

# **BUFFER OVERFLOW**



# INTRODUZIONE

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma scrive più dati in un buffer di quanti ne possa contenere, sovrascrivendo così la memoria adiacente. Questo può portare a vari problemi, inclusi crash del programma, corruzione dei dati e, in alcuni casi, esecuzione di codice arbitrario da parte di un attaccante.

Il codice accanto è un esempio classico di potenziale vulnerabilità di buffer overflow. La funzione scanf legge un input da tastiera e lo memorizza nel buffer. Tuttavia, non c'è alcun controllo sulla lunghezza dell'input, il che può portare a un buffer overflow se l'utente inserisce una stringa più lunga di 30 caratteri.

```
3 #include <stdio.h>
4
5 int main (){
6
7     char buffer [30];
8
9     printf("Si prega di inserire il nome utente: ");
10    scanf("%s", buffer);
11
12    printf("Nome utente inserito: %s\n", buffer);
13
14    return 0;
15 }
16
```

Infatti andando ad inserire in input una stringa più corta di 30 non avremo nessun problema, però se ne inseriamo una più lunga ci appare un errore di segmentazione.

```
└─(kali㉿kali)-[~/Desktop/Epicode/S7_L4]
$ gcc -g BOF.c -o BOF

└─(kali㉿kali)-[~/Desktop/Epicode/S7_L4]
$ ./BOF
Si prega di inserire il nome utente: qwertyuioplkmjnbgvfcdxszasxdcffdebyb
Nome utente inserito: qwertyuioplkmjnbgvfcdxszasxdcffdebyb

└─(kali㉿kali)-[~/Desktop/Epicode/S7_L4]
$ ./BOF
Si prega di inserire il nome utente: qwertyuiopèokijuhgfdsgf
Nome utente inserito: qwertyuiopèokijuhgfdsgf

└─(kali㉿kali)-[~/Desktop/Epicode/S7_L4]
$ ./BOF
Si prega di inserire il nome utente: qwqerxctyuijkoiyxcvyjbuijokòlkvbjnlkòlkcjgvhbnjb
Nome utente inserito: qwqerxctyuijkoiyxcvyjbuijokòlkvbjnlkòlkcjgvhbnjb
zsh: segmentation fault ./BOF
```

# Come Prevenire il Buffer Overflow

Per prevenire questa vulnerabilità, si può limitare la lunghezza dell'input che scanf legge, utilizzando il modificatore di larghezza nel formato della stringa. Così se in input viene inserita una stringa più lunga essa verrà troncata a 29 caratteri.

```
2
3 #include <stdio.h>
4
5 int main (){
6
7     char buffer [30];
8
9     printf("Si prega di inserire il nome utente: ");
10    scanf("%29s", buffer);
11
12    printf("Nome utente inserito: %s\n", buffer);
13
14    return 0;
15 }
16 |
```