

BOF-Buffer Overflow

posizioniamoci sul desktop via `cd desktop`

creiamo un nuovo file con il comando `touch` e chiamiamolo `BOF.C`

Adesso come da consegna editiamo il file appena creato , userò l'editor di testo `nano`

e scriviamo un breve script che salverà in memoria un numero preciso di caratteri

```
#include <stdio.h>

int main (){

char buffer [10];

printf("si prega di inserire il nome utente:");
scanf("%s", buffer);

printf("nome utente inserito: %s\n", buffer);

return 0;
}
```

salviamo dunque e successivamente compiliamo il file
per fare ciò digitiamo :

`gcc -g BOF.c -o BOF`

adesso eseguiamo lo script digitando

`./BOF.c`

```
./BOF.c
si prega di inserire il nome utente:woeqmjoinqeqweqwdjbcqlcweqw
nome utente inserito: woeqmjoinqeqweqwdjbcqlcweqw
zsh: segmentation fault ./BOF
```

come previsto, se inseriamo oltre 10 caratteri otteniamo un errore , basterà cambiare il numero di caratteri cambiando il valore tra parentesi quadre