Buffer overflow

La traccia di oggi era quella di testare il buffer overflow, questa vulnerabilità che è la conseguenza di un mancato controllo sull' input dell' utente. Il nostro test in particolare era sul seguente codice in c.

```c
#include <stdio.h>

int main() {

char buffer [10];

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

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

return 0;

}
```

Un volta scritto il codice bisognava compilare con il comando **gcc -g BOF.c -o BOF**. Andiamo poi a testare l' esecuzione prima con un inserimento che rientrasse nella grandezza del vettore come di seguito:

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

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

Di testarlo poi dopo andando a forare il vettore come di seguito:

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

Come si può vedere il programma ci riporta un errore, significa quindi che abbiamo inserito un numero di caratteri superiore rispetto a quello che si aspetta il buffer che abbiamo impostato andando a sovrascrivere aree di memorie inaccessibili.

Ho poi modificato la grandezza del vettore a 30 testando di nuovo il programma. In questo caso l’errore non apparirà poiché non abbiamo sforato il buffer.

```c
#include <stdio.h>


int main() {

char buffer [30];


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

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

return 0;

}
```

Ma anche in questo caso inserendo più caratteri rispetto a quelli che si aspetta il nostro buffer ci comparirà l’ errore di **segmetation fault:**

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