Quest'oggi andrò a fare un codice in linguaggio C che è intenzionalmente vulnerabile agli attacchi di tipo Buffer Overflow (BOF), e cercherò di provocare un errore specifico noto come "segmentation fault". Quest'ultimo è un errore di memoria che si verifica quando un programma tenta inconsapevolmente di scrivere in una posizione di memoria dove tale operazione non è consentita, come ad esempio in una zona di memoria dedicata alle funzioni del sistema operativo.

```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;
}

```

Se inserisco 30 caratteri il programma ci ritorna un errore, «segmentation fault», ovvero errore di segmentazione. L'errore di segmentazione avviene quando un programma tenta di scrivere contenuti su una porzione di memoria alla quale non ha accesso. Questo è un chiaro esempio di BOF, ho inserito 30 caratteri in un buffer che ne può contenere solamente 10 e di conseguenza alcuni caratteri stanno sovrascrivendo aree di memorie inaccessibili:

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

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

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

Provo a ridurre l'errore di segmentazione aumentando la dimensione del vettore a 30:

```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;
}

```

Notiamo come ora il problema comunque persiste, in quanto se digito una stringa con più di 30 caratteri il programma ci ritorna sempre l'errore di segmentazione:

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

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

┌──(kali㉿kali)-[~/Desktop]
└─$
```