Creiamo il file in c con il programma che poi andremo ad eseguire

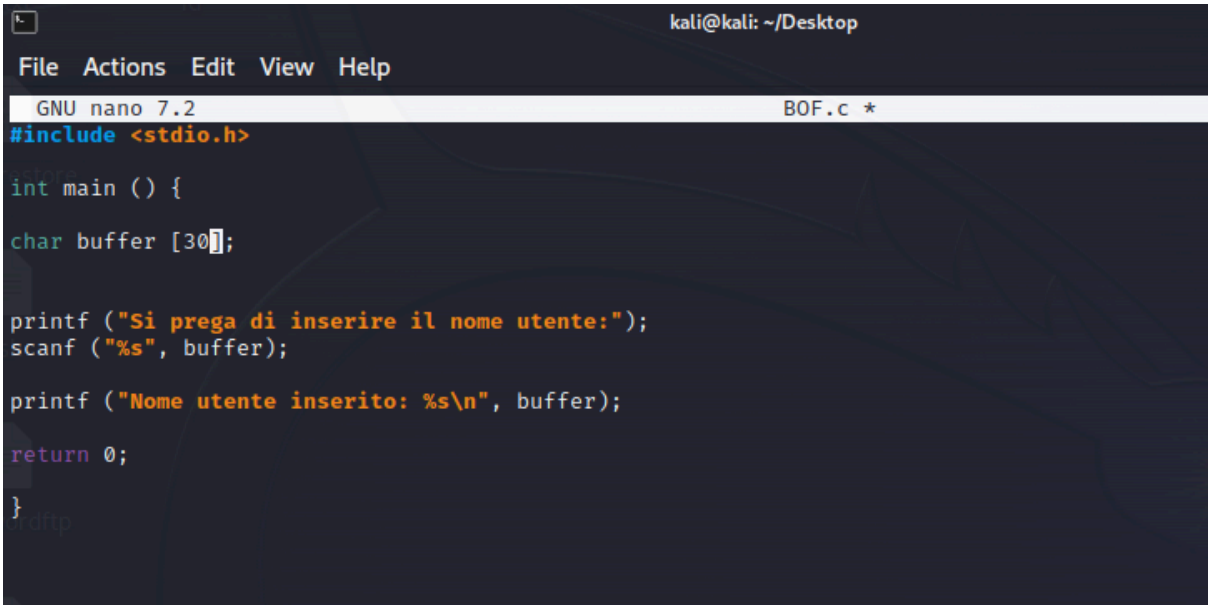
```c
#include <stdio.h>


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;

}
```

Utilizzando il programma inseriamo il nome utente, affinché inseriamo un nome pari o inferiore a 10 non abbiamo problemi, mentre quando inseriamo un nome superiore a 10 ci da errore e avviene il fenomeno del buffer overflow.

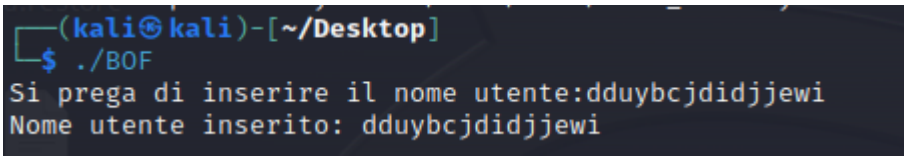
```
┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -g BOF.c -o BOF

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

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

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Per attenuare questo problema aumentiamo la dimensione del vettore a 30

Creiamo il file in c con il programma che poi andremo ad eseguire



ora possiamo notare che si accettano anche nomi utenti superiori a 10, ma inferiori a 30



BUFFER OVERFLOW

Il buffer overflow è una vulnerabilità informatica in cui un programma non controlla correttamente la quantità di dati che accetta in un buffer di memoria temporanea. Quando vengono inseriti più dati di quelli previsti nel buffer, il superfluo può sovrascrivere aree di memoria adiacenti, causando malfunzionamenti, crash del programma o, in alcuni casi, permettendo ad un attaccante di eseguire codice dannoso.