Relazione S7L4

L'esercizio richiedeva di evitare il buffer overflow, più specificatamente il **segmentation fault.** Questo errore è dato dal fatto che noi inseriamo un numero di caratteri maggiore di quello dichiarato nella variabile. In pratica andiamo a cercare di salvare dei dati in una cella di memoria in cui non siamo autorizzati a scrivere perché “sforiamo” lo spazio allocato per quella variabile.

```
┌──(davide㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:qiopdhjqio0pjdfo0ipqjfo0qwjfiwjefiwhjfijwfiwnfiwnfiwnfiwenfiwnfnwoifnwifnwinfwifoiwnfeiowfebnweruiog
Nome utente inserito qiopdhjqio0pjdfo0ipqjfo0qwjfiw
```

```c
#include <stdio.h>
#include <string.h>

int main () {
char buffer [30];
int bufferLen = 0;

    printf("Inserire il nome utente: ");
    scanf("%s", buffer);
    bufferLen = strlen(buffer);
    printf("Lunghezza stringa %d\n", bufferLen);
    if (bufferLen > 30) {
        for (int i=0; i < bufferLen; i++) {
            printf("indirizzo di memoria del carattere %d : %p\n", i, (void *)&buffer[i]);
        }
    }
    else {
        printf("nome utente inserito: %s\n", buffer);
    }


return 0;

}
```

Per risolvere il problema ci sono dei modi differenti. Avremmo potuto inserire un ciclo do while e fino a che l'utente non avrebbe inserito il numero corretto di caratteri avremmo fatto ripetere l'input all'infinito.

Ho optato comunque per un metodo più veloce, ovvero ho dichiarato il numero massimo di caratteri stampabili nello scanf, in questo modo possiamo evitare l'errore con solo una piccolissima modifica del codice.

```c
#include <stdio.h>
#include <string.h>

int main () {
char buffer [30];
int bufferLen = 0;

    printf("Inserire il nome utente: ");
    scanf("%s", buffer);
    bufferLen = strlen(buffer);
    printf("Lunghezza stringa %d\n", bufferLen);
    if (bufferLen > 30) {
        for (int i=0; i < bufferLen; i++) {
            printf("indirizzo di memoria del carattere %d : %p\n", i, (void *)&buffer[i]);
        }
    }
    else {
        printf("nome utente inserito: %s\n", buffer);
    }


return 0;

}
```

Per quanto riguarda lo stampare gli indirizzi di memoria, qui sotto si possono vedere i vari indirizzi e si vede che vengono occupati gli indirizzi attigui a quelli occupati “legittimamente”.

```
┌──(davide㉿kali)-[~/Desktop]
└─$ ./BOF
Inserire il nome utente: qknfqwnfiopqwenfpqwnpefwefwofnmwfnpkwinfkwnefjklwenf
Lunghezza stringa 52
indirizzo di memoria del carattere 0 : 0x7ffe15b60b40
indirizzo di memoria del carattere 1 : 0x7ffe15b60b41
indirizzo di memoria del carattere 2 : 0x7ffe15b60b42
indirizzo di memoria del carattere 3 : 0x7ffe15b60b43
indirizzo di memoria del carattere 4 : 0x7ffe15b60b44
indirizzo di memoria del carattere 5 : 0x7ffe15b60b45
indirizzo di memoria del carattere 6 : 0x7ffe15b60b46
indirizzo di memoria del carattere 7 : 0x7ffe15b60b47
indirizzo di memoria del carattere 8 : 0x7ffe15b60b48
indirizzo di memoria del carattere 9 : 0x7ffe15b60b49
indirizzo di memoria del carattere 10 : 0x7ffe15b60b4a
indirizzo di memoria del carattere 11 : 0x7ffe15b60b4b
indirizzo di memoria del carattere 12 : 0x7ffe15b60b4c
indirizzo di memoria del carattere 13 : 0x7ffe15b60b4d
indirizzo di memoria del carattere 14 : 0x7ffe15b60b4e
indirizzo di memoria del carattere 15 : 0x7ffe15b60b4f
indirizzo di memoria del carattere 16 : 0x7ffe15b60b50
indirizzo di memoria del carattere 17 : 0x7ffe15b60b51
indirizzo di memoria del carattere 18 : 0x7ffe15b60b52
indirizzo di memoria del carattere 19 : 0x7ffe15b60b53
indirizzo di memoria del carattere 20 : 0x7ffe15b60b54
indirizzo di memoria del carattere 21 : 0x7ffe15b60b55
indirizzo di memoria del carattere 22 : 0x7ffe15b60b56
indirizzo di memoria del carattere 23 : 0x7ffe15b60b57
indirizzo di memoria del carattere 24 : 0x7ffe15b60b58
indirizzo di memoria del carattere 25 : 0x7ffe15b60b59
indirizzo di memoria del carattere 26 : 0x7ffe15b60b5a
indirizzo di memoria del carattere 27 : 0x7ffe15b60b5b
indirizzo di memoria del carattere 28 : 0x7ffe15b60b5c
indirizzo di memoria del carattere 29 : 0x7ffe15b60b5d
indirizzo di memoria del carattere 30 : 0x7ffe15b60b5e
indirizzo di memoria del carattere 31 : 0x7ffe15b60b5f
indirizzo di memoria del carattere 32 : 0x7ffe15b60b60
indirizzo di memoria del carattere 33 : 0x7ffe15b60b61
indirizzo di memoria del carattere 34 : 0x7ffe15b60b62
indirizzo di memoria del carattere 35 : 0x7ffe15b60b63
indirizzo di memoria del carattere 36 : 0x7ffe15b60b64
indirizzo di memoria del carattere 37 : 0x7ffe15b60b65
indirizzo di memoria del carattere 38 : 0x7ffe15b60b66
indirizzo di memoria del carattere 39 : 0x7ffe15b60b67
indirizzo di memoria del carattere 40 : 0x7ffe15b60b68
indirizzo di memoria del carattere 41 : 0x7ffe15b60b69
indirizzo di memoria del carattere 42 : 0x7ffe15b60b6a
indirizzo di memoria del carattere 43 : 0x7ffe15b60b6b
indirizzo di memoria del carattere 44 : 0x7ffe15b60b6c
indirizzo di memoria del carattere 45 : 0x7ffe15b60b6d
indirizzo di memoria del carattere 46 : 0x7ffe15b60b6e
indirizzo di memoria del carattere 47 : 0x7ffe15b60b6f
indirizzo di memoria del carattere 48 : 0x7ffe15b60b70
indirizzo di memoria del carattere 49 : 0x7ffe15b60b71
indirizzo di memoria del carattere 50 : 0x7ffe15b60b72
indirizzo di memoria del carattere 51 : 0x7ffe15b60b73
```

Davide Lecci