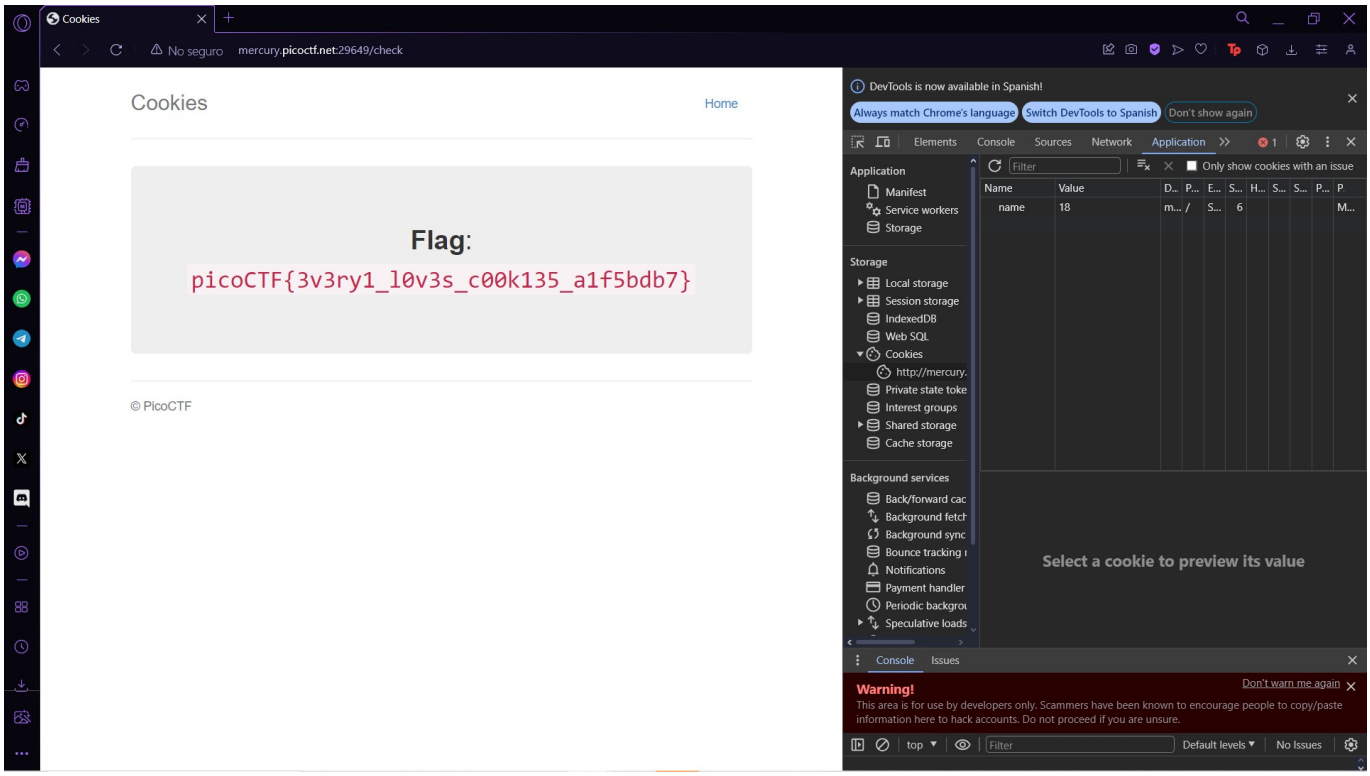
PICO CTF

Cookies

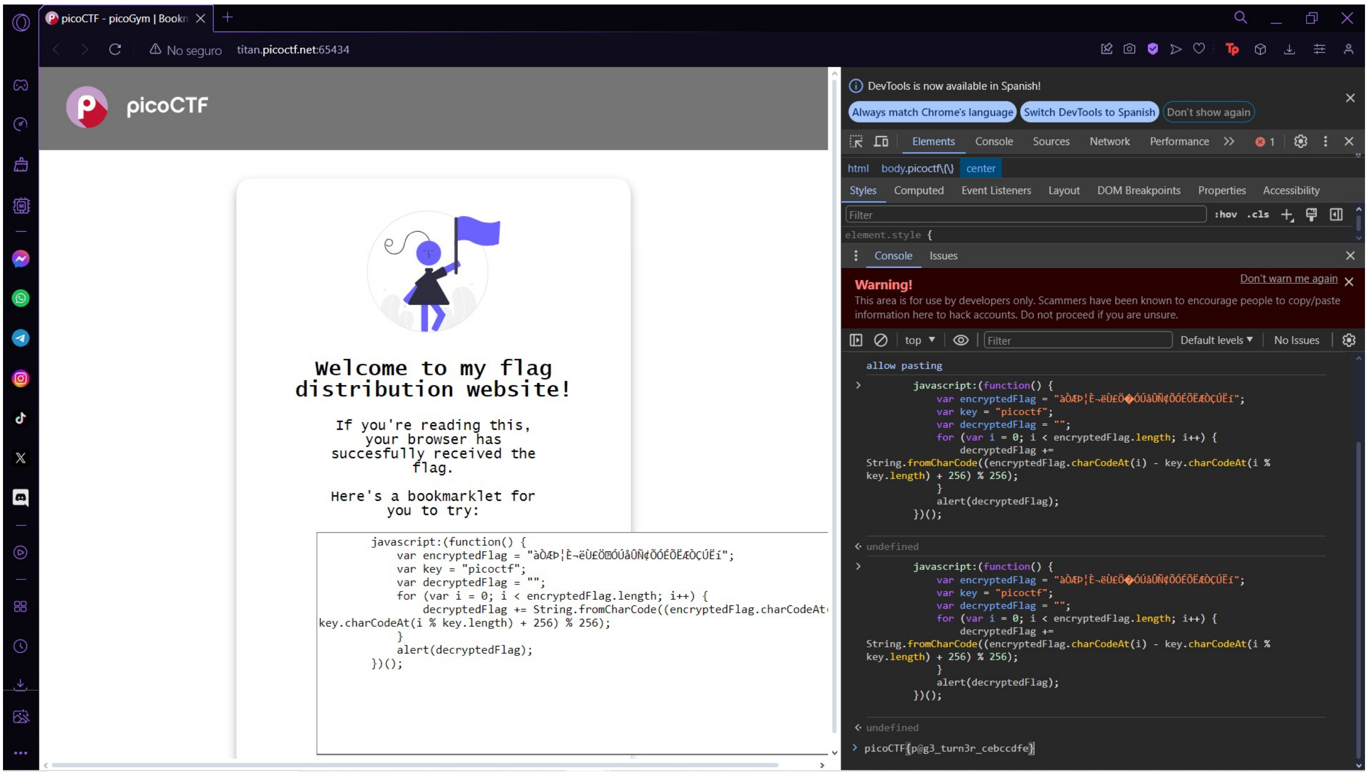
The process involves accessing a redirected page from a link, where we encounter a form. In this form, we input a word as a placeholder. Simultaneously, we receive a default message while changing the value of a cookie in the page inspection window, incrementing from 0 to 17. When reaching the value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



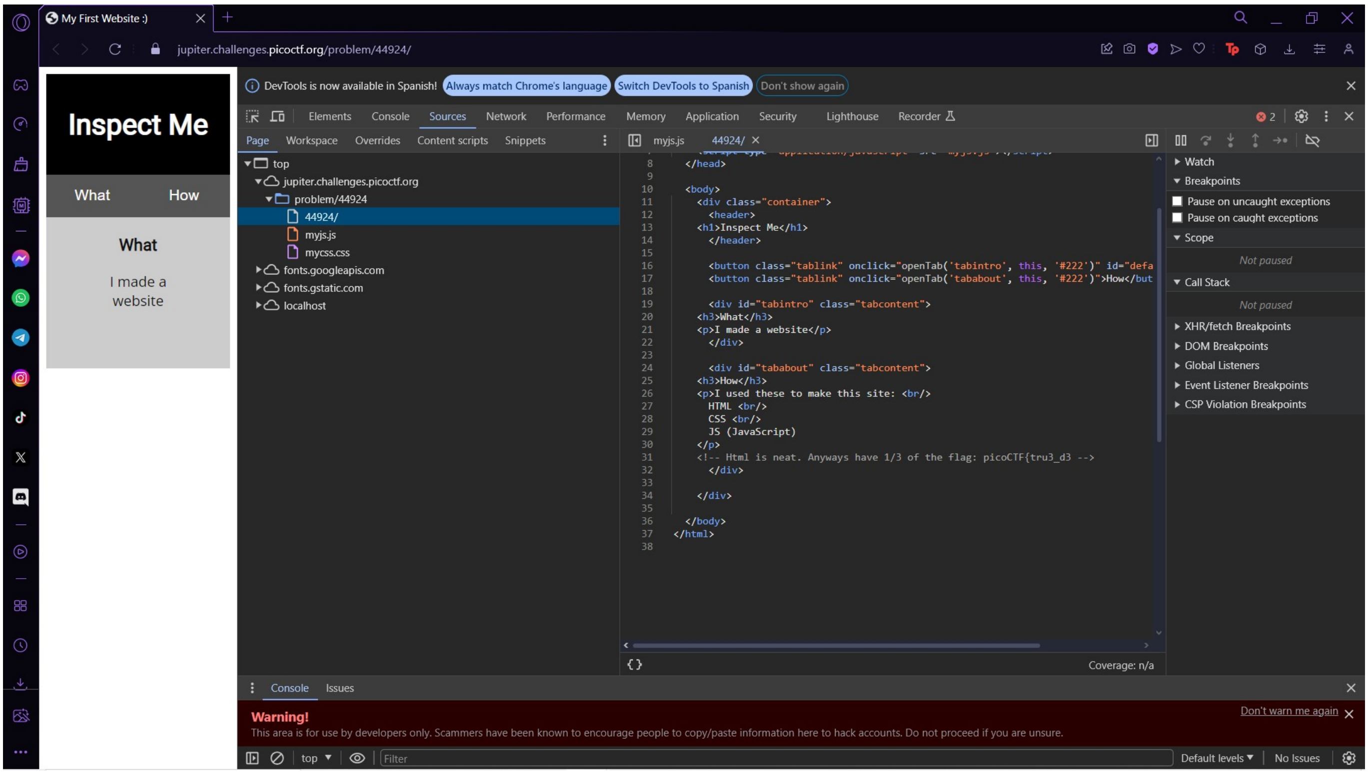


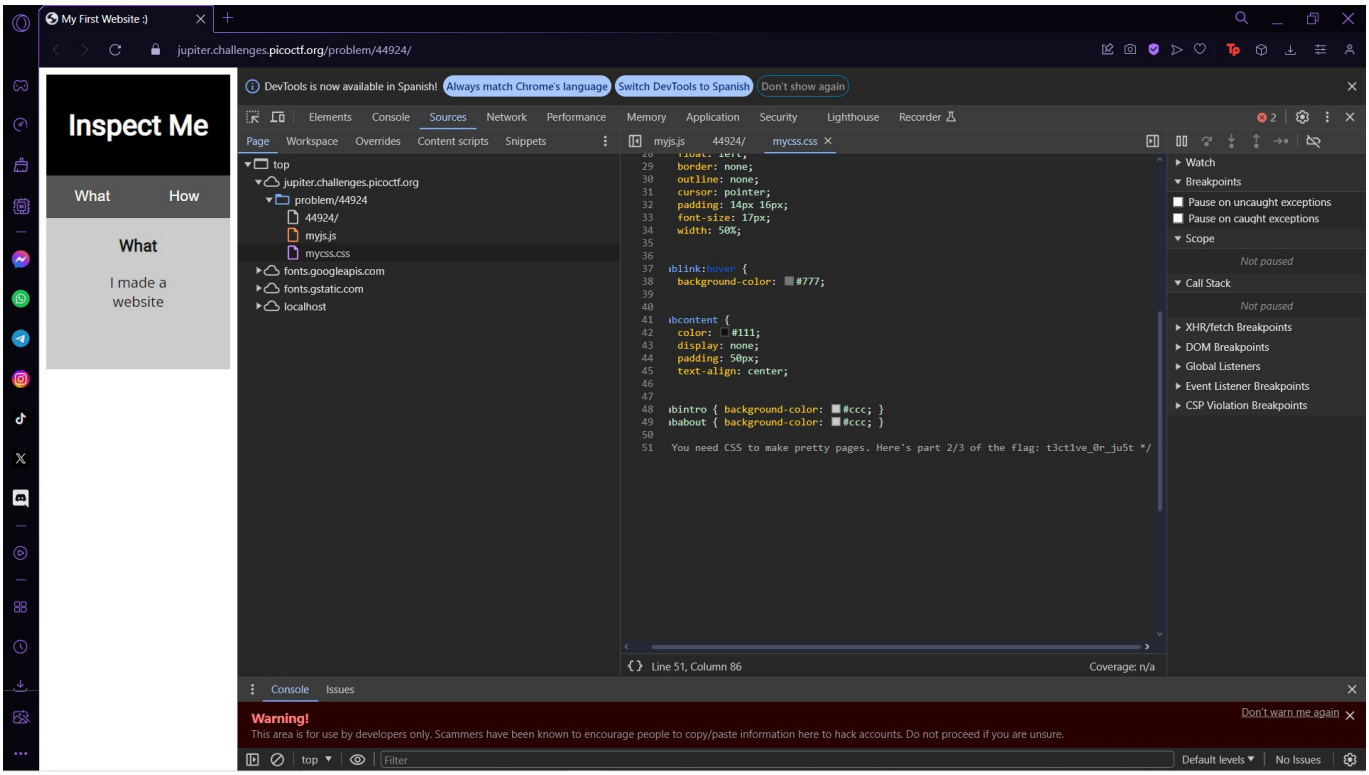


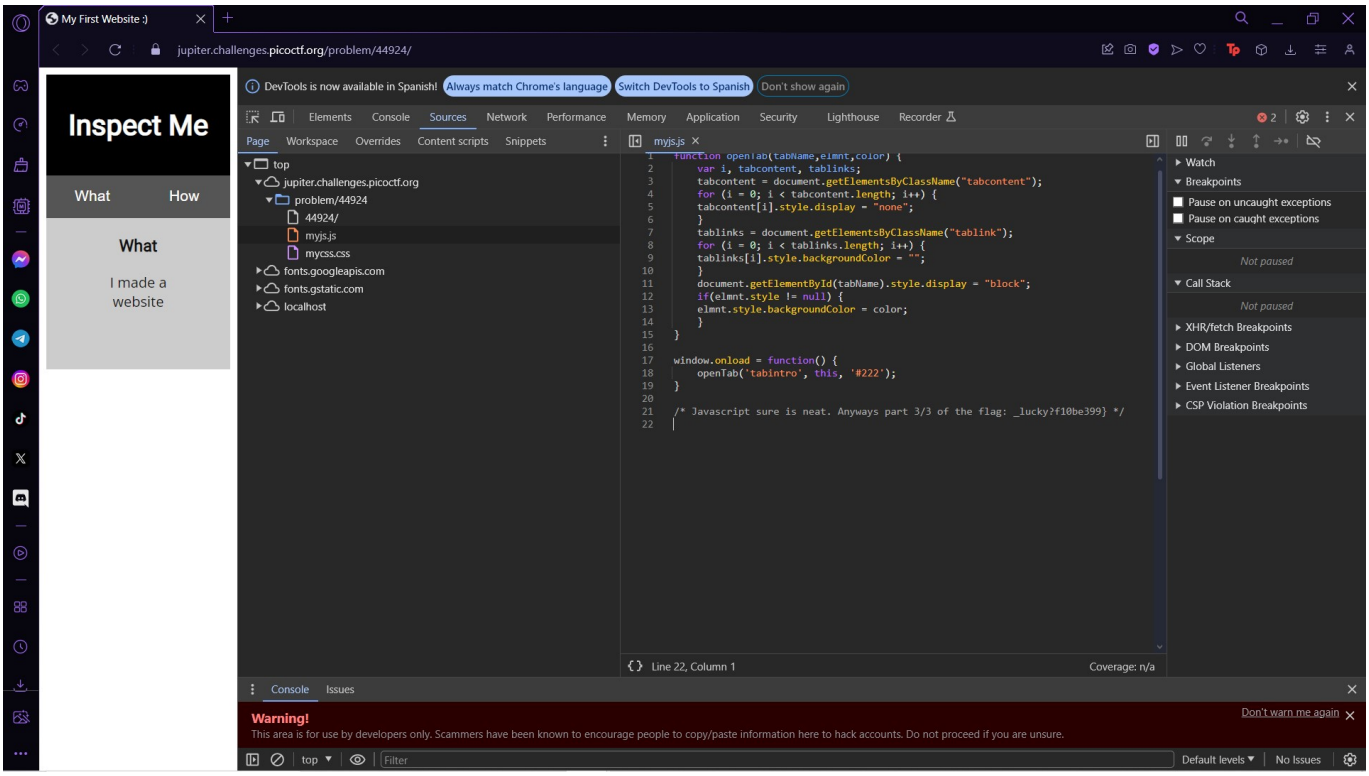
Bookmarklet


picoCTF - picoGym | Bookm
No seguro titan.picoctf.net:65434
picoCTF
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 key = "picoctf";
var decryptedFlag = "";
for (var i = 0; i < encryptedFlag.length; i++) {
alert(decryptedFlag);
})();
DevTools is now available in Spanish!
Always match Chrome's language
Switch DevTools to Spanish
Don't show again
Elements Console Sources Network Performance
Styles Computed Event Listeners Layout DOM Breakpoints Properties Accessibility
Console Issues
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.
allow pasting
undefined
picoCTF{p@g3_turn3r_cebccdfe}

Insp3ct0r


My First Website :)
jupiter.challenges.picoctf.org/problem/44924/
Inspect Me
What
How
What
I made a website
DevTools is now available in Spanish!
Always match Chrome's language
Switch DevTools to Spanish
Don't show again
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder
Page Workspace Overrides Content scripts Snippets
top
jupiter.challenges.picoctf.org
problem/44924
44924/
myjs.js
mycss.css
fonts.googleapis.com
fonts.gstatic.com
localhost
<h1>Inspect Me</h1>
<h3>What</h3>
I made a website
<h3>How</h3>
I used these to make this site:
HTML
CSS
JS (JavaScript)
<!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
Coverage: n/a
Console Issues
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.





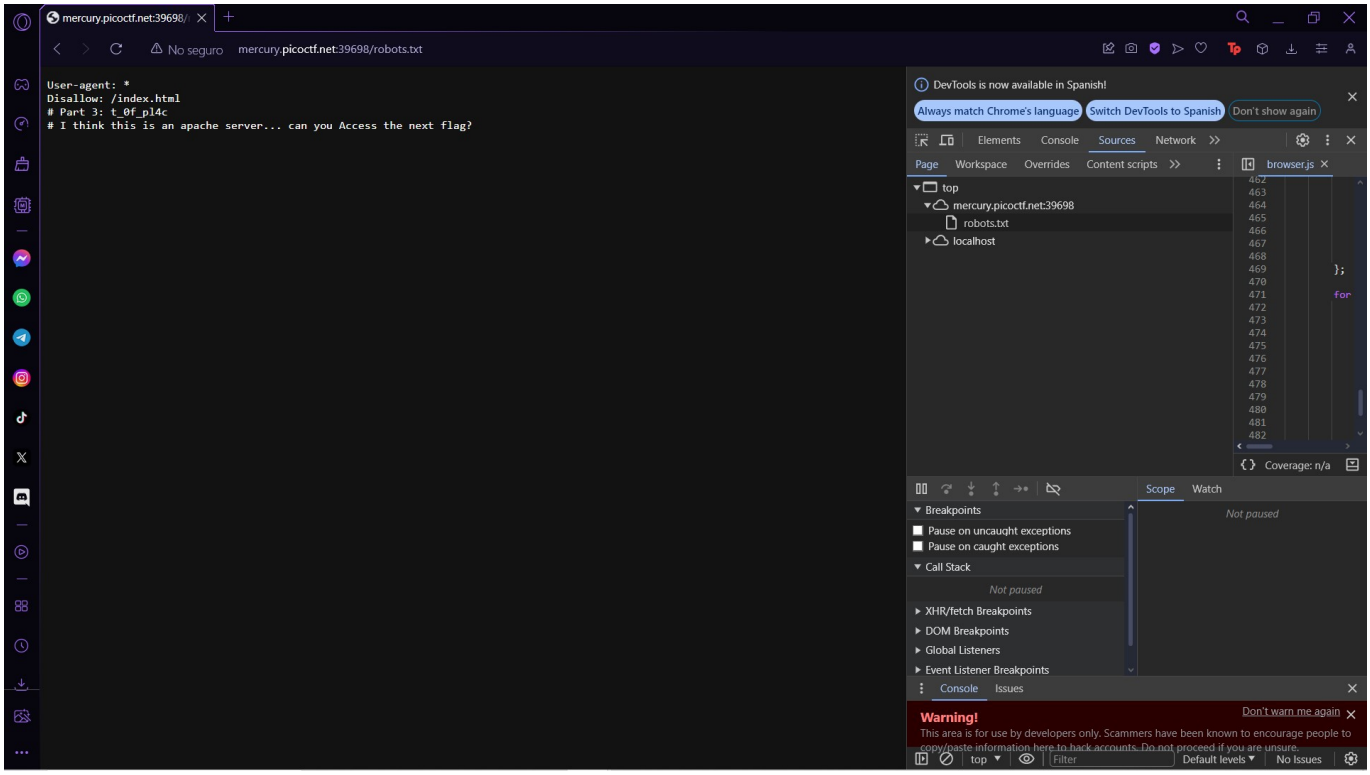
Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3

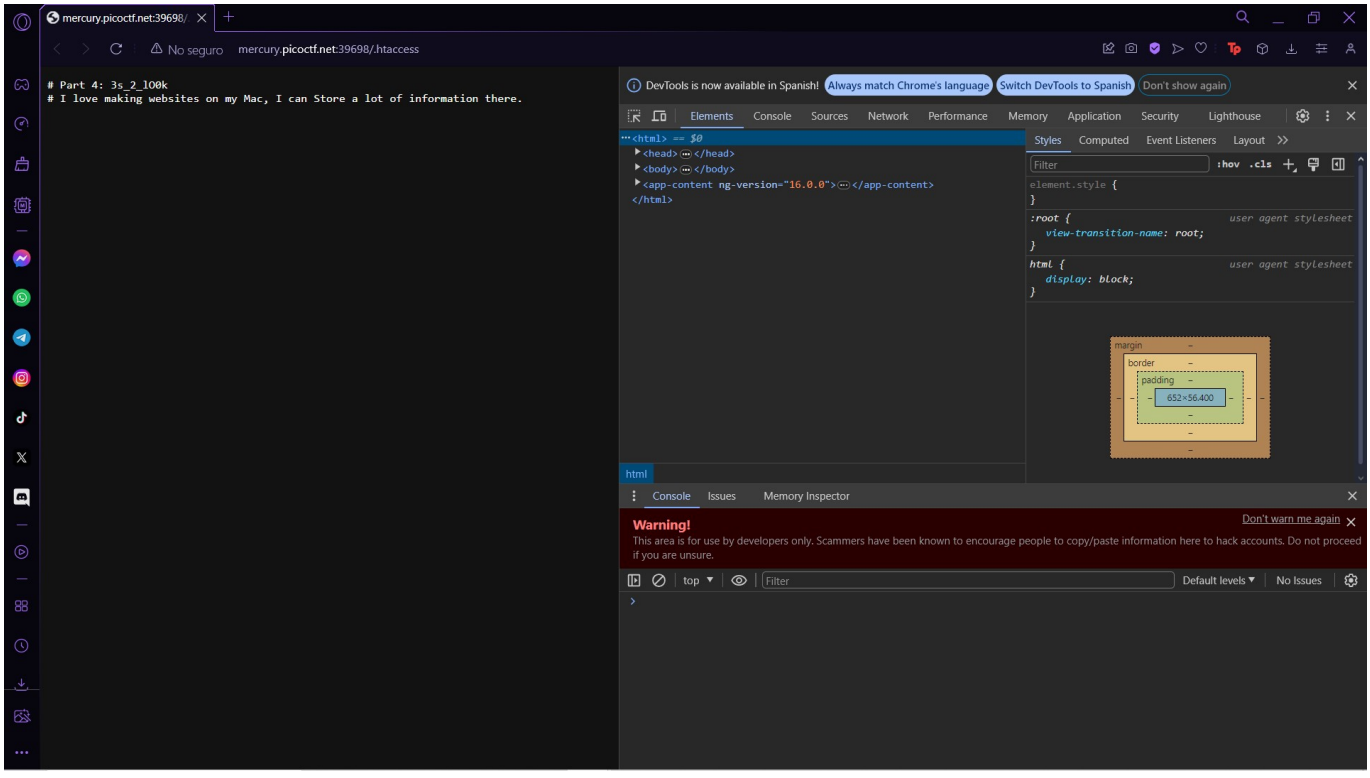
You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t

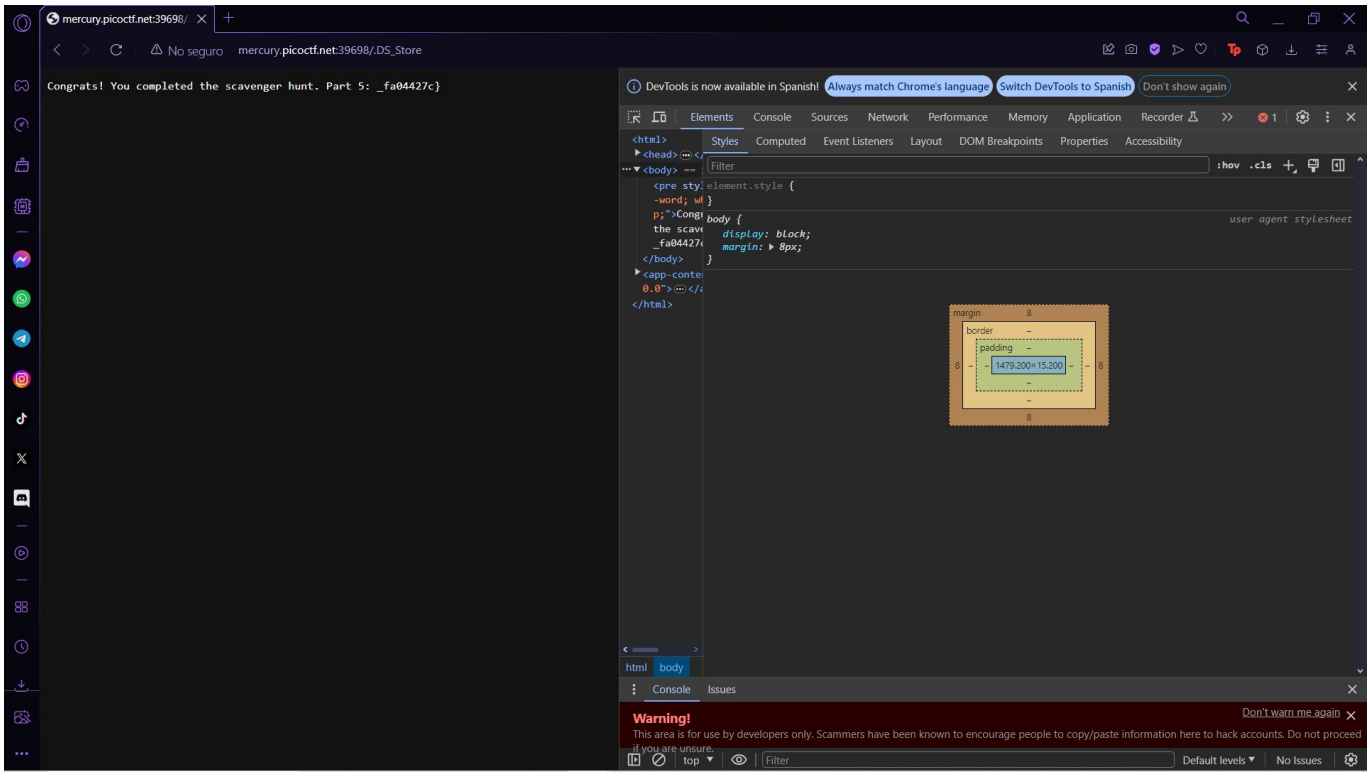
Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399}

- picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?f10be399}

Scavenger Hunt







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?

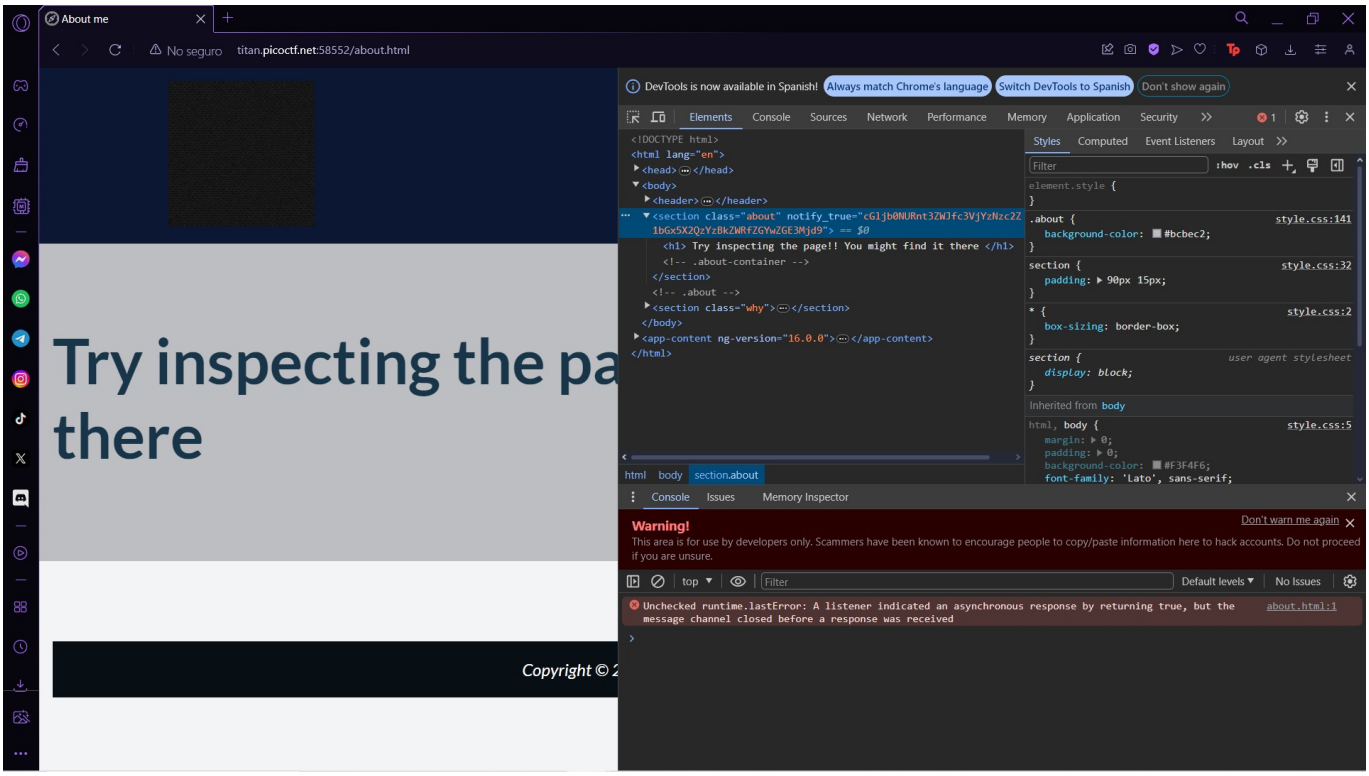
CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0

Part 4: 3s_2_lO0k 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_lO0k_fa04427c}

WebDecode



Decode from Base64 format

Simply enter your data then push the decode button.

cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfZGYwZGE3Mjd9

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

UTF-8 Source character set.

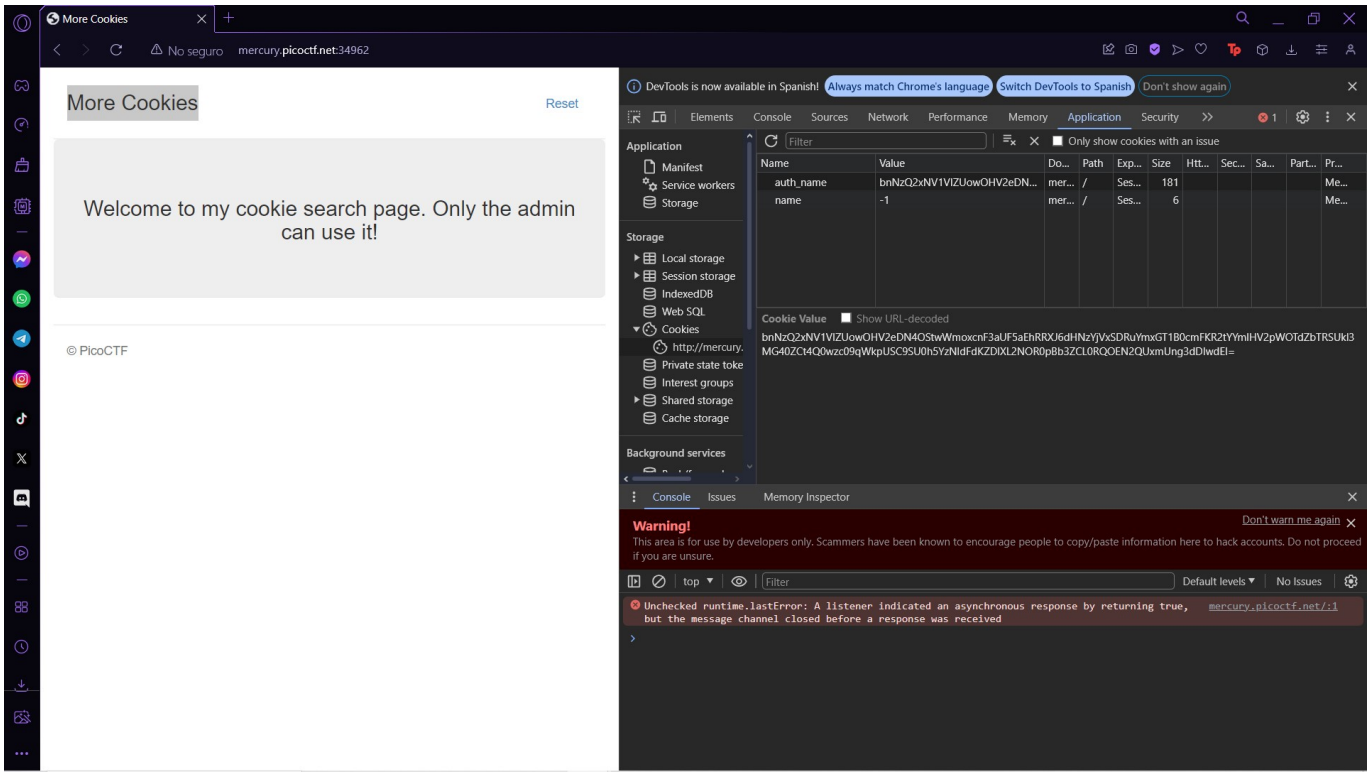
Decode each line separately (useful for when you have multiple entries).

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.

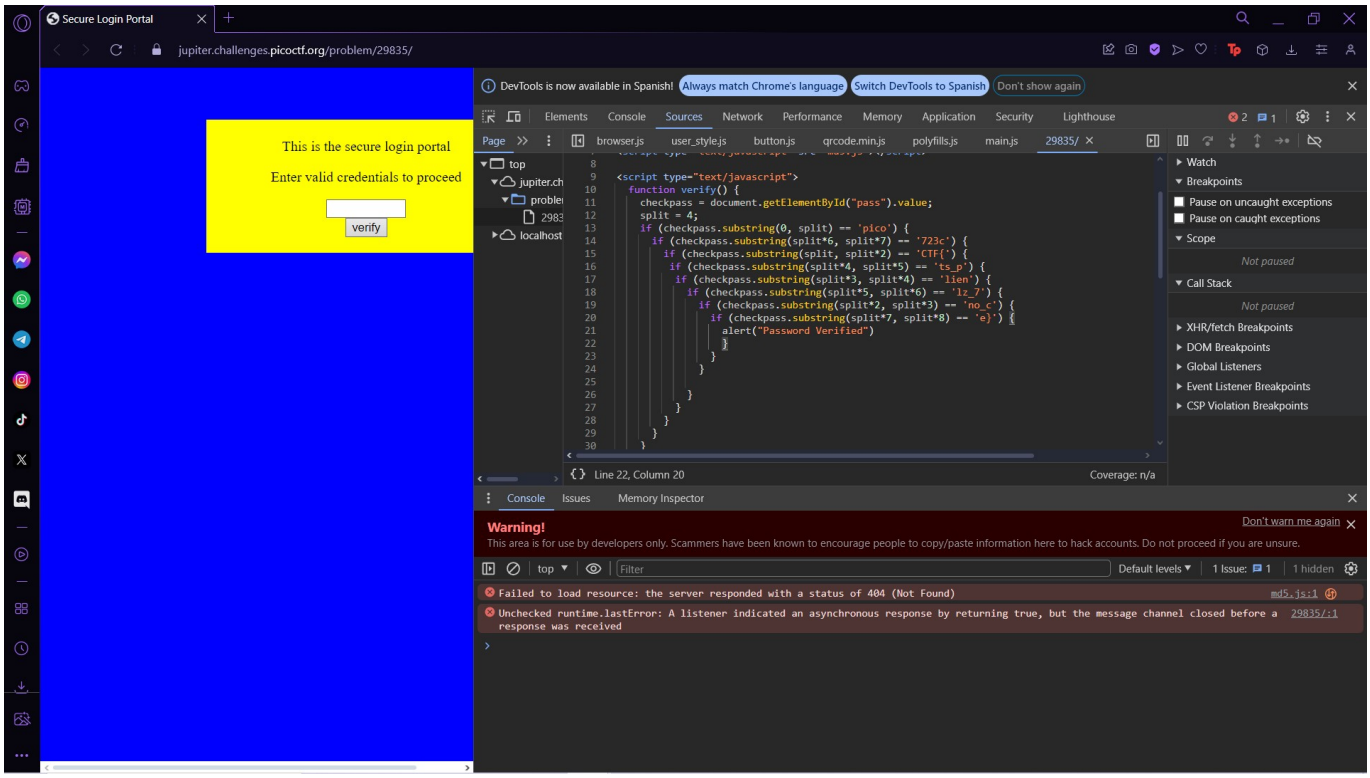
picoCTF{web_succ3ssfully_d3c0ded_df0da727}

More Cookies



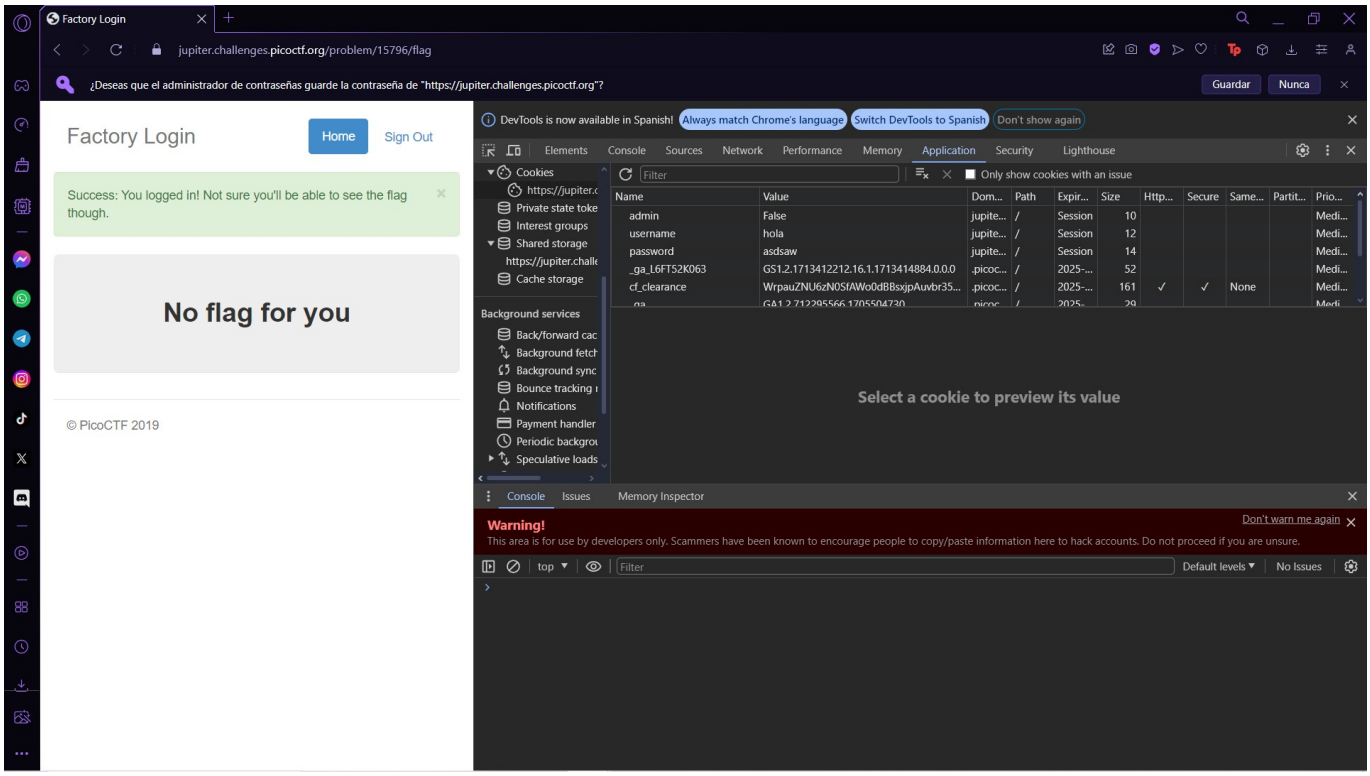
9%|▉ | 9/96 [00:05<00:53, 1.62it/s]Admin bit found in byte 9 bit 0. Flag: picoCTF{cO0ki3s_yum_e40d16a9}

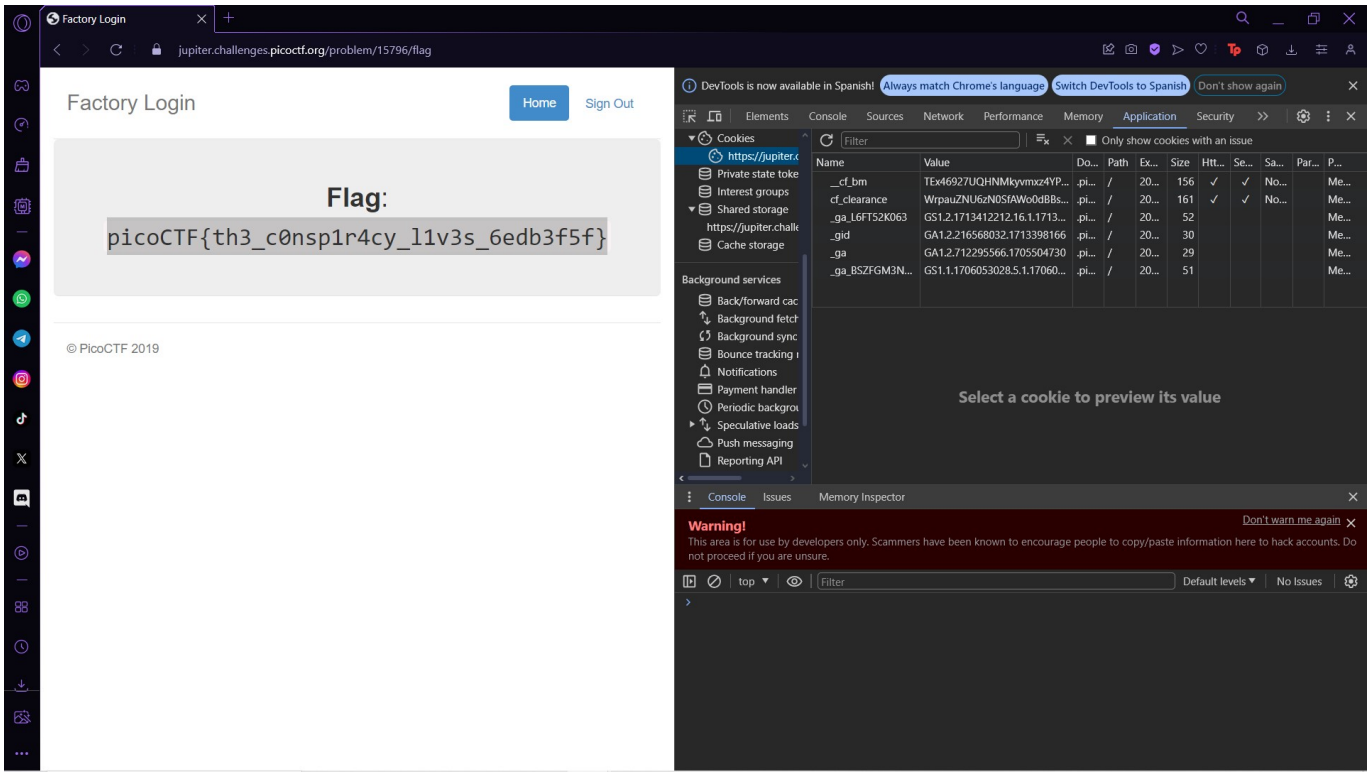
Dont-use-client-side



picoCTF{no_clients_plz_7723ce}

logon





Who are you?

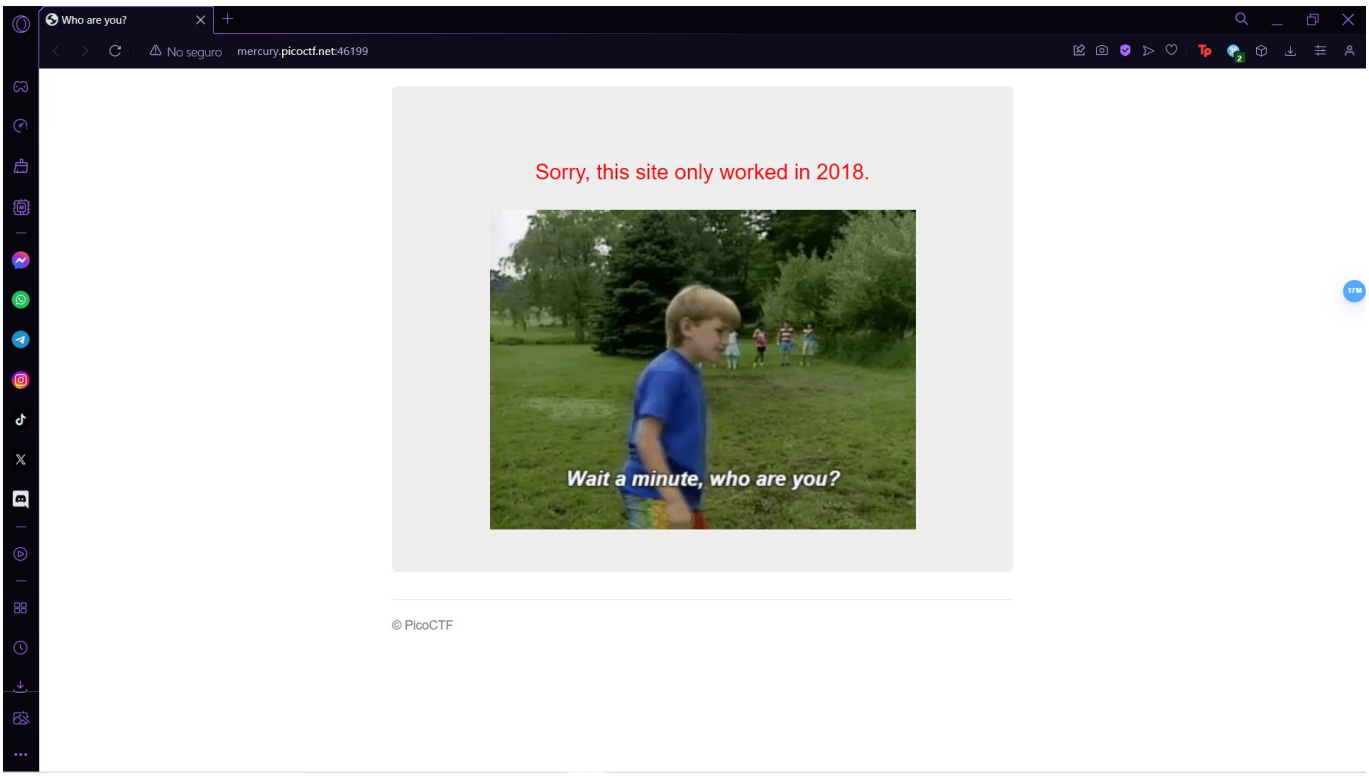
User-Agent: PicoBrowser

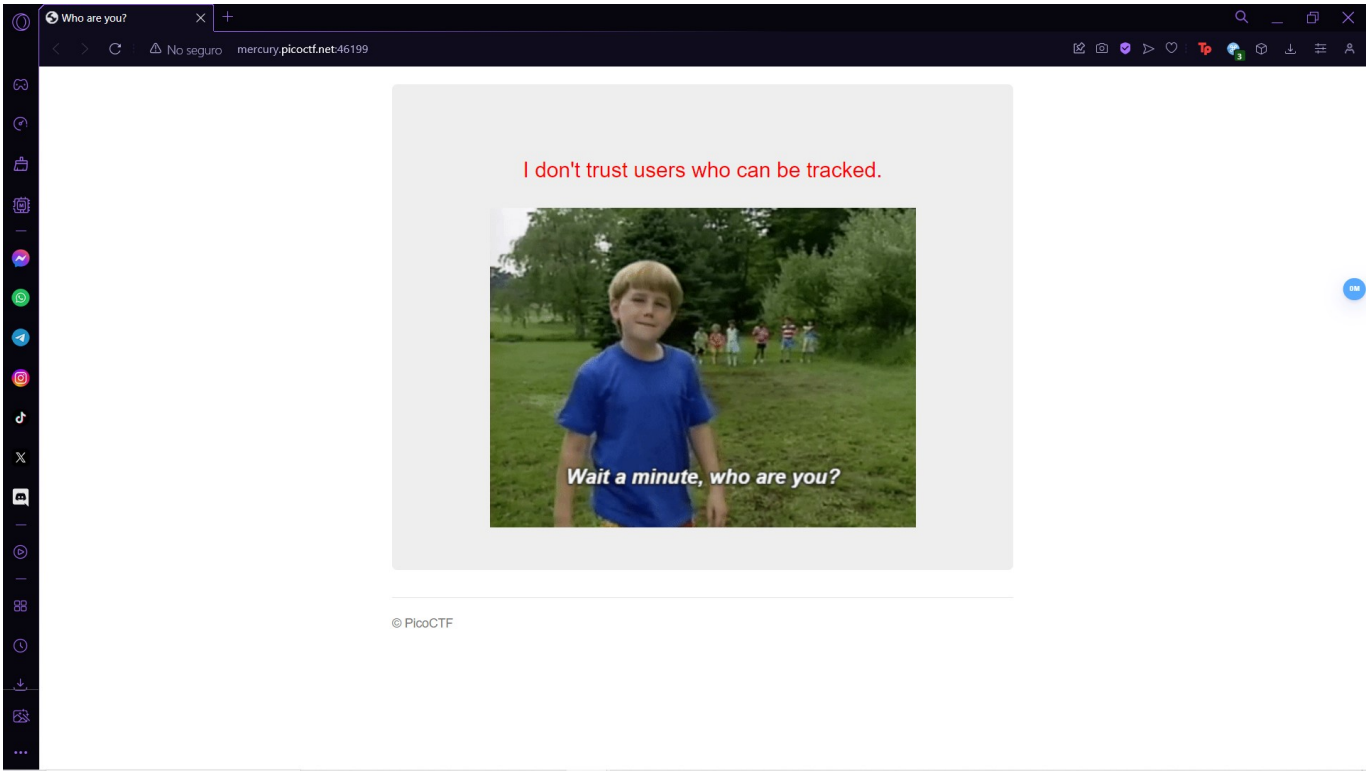
Date: 2018

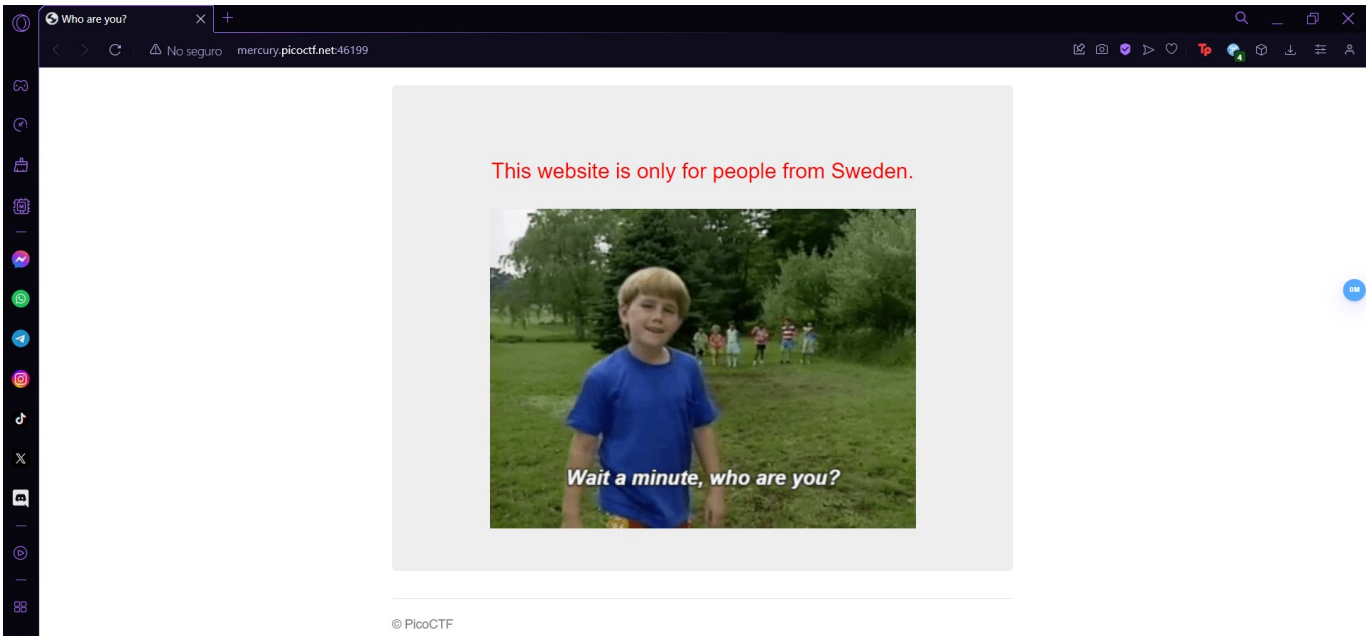
DNT: 1

X-Forwarded-For: 2.16.66.0

Accept-Language: sv






Who are you?
No seguro
mercury.picoctf.net:46199
This website is only for people from Sweden.
Wait a minute, who are you?
© PicoCTF