Some Assembly Required 1 70 points

<http://mercury.picoctf.net:40226/index.html>

Well one thing is for sure! I suck at working with confiscated Javascript, I remember spending hours on figuring this out but I just couldn’t! Make sure to check out the source to find where I got the answer from!

Currently we have received a button that will check the flag for us:

Graphical user interface, application

Description automatically generated

What this means is that the flag is hidden in the confiscated Javascript (Ofcorse irl that won’t be the case, just for this flag)

When checking the JavaScript an ugly blob of js code has been given:



The first thing we should do is beautify this js code in order to at least a little better understand what it is trying to do using: <http://jsnice.org/>

Text

Description automatically generated

Still not too clear.. Javascript is definitely not my best language and with all the weird letters and popping going on it is not getting any easier!

In order to find out what things mean we can use the developer console to find out what some of these const’s mean, there are 2 const’s that stand out: findmiddleposition and navigatePop.

Text

Description automatically generated

Text

Description automatically generated

First we need to define navigatePop in the console using the same value used in the javascript code so first we do:

const navigatePop = \_0x4e0e;

When we got navigatePop defined we can start checking out what these values actually mean

navigatePop(484)

Graphical user interface, text, application

Description automatically generated

Going through all these values we can get a better image of what the Javascript code is actually trying to do!

Text, letter

Description automatically generated

After this things in the guide got overly complicated for the level of the guide so I looked somewhere else and learned that the flag was fetched from somewhere:

Text

Description automatically generated

When downloading this file and opening in with NotePad++ the code flag was fully visible

Text

Description automatically generated

picoCTF{cb688c00b5a2ede7eaedcae883735759}

Note: looking back a lot of this wasn’t needed in order to find this flag but it was definitely a really useful learning experience that will come in handy for the next flags!