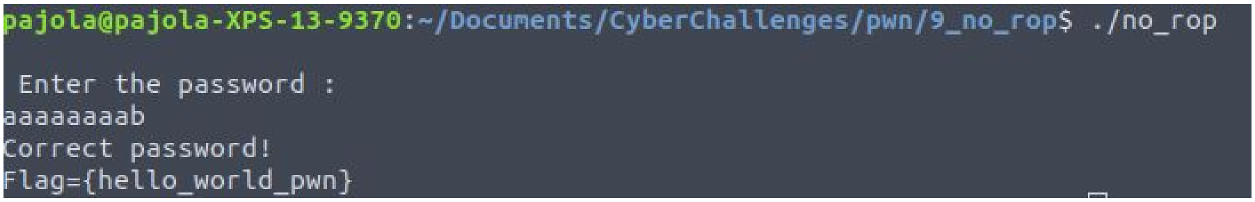
Pwn 9: No Rop

This challenge addresses the classic buffer overflow attacks aimed at corrupting the values of program's variables.

We are asked to reach the *print_flag* instruction on line 18 and, in order to execute it, the variable *pass* should be "true". Let's explain the idea: in *C*, when we have a condition such as *if(variable)*, this will be true for any value of *variable* other than zero. Considering this, we can just set the variable *pass* to something that is not zero in order to capture the flag, i.e., any random value is ok.

Well, the solution is quite naive: suppose that the two memory zones are placed continuously, we just need to manually insert 9 characters in order to solve the exercise and, of course, reach the flag.



```
pajola@pajola-XPS-13-9370:~/Documents/CyberChallenges/pwn/9_no_rop$ ./no_rop

 Enter the password :
aaaaaaaab
Correct password!
Flag={hello_world_pwn}
```