Pointer Rules

Compiler optimization: may eliminate needed tests (cheddar_bay)

Use-after-free: zero out sensitive data when freeing (ptr-2)

Use-after-free: set pointer to null after free (ptr-0)

Double-free: free in the same module as memory obtained (ptr-9)

Out-of-bounds pointer: make checks before dereference (ptr-3/4/5)

Pointer de-references past flexible structure: (ptr-7)

Null pointer arithmetic: (ptr-8)