

07 MARZO 2024

REPORT - EPISODE

S7L4

PRESENTED BY

Alessandro Marasca

BUFFER OVERFLOW

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).

ESITO

```
[kali㉿kali)-[~]
$ ./BOF
```

Inserire il nome utente: alessandromarasca1994natoaromail27/11/1994
Nome utente inserito: alessandromarasca1994natoaromail27/11/1994
zsh: segmentation fault . ./BOF

```
[kali㉿kali)-[~]
$ |
```

Alessandro Marasca

Epicode

S7L4- CS0124

07 MARZO 2024