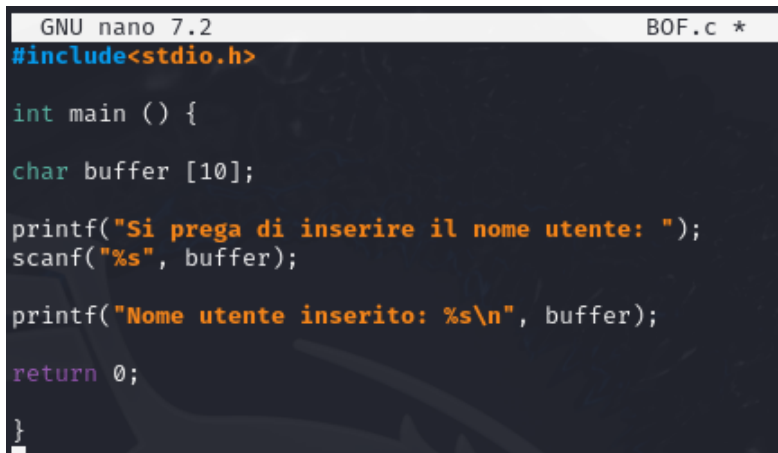


ESERCIZIO S7L4

Traccia: Dato un codice .c che cerca di riprodurre un errore di segmentation fault a causa del buffer overflow, si cerca di riprodurre lo stesso errore aumentando la dimensione del parametro di input.

SVOLGIMENTO

Inizialmente si crea il codice BOF.c come mostrato nella figura sottostante. Questo codice accetta in input una stringa di lunghezza massima di 10 caratteri.



```
GNU nano 7.2 BOF.c *
#include<stdio.h>

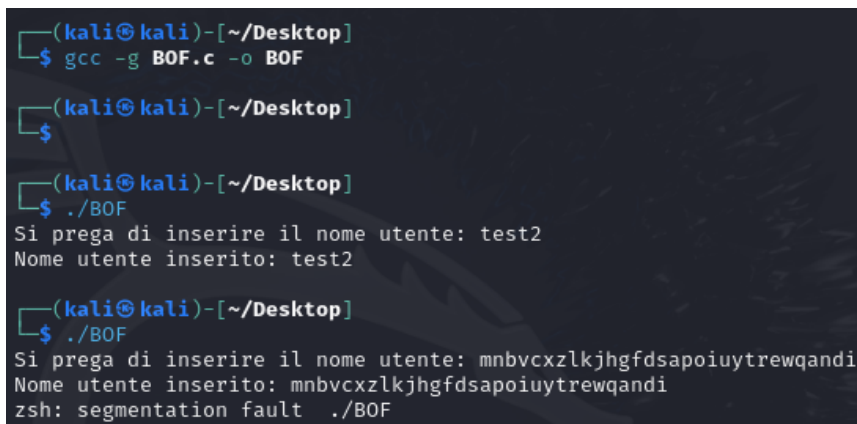
int main () {
char buffer [10];

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

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

return 0;
}
```

Dopo aver compilato il codice con il comando **gcc -g BOF.c -o BOF**, ed eseguito con il comando **./BOF**, il codice ci richiede di immettere un input senza specificarne la lunghezza. Immettendo un qualunque input di lunghezza maggiore di 10 caratteri, si otterrà un errore di **Segmentation fault**, ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere. In questo caso è stato inserito un input di lunghezza 30 caratteri.



```
(kali㉿kali)-[~/Desktop]
$ gcc -g BOF.c -o BOF

(kali㉿kali)-[~/Desktop]
$

(kali㉿kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: test2
Nome utente inserito: test2

(kali㉿kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente: mnbvcxzlkjhgfdsapoiuytrewqandi
Nome utente inserito: mnbvcxzlkjhgfdsapoiuytrewqandi
zsh: segmentation fault ./BOF
```

Sotto richiesta dell'esercizio si va ad aumentare la dimensione dell'input a 30 caratteri, e si cerca di riprodurre lo stesso errore di segmentation fault.

```
GNU nano 7.2 B0F.c
#include<stdio.h>

int main () {
char buffer [30];

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

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

return 0;
}
```

Dopo aver modificato il codice, averlo ricompilato ed eseguito, per ottenere un errore di segmentation fault si va ad inserire un input di dimensione maggiore di 30 caratteri.

```
(kali㉿kali)-[~/Desktop]
$ ./B0F
Si prega di inserire il nome utente: maquantoebelloquestoeserciziomistodivertendotanto
Nome utente inserito: maquantoebelloquestoeserciziomistodivertendotanto
zsh: segmentation fault ./B0F

(kali㉿kali)-[~/Desktop]
$
```