CI/CD
Lecture 7-Static Analysis: Overview

Omkarendra Tiwari

September 13, 2022

Outline

Static Code Analysis

Similar to

- White Box Testing
- Source Code Analysis
- Inspecting source code's behavior without executing

Uses

- Data Flow Analysis
- Taint Analysis
- Source code analysis tools/techniques

Data Flow Analysis

- Deriving run-time behavior of the program
- Used for Optimization
- Makes use of IRs such as CFG

Basic Block

- Set of statements with no branches
- Sequential execution of the statements within the block
- Utilizes three-address code for identification

Control Flow Graph

- A graph representation
- Each node is a basic block
- Has two special nodes, *entry* and *exit*

Abstract Syntax Tree

Tools

- http://www.eclipse.org/jdt/ui/astview/index.php
- https://javaparser.org/
- https://github.com/INRIA/spoon

Further Reading

Highly Recommended

- https://owasp.org/www-community/controls/Static_Code_Analysis
- http://www.eclipse.org/articles/Article-JavaCodeManipulation_AST/index.html