REPORT BOF

Per buffer overflow s’intende una vulnerabilità generata da una mancanza di controllo dei limiti dei buffer che accettano input utente.

In questo caso andremo ad esaminare un codice in C vulnerabile ai BOF, esaminando una situazione di errore chiamata “segmentation fault”, ossia un errore di memoria.

Creiamo quindi un file estensione in c in cui andremo a scrivere il codice presente nelle slide, che andremo poi ad incollare in un file BOF.c

```c
#include <stdio.h>
int main () {

char buffer [10];


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

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

return 0;

}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano BOF.c

┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -g BOF.c -o BOF

┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Nome utente
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF2
Si prega di inserire il nome utente:jdkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk
Nome utente inserito: jdkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk
zsh: segmentation fault  ./BOF2
```

Ci verrà appunto restituito un segmentation fault, a questo punto possiamo provare a ripetere l’errore aumentando il numero del vettore a 30.