Exercise 4

Alberto Martin Lionardi , 7001812

January 2023

1 Task 1

a) `flag{YOUR_NAME_MAKES_MY_HEART_BLEED}`

2 Task2

a) `flag{CANARY_IS_A_SMALL_SONG_BIRD}`

3 Task3

a) `flag{can_i_get_a_cve_for_this_?}`
b) with p.recvline(), we can just do

```
libc = p.libc
system_addr = libc.sym['system']
```

Then we could easily get the system addres.
c) if this is possible to print system function or any other function from a setuid binary, attacker could just bypass ASLR, and security implication on privilage escalation