

## Report Vulnerabilità Buffer Overflow

Per questo attacco abbiamo sfruttato una vulnerabilità nel codice ovvero il limite del buffer, che ci permetteva di occupare spazio di memoria non dedicato a noi.

```
GNU nano 7.2 /home/kali/Desktop/ esempio.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 vediamo il limite dell'array è 30, quindi avremo un determinato spazio di memoria massimo per inserire il nome utente, se proviamo a inserire un nome utente con più di 30 caratteri il sistema andrà in buffer overflow, come vediamo dall'errore che viene riportato:

```
(root@kali)-[/home/kali/Desktop]
# ./esempio
Si prega di inserire il nome utente:123456789101112131415161718192021222324252627282930
Nome utente inserito: 123456789101112131415161718192021222324252627282930
zsh: segmentation fault ./esempio
```

In questo modo, l'attaccante potrebbe sovrascrivere posizioni di memoria adiacenti che contengono informazioni critiche, come puntatori a funzioni o indirizzi di ritorno.

Ciò può portare a due tipi principali di attacchi: accesso non autorizzato ed esecuzione di codice.