Program Analysis
Random Testing and Fuzzing
(Part 1)
Automated Testing

- **Manual testing**
  - Important but limited by human time

- **Automated testing**
  - Test execution: Regularly execute regression test suite
  - Test creation: Automatic test generation
Automated Testing

- **Manual testing**
  - Important but limited by human time

- **Automated testing**
  - Test execution: Regularly execute regression test suite
  - Test creation: Automatic test generation

Focus of this lecture
Kinds of Approaches

- **Blackbox**
  - No analysis of program

- **Greybox**
  - Lightweight analysis of program
  - E.g., coverage achieved by inputs

- **Whitebox**
  - More heavyweight analysis of program
  - E.g., conditions that trigger specific paths
Kinds of Approaches

- **Blackbox**
  - No analysis of program

- **Greybox**
  - Lightweight analysis of program
  - E.g., coverage achieved by inputs

- **Whitebox**
  - More heavyweight analysis of program
  - E.g., conditions that trigger specific paths
Kinds of Approaches

- Blackbox
  - No analysis of program

- Greybox
  - Lightweight analysis of program
  - E.g., coverage achieved by inputs

- Whitebox
  - More heavyweight analysis of program
  - E.g., conditions that trigger specific paths
Kinds of Approaches

- **Blackbox**
  - No analysis of program

- **Greybox**
  - Lightweight analysis of program
  - E.g., coverage achieved by inputs

- **Whitebox**
  - More heavyweight analysis of program
  - E.g., conditions that trigger specific paths

All of them:
Use feedback from test executions
What’s “the Program”?

- Many possible answers
  - Individual function
  - Class and its methods
  - Entire library
  - Entire stand-alone tool

- Ideas discussed here work (in principle) on multiple levels
Outline

- Introduction
- Randoop
  - Based on *Feedback-Directed Random Test Generation*, Pacheco et al., ICSE 2007
- Greybox fuzzing in AFL
  - Based on https://lcamtuf.coredump.cx/afl/technical_details.txt