

Esercitazione Capitolo 2:

Type safety

1 Buffer overflow

Scrivi un esempio di funzione che mediante buffer overflow modifica una variabile del main NON passata come argomento. Ad esempio

```
void foo(int* a) {
    *(a + 1) = 20;
}

void main(void) {
    int x = 0, y = 10;
    printf("%d %d\n", x, y); // -> 0 10
    foo(&y);
    printf("%d %d\n", x, y); // -> 20 10
}
```

2 Buffer overflow - strcpy

Scrivi un esempio di funzione che mediante strcpy e buffer overflow modifica una variabile stringa del main NON passata come argomento.

3 Dangling pointer su stack

Scrivi un esempio di funzione che restituisce un dangling pointer sullo stack usando le struct. Nel main prova a chiamare la funzione: c'è modo di accorgerti che il puntatore è dangling?

4 Dangling pointer con free

Scrivi un esempio di funzione che restituisce un dangling pointer sullo heap usando le struct (e free). Nel main prova a chiamare la funzione: c'è modo di accorgerti che il puntatore è dangling?