**Traceme3**

Reverse engineering - Easy

Challenge: Please find the correct input.

flag: mocsctf{1t\_15\_@\_m@5k3d\_c1pher}

1. First, we recognize the program is for Linux environment:



1. Use tools like IDA pro to decompile the code of main function:

Graphical user interface, text, application

Description automatically generated

1. Found there is a function called “check\_pw”. Continue to chase the code for this function:

Graphical user interface, text, application

Description automatically generated

1. From the highlighted code, the checking is to compare each byte of variable a1 to corresponding byte of variable a2 and minus offset of a3. Mapped to the original main function, a1 -> v3, a2->v8, a3->v5
2. Back to main function, actually we can find that v8 is actually a string and v5 can be converted to hex to get the actual offset to align the comparison in byte under check\_pw:

Text

Description automatically generated

1. The actual order of the characters are reversed in each of variable. e.g. {iuhudop actual order is poduhui{. For 0x3010502010003LL the actual offset order is 03,00,01,02,05,01,03. With this approach we can get the below table for the input required:

Table

Description automatically generated

1. Use the expected input as argument of the program and run the program in Linux:



A picture containing text, shoji, crossword puzzle, light

Description automatically generated

mocsctf{1t\_15\_@\_m@5k3d\_c1pher}