

# ESERCITAZIONE S7L4

Partendo dal codice originale:

```
GNU nano 7.2
#include <stdio.h>

int main(){
char buffer [10];

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

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

return 0;
}
```

È sufficiente modificare la dichiarazione del buffer, da 10 a 30.

Inserendo una stringa maggiore di 30 caratteri, si può notare che l'errore di segmentazione viene riprodotto correttamente

```
(kali㉿kali)-[~/Desktop]
$ ./flow
Si prega di inserire il tuo nome:123456789123456789123456789123456789123456789
Nome utente inserito: 123456789123456789123456789123456789123456789
zsh: segmentation fault ./flow

(kali㉿kali)-[~/Desktop]
$
```

Per evitare questo tipo di errore, conosciuto come buffer overflow, possiamo modificare il codice come segue

```
GNU nano 7.2 buffer.c
#include <stdio.h>
#include <string.h>

int main() {
    char buffer[30];

    printf("Si prega di inserire il tuo nome: ");

    // Utilizza fgets per leggere la stringa con una dimensione massima specificata
    if (fgets(buffer, sizeof(buffer), stdin) != NULL) {
        // Rimuovi il carattere di nuova linea se presente
        size_t len = strlen(buffer);
        if (len > 0 && buffer[len-1] == '\n') {
            buffer[len-1] = '\0';
        }

        printf("Nome utente inserito: %s\n", buffer);
    } else {
        printf("Errore durante la lettura dell'input.\n");
    }

    return 0;
}
```

La funzione fgets specifica la dimensione massima dell'input, impedendo così che venga superato il buffer. La variabile input è dichiarata come un array di caratteri di dimensione MAX\_INPUT\_LENGTH + 1.

Nel caso in cui l'utente inserisca più di MAX\_INPUT\_LENGTH caratteri, fgets leggerà e memorizzerà solo i primi MAX\_INPUT\_LENGTH caratteri nel buffer input, e i caratteri successivi verranno ignorati. Pertanto, non avrai un buffer overflow in questo caso. La precauzione principale è assicurarsi che la dimensione specificata a fgets sia sufficiente per memorizzare l'input. In questo esempio, ciò è gestito correttamente grazie all'uso di sizeof(input), che riflette la dimensione dell'array.

Eseguendo il codice possiamo notare come il carattere in più viene scartato, prendendo in input solo i primi 30

```
(kali㉿kali)-[~/Desktop]
└─$ ./buffer
Si prega di inserire il tuo nome: 123456789012345678901234567890
Nome utente inserito: 12345678901234567890123456789

(kali㉿kali)-[~/Desktop]
└─$
```

I caratteri in overflow vengono scritti in un'allocazione di memoria che si può rintracciare con l'esecuzione in debug del programma

```
Reading symbols from ./flow...
(gdb) zoom
Undefined command: "zoom". Try "help".
(gdb) run
Starting program: /home/kali/Desktop/flow
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Si prega di inserire il tuo nome:123456789012345678901234567890123456789012345678901234567890123456789
Nome utente inserito: 123456789012345678901234567890123456789012345678901234567890123456789

Program received signal SIGSEGV, Segmentation fault.
0x00005555555551a1 in main () at flow.c:12
12
(gdb) bt
#0  0x00005555555551a1 in main () at flow.c:12
(gdb) info registers
rax            0x0
rbx            0x7fffffffdf58    140737488346968
rcx            0x0
rdx            0x0
rsi            0x5555555592a0    93824992252576
rdi            0x7fffffffcd40    140737488346176
rbp            0x3039383736353433  0x3039383736353433
rsp            0x7fffffffde48    0x7fffffffde48
r8             0x5555555592bb    93824992252603
r9             0x7fffffff7b40    140737353317184
r10            0x0
r11            0x202            514
r12            0x0
r13            0x7fffffffdf68    140737488346984
r14            0x555555557dd8    93824992247256
r15            0x7fffffffdd00    140737354125312
rip            0x5555555551a1    0x5555555551a1 <main+88>
eflags        0x10206    [ PF IF RF ]
cs             0x33            51
ss             0x2b            43
ds             0x0
es             0x0
fs             0x0
gs             0x0
(gdb)
```