Why are we still vulnerable to buffer overflows and other memory corruption vulnerabilities?

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 ...)

Why are we still vulnerable to buffer overflows and other memory corruption vulnerabilities?

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 ...)

Choosing a better programming language

Some languages are type-safe (i.e memory safe)

- Pure Rust, Lisp, pure Java, ADA, ML …

Some languages isolate potentially unsafe code

- Modula-3, Java with native methods, C# …

Some languages are hopeless

- Assembly languages, C …