

BUFFER OVERFLOW

FRANCESCO PERSICHETTI

Esempio di esercizio in C vulnerabile al BOF (buffer overflow)

Scrivo il mio codice in C dove imposto che l'utente può inserire una stringa di massimo 10 caratteri, con il comando "sudo nano BOF.c"

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

L'esempio di codice sarà così

```
File Actions Edit View Help
GNU nano 6.4
#include <stdio.h>

int main () {
char buffer [10];

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

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

return 0;
}
```

Eseguendolo e lanciandolo vedremo che una stringa entro i 10 caratteri verranno accettati

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

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

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

Nel caso scrivessi una stringa più lunga mi restituirà l'errore "segmentation fault" ossia errore di segmentazione che avviene quando il programma tenta di sovrascrivere dati in una porzione di memoria a cui non ha accesso

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

Si può risolvere aumentando le dimensioni del buffer

```
File Actions Edit View Help
GNU nano 6.4
#include <stdio.h>

int main () {
char buffer [30];

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

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

return 0;
}
```

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