COM 402 exercises 2023, session 7: Fuzzing

Exercise 7.1

What is coverage-guided fuzzing, and how does it differ from black-box fuzzing?

Exercise 7.2

Given the following program, how likely is it for a blackbox, greybox, or whitebox fuzzer to find the correct value for `user_input`?

```
int foo(uint32_t user_input) {

        /* ... */

        if (user_input == CONSTANT) {
                /* ... */
                crash();
                /* ... */
        }

        /* ... */

        return 0;
}
```

Exercise 7.3

What is a sanitizer and why is it helpful in fuzzing? Why can certain bugs only be detected when using sanitizers?