



EPICODE CS0124

REPORT S7L4

La traccia richiede di creare un file in codice C che possa sfruttare la vulnerabilita' del buffer overflow e di scatenare un segmentation fault

Dopo aver creato il file lo lanciamo su terminale e lo compiliamo e successivamente lo avviamo prima con 10 caratteri e dopo con 30;

In entrambi i casi vediamo che compare la scritta segmentation fault quindi l'operazione e' andata a buon fine.

The screenshot displays two terminal windows side-by-side. The left window, titled '~/Desktop/Esercizi/buffer.c - Mousepad', shows the source code for a C program named buffer.c. The code includes <stdio.h>, defines a char array buffer of size 30, and contains a main function that prompts the user to enter their name and prints it back. The right window, titled 'kali@kali: ~/Desktop/Esercizi', shows the process of compiling and running the program. It starts with 'cd Desktop/Esercizi', followed by 'gcc -g buffer.c -o BOF'. Then, './BOF' is executed, leading to a prompt 'Si prega di inserire il nome utente:' where 'Francesco' is entered. This is repeated with a longer string 'francescoahahahahahahahahahahahahahahahahahahah' which results in a segmentation fault. Finally, another run with 'Andonioahahahahahahahahaaahahahahahahaa' also leads to a segmentation fault.

```
kali@kali: ~/Desktop/Esercizi  
File Actions Edit View 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
```

```
kali@kali: ~/Desktop/Esercizi  
❏  
❏ (kali@kali)-[~]  
$ cd Desktop/Esercizi  
❏ (kali@kali)~/Desktop/Esercizi  
$ gcc -g buffer.c -o BOF  
❏ (kali@kali)~/Desktop/Esercizi  
$ ./BOF  
Si prega di inserire il nome utente:Francesco  
Nome utente inserito: Francesco  
❏ (kali@kali)~/Desktop/Esercizi  
$ ./BOF  
Si prega di inserire il nome utente:francescoahahahahahahahahahahahahahahahahahahah  
Nome utente inserito: francescoahahahahahahahahahahhahahahahahahahahahahah  
zsh: segmentation fault ./BOF  
❏ (kali@kali)~/Desktop/Esercizi  
$ gcc -g buffer.c -o BOF  
❏ (kali@kali)~/Desktop/Esercizi  
$ ./BOF  
Si prega di inserire il nome utente:Andonioahahahahahahahahaaahahahahahahaa  
hahahahahahahahahahahahahahahahahahaahahahahaha  
Nome utente inserito: Andonioahahahahahahahahahahaahahahahahahaaahahahahahah  
ahahahahahahahahahaaaahahahahah  
zsh: segmentation fault ./BOF  
❏ (kali@kali)~/Desktop/Esercizi  
$
```