# Lab 4 - Static Code Analysis – PART OF YOUR CA

## 1. Introduction

Static code analysis is a type of program analysis that is performed without actually executing programs but rather examining the source or object code. There are many commercial and open-source tools designed to inspect code and report found issues. In this lab, students will use them, to find bugs in a given Java project.

The objective of this lab is to let students know that tools like **SpotBugs**, **PMD** and **SonarLint** exist and to get some hands-on experience in how to use them and how to interpret reported issues so that it can help improve the quality of the code.

### Analysis tool:

SpotBugs, Sonar Lint and PMD are **Static code analysis tools** that analyses Java bytecode and detect a wide range of problems based on the concept of bug patterns. Since we will be working with a Java project if you are using Eclipse or VS-Code, we will use the plugins and extensions available in these IDEs. For this lab you can choose any static analysis tool/plugins/extension to use (EG: SpotBugs, Sonar Lint, PMD)

**Note: If you are using IntelliJ or other editor, ensure that you can install the required plugins.**

### System under test (SUT):

The project that we will be testing in this lab is a Billing System, which is a simple Java project for sales and inventory. This project was created as a sample project for this lab, therefore it should not be looked at as a complete system. You may generate a database if you wish to run the code, but it is not necessary!

## 2. Tasks (Use either Eclipse or VS Code)

#### 2.1 Set up your **Eclipse** IDE:

* Install (if not already installed) any **two** of the following plugins : **SpotBugs, PMD** or **SonarLint**, from the Eclipse Market Place.
* Import the Billing System project code (See Blackboard)
* More instructions can be found in the document “Billing System Overview and Tool Setup”.

#### 2.2 Set up your **VS Code** IDE:

* Install (if not already installed) **SonarLint**, from the Extensions Menu.
* Download and extract the Billing System project code (See Blackboard)
* In VS Code click ‘File’ and then ‘Open Folder’ and navigate and select the Billing System folder

## 3. Lab Deliverables

### Analyse bugs

Your task is to analyse **two bugs** of your choice, found by the plugin/extension that you installed in your IDE for the Billing System project. In your report mention if you think the given bug is an actual fault or a false positive (see class notes). In case of an actual fault, try to think of a solution to the problem. Discuss the bugs that you identify, why they are a problem and what vulnerabilities/issues they could cause. Fix the code and show the corrected code in your Lab report.

## Marking Scheme

|  |  |
| --- | --- |
|  | **Marks Available** |
| Introduction/Description | 5 |
| Aims | 5 |
| Method | 10 |
| **Analysis of bug 1**  Identification of issue – what is the bug that was found  Solution to this bug  code fix – show and explain code changes | 25 |
| **Analysis of bug 2**  Identification of issue - what is the bug that was found  Solution to this bug  code fix – show and explain code changes | 25 |
| Conclusion | 30 |
| **TOTAL** | **100** |