Introduction to Static Analysis

CS 3750
An Example

With a partner, try and brainstorm examples you have seen where test cases failed to expose a defect. See if one of you can write a simple code snippet with a defect that escapes detection by test cases created by the other person.
Definitions

According to the Wikipedia article on software verification, static verification includes activities like:

- Code conventions verification
- Bad practices (anti-pattern) detection
- Software metrics calculation
- Formal verification
Several studies have found that static analysis activities are more effective and efficient at finding defects than testing!

These defects in various quality attributes are “easy” to find given the fact that computer software must adhere to a particular structured syntax which must be “easy” to parse and analyze.
There are numerous static analysis tools available and widely used. Several examples taken from Wikipedia’s article on static code analysis:

- Splint
- Pylint
- JSLint
- ShellCheck
- Checkstyle
- PMD
- FindBugs