Secure Programming
Program Analysis and Testing

Dr. Fatma ElSayed

Computer Science Department
fatma.elsayed@fci.bu.edu.eg

Program Analysis

Definition: The process of using automated tools to analyze the behavior of computer programs for particular properties

Areas where it's used:

- **Compiler development**

  Compilers have to analyze code, and turn it into executable binaries or bytecode

- **Verification**

  We may want to verify that a program is correct (implements its specification properly)

- **Security**

  We want to fnd code that can lead to vulnerabilities

Program Analysis Approaches

- **Static analysis:** performed without executing the program.
  - Uses the program's static artifacts (usually, source code, but sometimes binary executables)
  - We call it "reading the code", or "code review"
- **Dynamic analysis:** performed at runtime.
  - Actually runs the program (or part of it)
  - We call it "debugging" or "manually running tests"
- **Hybrid:** a mix of the previous two.

Benefits of Program Analysis

- Catch bugs early
- Improve security
- Make code more reliable
- Help developers write better code

Static vs Dynamic Analysis

Static Analysis	Dynamic Analysis
Doesn't run the code	Runs the code
Fast to use	Slower, but detailed
Finds syntax errors	Finds runtime issues
Example: Linter	Example: Unit tests

Static Analysis Tools

- **ESLint (JavaScript)** – Style and error checking.
- **Bandit (Python)** – Security-focused analysis.
- **Fortify** – Enterprise-grade security tool.
- **SonarQube** – Quality and security across languages.

Dynamic Analysis

How it is work

- **Memory Interactions**
  - Monitor memory allocation and data flow
- **I/O Monitoring**
  - Monitor system inputs and outputs during execution
- **Runtime Error Detection**
  - Detect runtime exceptions and crashes

Types of Testing

Unit Testing

- Testing individual components or functions of a program in isolation, done by developers.

Integration Testing

- Testing how multiple units/modules work together when combined, done by developers.

System Testing

- Testing the entire system as a whole to verify it meets the specific requirements, done by testing team.

Acceptance Testing

- Testing done to verify the system meets business needs and is ready to release, done by end users or clients.

THANK YOU