

Buffer Over Flow

- Il BOF (Buffer Over Flow) è un errore che si verifica quando un'applicazione non viene “sanitizzata” durante la programmazione. Come possiamo vedere nello screenshot successivo andando ad inserire oltre 30 caratteri si verifica l'errore BOF.

Buffer Over Flow

~/Desktop/BOF.c - Mousepad

File Edit Search View Document Help

File Edit Search View Document Help

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

kali@kali: ~/Desktop

File Actions Edit View Help

(kali@kali)-[~]
\$ cd

(kali@kali)-[~]
\$ cd Desktop

(kali@kali)-[~/Desktop]
\$ ls

BOF.c	DirBusterReport-192.168.49.101-80.txt	Nessus-10.7.0-ubuntu1404_amd64.deb
brute3.py	dvwa_test.py	portscan.py
bruteDvwaGet.py	head.py	pratic3.py
brutephp.py	metodo.py	praticas3.py
brute.py	metod.py	starting_point_Ciaska.ovpn

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

(kali@kali)-[~/Desktop]
\$./BOF

Si prega di inserire il nome utenteQuesta è una prova per vedere se riesco a bucare questo esercizio inserendo più di trenta caratteri.
Nome utente inserito: Questa

(kali@kali)-[~/Desktop]
\$./BOF

./BOF: command not found

(kali@kali)-[~/Desktop]
\$./BOF

Si prega di inserire il nome utenteOK
Nome utente inserito: OK

(kali@kali)-[~/Desktop]
\$./BOF

Si prega di inserire il nome utente
Nome utente inserito: sdjbhskdhfbwkjfbwjbfiwfbuqfkhqefhbqlerihfbrbqlerhrrfbvl
vbahfdvldhfvbqlqehflakfhdvblevb
Nome utente inserito: sdjbhskdhfbwkjfbwjbfiwfbuqfkhqefhbqlerihfbrbqlerhrrfbvlvbahfdvldhfv
lqehflakfhdvblevb
zsh: segmentation fault ./BOF

(kali@kali)-[~/Desktop]
\$

Grazie