

# S7 L4

Davide Andreozzi

# Buffer overflow

Abbiamo impostato il valore della variabile buffer a 30 caratteri.

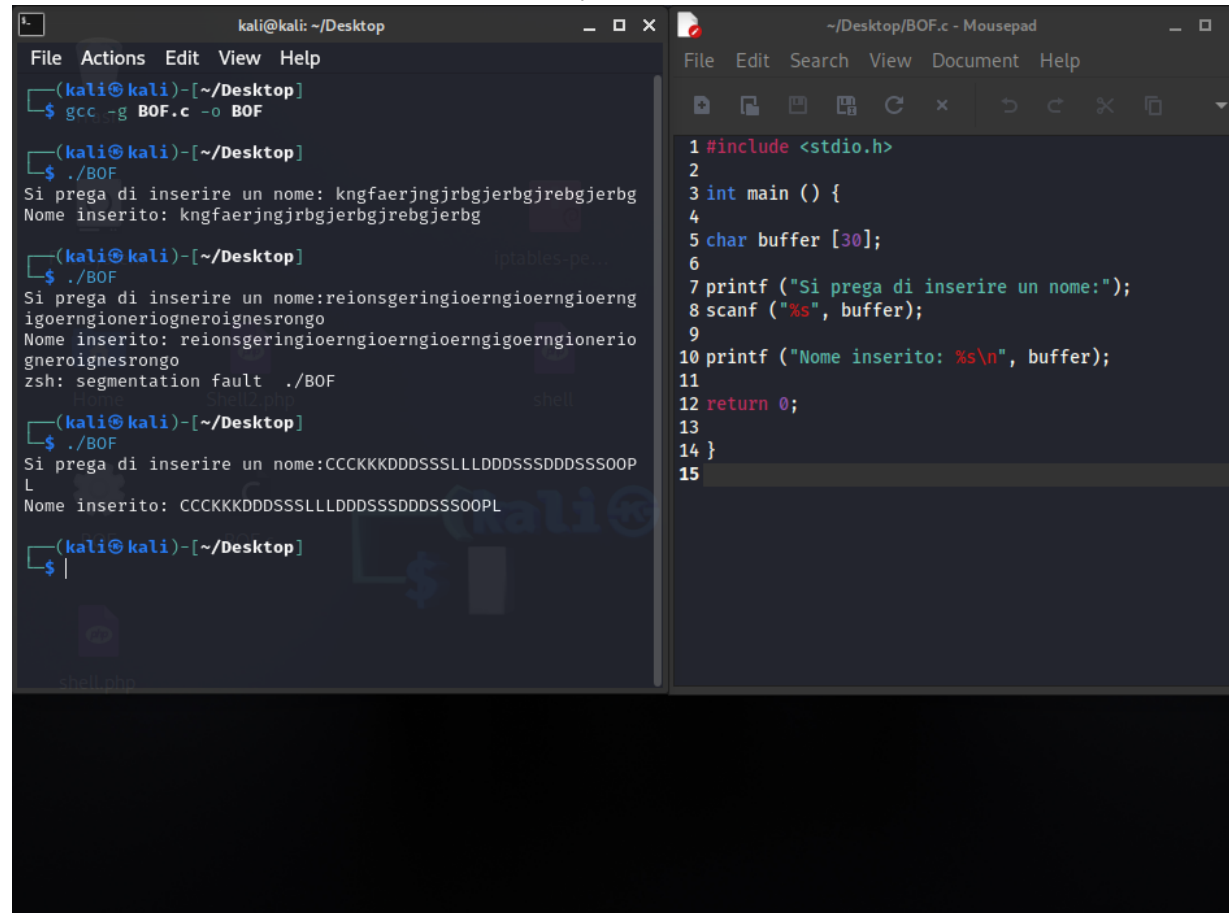
Nel caso centrale abbiamo inserito oltre i 35 caratteri e avviene l'errore in figura.

Mentre andando ad inserire 31 caratteri non abbiamo nessun errore ma ciò non vuol dire che non si verifichi effettivamente un buffer overflow.

Per risolvere il problema in questione andiamo a modificare lo scanf in questo modo:

`scanf("%29s", buffer)`

Così andiamo a leggere al massimo 29 caratteri e evitiamo il problema



The image shows a side-by-side comparison of a C program's behavior before and after a buffer overflow fix. On the left, a terminal window titled 'kali@kali: ~/Desktop' shows the execution of a program named 'BOF'. The first run with a 35-character string works. The second run with a 36-character string results in a 'segmentation fault'. The third run with a 31-character string also results in a 'segmentation fault'. On the right, a code editor titled '~/Desktop/BOF.c - Mousepad' shows the source code. The original code uses 'scanf ("%s", buffer);'. The fixed code, shown in the rightmost part of the editor, changes this to 'scanf ("%29s", buffer);'.

```
File Actions Edit View Help
(kali@kali)~/Desktop
$ gcc -g BOF.c -o BOF

(kali@kali)~/Desktop
$ ./BOF
Si prega di inserire un nome: kngfaerjngjrbgjerbgjrebjgerbg
Nome inserito: kngfaerjngjrbgjerbgjrebjgerbg

(kali@kali)~/Desktop
$ ./BOF
Si prega di inserire un nome:reionsgeringioerngioerngioerng
igoerngioneriogneroignesrongo
Nome inserito: reionsgeringioerngioerngioerngigoerngionerio
gneroignesrongo
zsh: segmentation fault ./BOF

(kali@kali)~/Desktop
$ ./BOF
Si prega di inserire un nome:CCCKKKDDSSSSLLDDSSDDSSSOOP
L
Nome inserito: CCCKKKDDSSSSLLDDSSDDSSSOOPL

(kali@kali)~/Desktop
$ |

~/Desktop/BOF.c - Mousepad
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 un nome:");
8 scanf ("%s", buffer);
9
10 printf ("Nome inserito: %s\n", buffer);
11
12 return 0;
13
14 }
15
```