



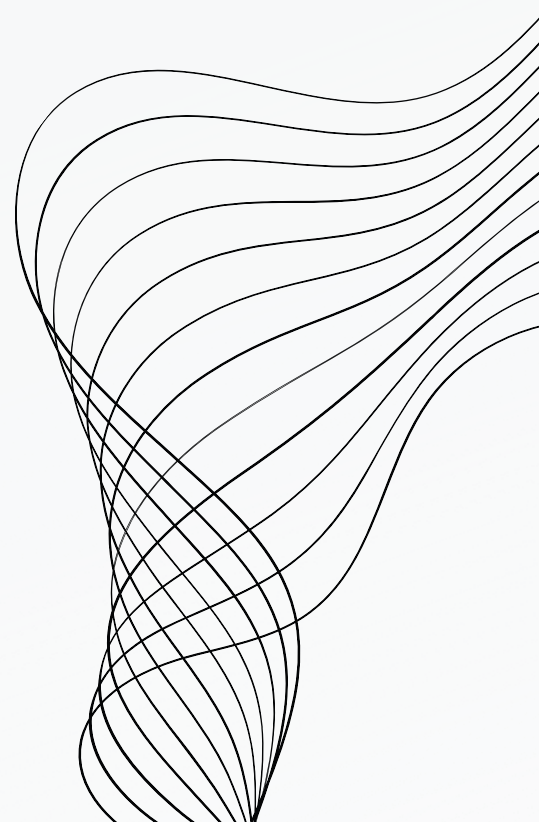
W7 L4

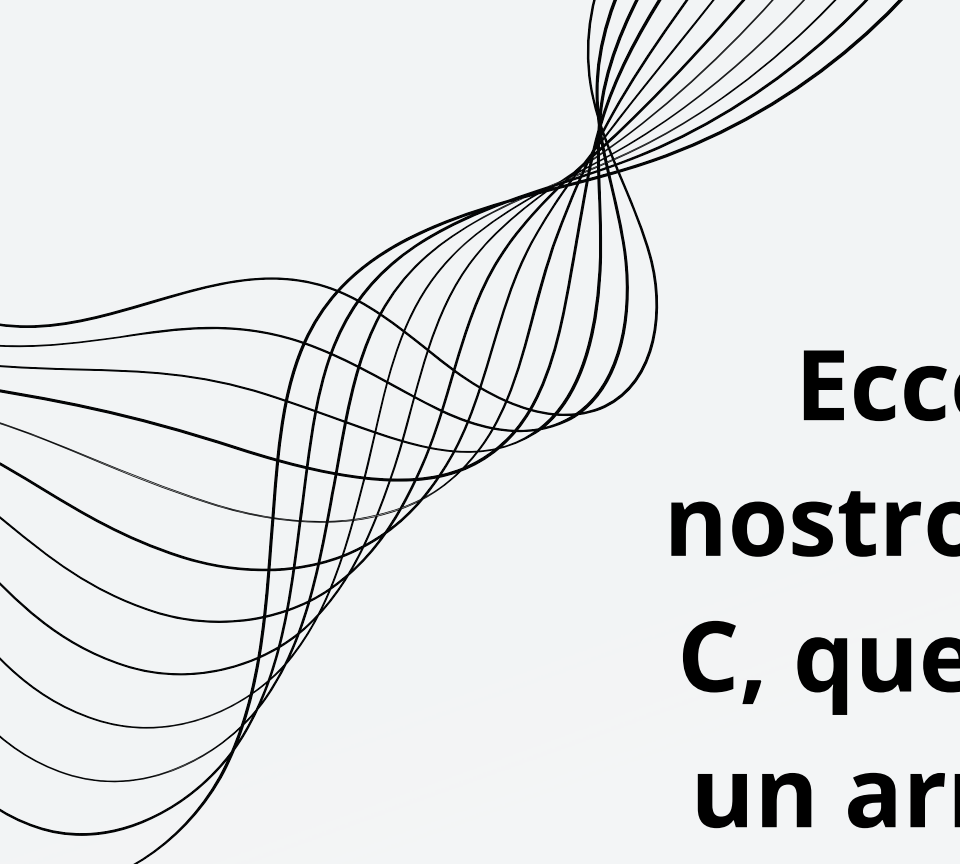
BUFFER OVERFLOW

Oggi andremo a vedere un programma in C che presenta una vulnerabilità di tipo buffer overflow, ovvero:

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma scrive dati oltre i limiti dello spazio di memoria allocato per un buffer, sovrascrivendo aree di memoria adiacenti.

Questo può portare a comportamenti imprevisti, crash del programma o, cosa più seria, a possibili attacchi informatici.





Ecco il corpo del nostro programma in C, questo va a creare un array di caratteri composto da 10 elementi, come possiamo vedere non c'è nessun controllo sul input il che ci espone al buffer overflow

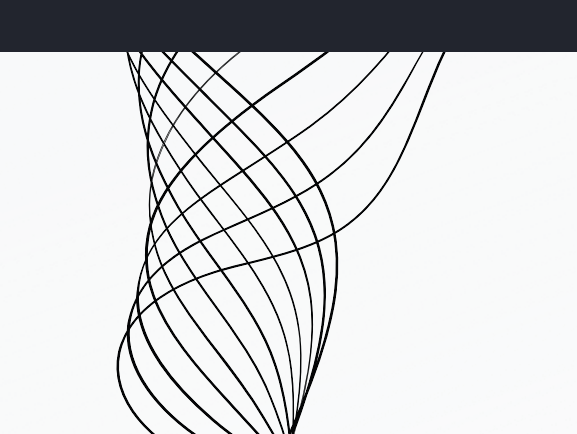
```
GNU nano 6.3
#include <stdio.h>

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;
}
```



**ima con
entito,**

[illegible]

"zsh: segmentation fault" è un messaggio di errore che indica un errore di segmentazione. Questo errore si verifica quando un programma tenta di accedere a una parte della memoria a cui non ha il permesso di accedere, o sta cercando di scrivere in una parte di memoria non consentita.

Andiamo ad apportare qualche modifica al nostro programma in modo da evitare il buffer overflow. Nello specifico abbiamo aumentato i caratteri dell'array e inoltre abbiamo aggiunto un controllo sul input, con il nuovo codice andrà ad accettare solo i primi 30 caratteri inseriti ed evitando così il buffer overflow

```
#include <stdio.h>

int main () {
    char buffer [30];

    printf ("Si prega di inserire il nome utente");
    scanf ("%30s", buffer );

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

    return 0;
}
```

Di seguito una dimostrazione del nostro codice :

```
(kali@kali)-[~/Desktop]  
$ nano BOF.c
```

```
(kali@kali)-[~/Desktop]  
$ gcc -g BOF.c -o BOF
```

```
(kali@kali)-[~/Desktop]  
$ ./BOF
```

Si prega di inserire il nome utente kosejijfbqjwkbfbhwbvrbhqrhqbfbjsjvbhqfsbfjksa jvkbajsbv ejvrbvhv
Nome utente inserito : kosejijfbqjwkbfbhwbvrbhqrhqbfb

```
(kali@kali)-[~/Desktop]  
$
```

FINE



Grazie.
Massimo
Cinquegrana

