

## **Esame Software Security Luglio 2022**

**Docente: Andrea Lanzi**

**(Tempo: 2 ore e mezza)**

Dato i programmi bof.c e rop.c, definiti nelle rispettive directory, scrivere due exploit in python che effettuano la seguente sequenza di operazioni:

- 1) bof.c eseguire lo shellcode, sfruttando la strcpy definite nella print\_function.
- 2) rop.c exploitare la vulnerabilità in modo che venga stampata la stringa "Congratulations user you win", dove user è il vostro nome.

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")
```