Flag Dance

Reverse Engineering/Misc

Easy



Flag: MOCSCTF{y0u\_can\_d0\_rever5e\_0r\_brutef0rce}

Challenge: Would you please help to give me the correct Flag Dance Code? (Remember to adjust to flag format MOCSCTF{ …..} 🡨 capital letter for ‘MOCSCTF’)

https://scratch.mit.edu/projects/768795855

Scratch account just in case needed:

username: mocsctf

password: M0C5CTF2023

Writeup:

With play around the program, user need to input a 4 digit input, if it’s correct then it’s expected that the flag will be shown. Otherwise just ‘No flag!’ is shown.

By investigating the program, actually the program relies on some calculation including user input and ‘memory’ variable as show below. And each element within ‘memory’ variable will form it’s own output, without influencing other elements within ‘memory’ variable.

Graphical user interface

Description automatically generated with medium confidence

In this case we may come up 2 approaches, first is to use brute force (as the input is only 4 digit numbers) or try to have all the elements in ‘memory’ variable divided by each of 4 digit number (0001-9999), then transform to character (a-z,0-9,{}-\_ as in the program) to see if any of the 4 digit number can make the output include ‘mocsctf{’ (as some of the elements may provide no output!)

Now we can change the program to below code for brute force. And run the program (Need to wait some time):

Graphical user interface

Description automatically generated with medium confidence

Can get the flag when input is 6194:

Graphical user interface, website

Description automatically generated