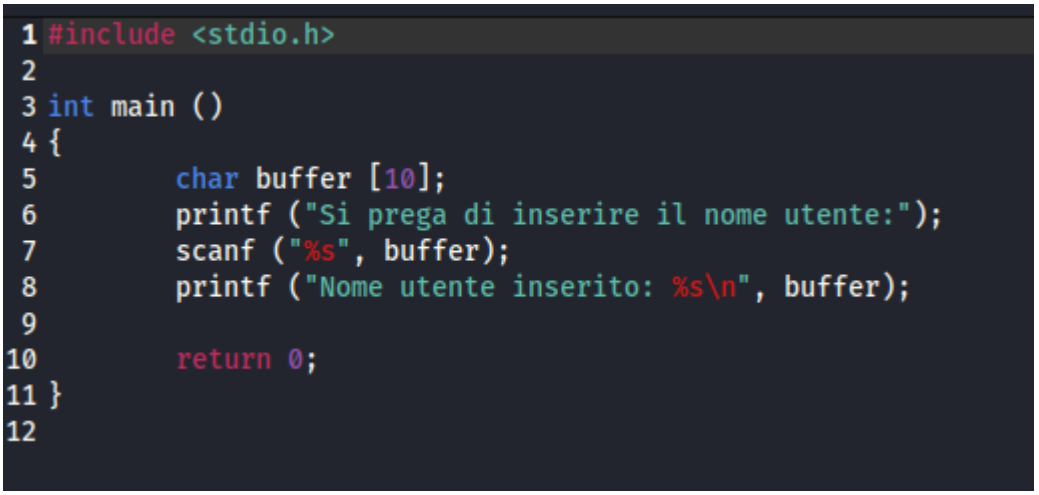
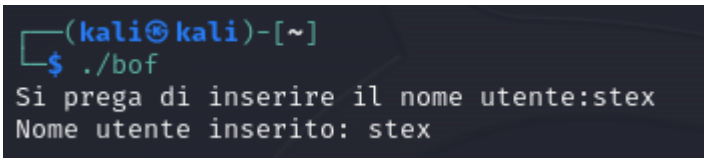
Nell’esercizio di oggi eseguiremo la dimostrazione di un buffer overflow attraverso un piccolo programma scritto in linguaggio C.
Un buffer overflow è una condizione di errore in presenza del quale viene eseguita una sovrascrittura delle aree di memoria adiacenti a quelle usate dal programma. È un difetto di programmazione che può portare a comportamenti imprevedibili, come per esempio crash del programma o del computer e si verifica quando vengono scritti dati in quantità maggiore di quelli attesi.



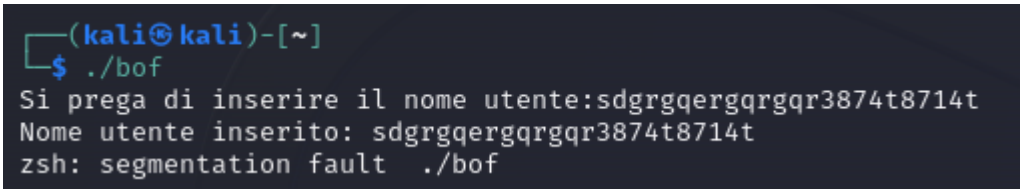
```c
#include <stdio.h>

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;
}

```

Possiamo vedere nell’immagine sopra il codice del programma. Si può notare come la variabile buffer abbia una dimensione massima di 10 caratteri.



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

Inserendo un numero di caratteri inferiori non succede niente di strano.
Proviamo ad inserirne di più:



```
┌──(kali㉿kali)-[~]
└─$ ./bof
Si prega di inserire il nome utente:sdgrgqergqrgqr3874t8714t
Nome utente inserito: sdgrgqergqrgqr3874t8714t
zsh: segmentation fault  ./bof
```

Come possiamo vedere il programma ci restituisce un errore. Questo perché non vi sono istruzioni per gestire questa casistica.
Adesso aumentiamo la grandezza massima del vettore.

```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;
}

```

Come possiamo vedere adesso la dimensione massima è di 30 caratteri.

```
┌──(kali㉿kali)-[~]
└─$ ./bof
Si prega di inserire il nome utente:370Y7Y047QV7836087QV46Q978YÒOÒAYNOYV4W9T83A4Y9487Y4983750968Q73YO479VQY3A7YP9844VNZWON9VA47TYO7A9V
B8A8Y4N
Nome utente inserito: 370Y7Y047QV7836087QV46Q978YÒOÒAYNOYV4W9T83A4Y9487Y4983750968Q73YO479VQY3A7YP9844VNZWON9VA47TYO7A9VB8A8Y4N
zsh: segmentation fault  ./bof
```

Ma comunque inserendo un numero di caratteri maggiori ci darà comunque un errore.
Questo tipo di errore è molto pericoloso perché può essere usato per prendere il controllo di un sistema.