

# ./level09



Decompiled file with *Ghidra*:



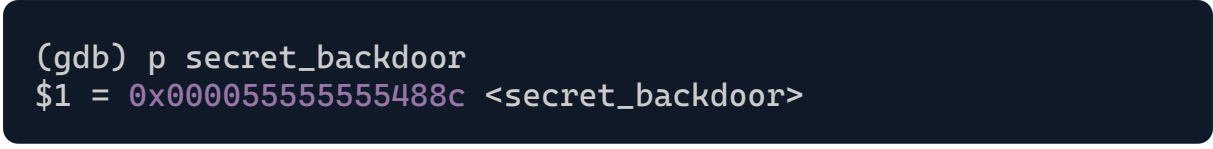
The program is in **64-bit** mode, which means addresses are 8 bytes long.  
The program includes a **secret\_backdoor** function, which allows executing a **system** command that we specify. In this exercise, the interesting part happens within the **handle\_msg** function, where there's a defined structure, consisting of:



Next, there are two functions that allow us to enter a username and a message, storing them inside the **MessageData** structure. The **set\_username** function allows entering a **41**-character username, creating a **buffer overflow** opportunity. Thus, we can **overwrite** the least significant byte of **msglen**, which is an int located just after the username, and set it the maximum **0xff**.

This enables an overflow on the **msg**, as the **msglen** specifies the number of bytes that **strncpy** copies. Consequently, we can overwrite the **handle\_msg** return address, rerouting the execution of the program to the **secret\_backdoor** function.

First, let's find the address of the secret\_backdoor function:



The final step is to find the exact offset between msg pointer and the return address of the handle\_msg function's stack frame:

