S7L4

Il buffer overflow, è una condizione di errore che si verifica a runtime quando in un buffer di una data dimensione vengono scritti dati di dimensioni maggiori.

Codice in c per testare un buffer di grandezza 10 e vedere come si comporta in caso di inserimento di un numero maggiore di caratteri e come possiamo notare, il programma genera effettivamente l'errore di overflow.

```
File  Actions  Edit  View  Help
#include <stdio.h>

int main() {

char buffer[10];

printf("Inserire il nome utente\n");
scanf("%s", buffer);
@sS
printf("Il nome utente inserito è: %s\n", buffer);

return 0;
}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./buffer
Inserire il nome utente
kalikalikalikalikali
Il nome utente inserito è: kalikalikalikalikal
zsh: segmentation fault  ./buffer
```

```c
#include <stdio.h>

int main() {

char buffer [30];

printf("Inserire il nome utente\n");
scanf("%s", buffer);
@sS
printf("Il nome utente inserito è: %s\n", buffer);

return 0;
}
```

Modificando la grandezza del buffer a 30, abbiamo la possibilità inserire un maggior numero di caratteri, ma nel caso in cui avremmo bisogno di inserire un numero ancora maggiore di caratteri dovremmo modificarlo per le nostre necessità.

Come mostrato in figura, questa volta i caratteri sono stati inseriti senza generare alcun tipo di errore.