

Sanitizer

2024.04.04

SWPP Practice Session

Seunghyeon Nam (with lots of derived works)

Clang Sanitizer

- Injects code to detect UB at runtime
- `clang -fsanitize=<target> code.c`
 - `undefined`: Detects UBs from arithmetic operations
 - `address`: Detects use-after-free, double free, etc
 - `memory`: Detects use of uninitialized memory
 - See examples in the class repository!