

Buffer Overflow

Traccia:

Provate a riprodurre l'errore di segmentazione modificando il programma come di seguito:

Aumentando la dimensione del vettore a 30;

Fare la prova dell'errore modificare il codice in modo che l'errore non si verifichi (es aumentare il vettore a 30 o fare dei controlli)

Verificare, modificando il codice, dove va a scrivere i caratteri in overflow

Dopo essermi spostata sul Desktop con il comando **cd Desktop** apro editor nano per scrivere il mio programma

```
(kali㉿kali)-[~]  
$ cd Desktop  
  
(kali㉿kali)-[~/Desktop]  
$ nano BOF.c
```

```
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;  
}
```

Eseguo il comando per compilare il codice in un file eseguibile (da rifare ogni volta che faccio modifiche al file) ed infine passo all'esecuzione avviando il programma.

```
(kali㉿kali)-[~/Desktop]  
$ gcc -g BOF.c -o BOF  
  
(kali㉿kali)-[~/Desktop]  
$ ./BOF  
Si prega di inserire il nome utente: Airam  
Nome utente inserito: Airam  
  
(kali㉿kali)-[~/Desktop]  
$ ./BOF  
Si prega di inserire il nome utente:123456789012345678901234567890  
Nome utente inserito: 123456789012345678901234567890  
zsh: segmentation fault ./BOF
```

Noto che inserendo un numero di caratteri superiore rispetto al numero massimo di caratteri stabilito dal programma ottengo un errore *segmentation fault*

Modificando il codice del programma porto il limite massimo a 30.

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

int main () {
//aumento la dimensione del vettore a 30
char buffer [30];

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

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

return 0;
}
```

inserisco in input 30 caratteri e noto che non ricevo più l'errore sopra citato.

```
(kali㉿kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente:123456789012345678901234567890
Nome utente inserito: 123456789012345678901234567890
```

Inserendone più di 30 noto che l'errore si ripresenta.

```
(kali㉿kali)-[~/Desktop]
$ ./BOF
Si prega di inserire il nome utente:1234567890123456789012345678901234
5678901234567890
Nome utente inserito: 123456789012345678901234567890123456789012345678
90
zsh: segmentation fault ./BOF
```