Why are we still vulnerable to buffer overflows?

Why code written in assembly code or C are subject to buffer overflow attacks?

➡ Because C has primitives to manipulate the memory directly (pointers ect ...)

If other programming languages are “memory safe”, why are we not using them instead?

- Because C and assembly code are used when a program requires high performances (audio, graphics, calculus …) or when dealing with hardware directly (OS, drivers ….)

Why are we still vulnerable to buffer overflows?

Why code written in assembly code or C are subject to buffer overflow attacks?

➡ Because C has primitives to manipulate the memory directly (pointers ect ...)

If other programming languages are "memory safe", why are we not using them instead?

- Because C and assembly code are used when a program requires high performances (audio, graphics, calculus …) or when dealing with hardware directly (OS, drivers ….)

TOCTOU attacks - Time Of Check to Time Of Use

(also called race condition attack)