3.4

BUFFER OVERFLOW

HISTORIA

- Documentado en 1972
- Explotado en 1988 por el *Morris Worm*
- Redescubierto y publicado en 1995 y 1996
- Usado para piratear la XBox
- USado para piratear la PS2

¿QUÉ ES?

- El excesivo relleno de una variable o recurso que resulta en un problema con el manejo de memoria, pudiendo incurrir en modificaciones de memoria, manipulación y acceso a direcciones de memoria y crasheos de programas

¿QUÉ ES?

```
#include <string.h>

void f(char* s) {
    char buffer[10];
    strcpy(buffer, s);
}

void main(void) {
    f("01234567890123456789");
}
```

BUFFER OVERFLOW

- Audita tu código
- Conoce la documentación del lenguaje y sus vulnerabilidades conocidas: Estándares de desarrollo, funciones inseguras…
- Herramientas de compilación específicas: StackShield, StackGuard…