PicoCTF Some Assembly Required 2 110 points

<http://mercury.picoctf.net:44570/index.html>

Another some assembly required, this is a follow p to the 1st part!

It’s the same layout as before:

A picture containing graphical user interface

Description automatically generated

With a long line of Javascript once again, the first thing we will do is nice it using: <http://jsnice.org/> :

Text

Description automatically generated

In order to do this one right we have to dig a little deeper and check out the web assembly! Using the ./ link we can find in the Javascript: A screenshot of a computer

Description automatically generated with medium confidence

I’ll start with getting the raw web assembly by doing:

wget [http://mercury.picoctf.net:44570/aD8SvhyVkb -q -O script.wasm](http://mercury.picoctf.net:44570/aD8SvhyVkb%20-q%20-O%20script.wasm)

I’ll then convert the wasm to wat and dcmp for readability of the web assembly

wasm2wat script.wasm > script.wat

wasm-decompile script.wasm > script.dcmp

first of all we see that the code is around the same as the code from assembly 1 with some extra lines added to it! Graphical user interface, text, application

Description automatically generated

Knowing this we can assume that the flag is once again at the top but this time its hidden: Shape

Description automatically generated with low confidence

At:

var i:int = g ^ h;

In:



We can see g (e[3]) being XOR’ed (^) by 8 (h)

We can simply revert this XOR by doing a simple python script:



Outputting:

b'picoCTF{64e2a9691192fcbd4aa9b8f5ee8134a2}T88T88'

picoCTF{64e2a9691192fcbd4aa9b8f5ee8134a2}