BENVENUTI LUIGI,

S7L4

Traccia:

Abbiamo già parlato del buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente. Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

Provate a riprodurre l'errore di segmentazione modificando il programma come di seguito:

- Aumentando la dimensione del vettore a 30;

Risoluzione:

Riscriviamo il codice come richiesto:

```
#include <stdio.h>


int main(){


char buffer [30]; //


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

scanf("%s", buffer);


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


return 0;


}
```

Possiamo notare come il segmentation fault sia stato ridotto, ma non risolto. Basterà infatti inserire una stringa di più di 30 caratteri e l'errore si ripeterà.