**Traceme1**

Reverse engineering - Easy

Challenge: Please find the message which is not in case of “Fail” and submit it with flag format.

flag: mocsctf{Y0u\_w1n\_0verf10w!}

1. Open the exe file with debugger like Olly. Press “run” button until the prompt is shown:

Graphical user interface

Description automatically generated

1. Try to input a password with normal way. e.g. AAAABBBBCCCCDDDD:

Shape, rectangle

Description automatically generated

Shape, rectangle

Description automatically generated

It will directly jump to “Fail!” and terminate the program. Even we try to lay some breakpoints in the program.

1. Try to provide longer input to see if we can trigger buffer overflow:

Text

Description automatically generated

1. We can overflow the program. And code preceding the crash is from 00401250:

Graphical user interface

Description automatically generated with medium confidence

Text

Description automatically generated with low confidence

1. Use “Follow in Disassembler” to trace the related code before crash. As it’s possible that the code address there is closed to program output, which we may be able to find output of different cases:

Graphical user interface, text

Description automatically generated with medium confidence

1. Scroll up to the top, the code starts at 00401000, then scroll down the code space a bit, we observe the output which is not the case of “Fail!”, so we can get the flag - mocsctf{Y0u\_w1n\_0verf10w!} :

Graphical user interface

Description automatically generated with medium confidence