Checklist of Undefined Behavior (UB) in C

1. Multiple Modifications in a Single Expression

Example: i = i++ + ++i;

2. Division by Zero

Example: int a = 5 / 0;

3. Using Uninitialized Variable

Example: int x; printf("%d", x);

4. Out-of-Bounds Array Access

Example: int arr[3] = {1,2,3}; int x = arr[5];

5. NULL Pointer Dereferencing

Example: int *p = NULL; int x = *p;

6. Dangling Pointer

Example: Pointer to a local variable returned and used later.

7. Signed Integer Overflow

Example: int a = 2147483647; a = a + 1;

8. Use-After-Free

Example: int *p = malloc(...); free(p); *p = 10;

9. Strict Aliasing Violation

Example: float f = 3.14; int* p = (int*)&f;

10. Double Free

Example: free(p); free(p);

11. Misaligned Memory Access

Example: char* p = malloc(4); int* q = (int*)p;

Checklist of Undefined Behavior (UB) in C

12. Modifying String Literals

Example: char *s = "hello"; s[0] = 'H';

13. Returning Pointer to Local Variable

Example: int* f() { int x; return &x; }

14. Missing Return in Non-void Function

Example: int f() { }

15. Infinite Recursion

Example: void f() { f(); }

16. Incorrect Format Specifier

Example: float x = 3.5; printf("%d", x);

17. Shifting Beyond Integer Size

Example: int x = 1 << 32; (on 32-bit int)

18. Modifying const through Pointer

Example: const int x = 5; int* p = (int*)&x; *p = 10;