Some Assembly Required 1 more advanced 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

I continued following the guide in order to learn more about web assembly as that is definitely an important thing to know for later!

First thing we do is find the Javascript link which is at:

<http://mercury.picoctf.net:40226/G82XCw5CX3.js>

Then we are able to do:



Wget is a noninteractive download utility for files on the web

First we put in the link

Then we say -q so it doesn’t display any output spam

And -O is used to print it to a file

And we will name it script, .wasm means WebAssembly file



When using: vi script.wasm we can check the contents

A picture containing timeline

Description automatically generated

We can already see the flag in here but for learning purpose we keep going in order to make this in clear text!

In order to do this I used wasm2wat and converted it:

wasm2wat script.wasm > script.wat

now we have the entire file in readable assembly code!

A screenshot of a computer

Description automatically generated

Once again we can see the picoCTF flag but for learning purposes I went and started commenting the important parts.

The code starts with a lot of stuff we won’t care about but then we will get out first function: strcmp which is once again not important so we will skip past that..

Directly after that comes: check\_flag and check\_flag which are for reference seen in the javascript code:

Text

Description automatically generated

In order to create a more clearer output we can also convert the webassembly to pseudocode using:

wasm-decompile script.wasm > script.dcmp

A computer screen capture

Description automatically generated with medium confidence