

Esame Software Security Gennaio 2022
Docente: Andrea Lanzi
(Tempo: 3 ore)

Dato il programma vuln.c, scrivere due exploit in python che effettuano la seguente sequenza di operazioni:

- 1) Exploitare la funzione vuln ed eseguire una shell di sistema.
- 2) Stampare la stringa "you Win!!!" sempre sfruttando la vulnerabilità definita all'interno della funzione vuln. (get_input->vuln->flag)

Per ogni exploit descrivere la metodologia utilizzata. Mostrare come sono stati estratti i vari indirizzi di memoria, riportare lo script in python che contiene l'exploit e la prova in screenshot della sua esecuzione che mostra con quali parametri vengono lanciati gli exploit.

Shellcode da utilizzare:

```
shellcode=(b"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80")
```