# **Practical 5 - Static Code Analysis**

## **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, you will use them, to find bugs in a Java project.

The objective of this lab is to let you know that tools like **SpotBugs**, **PMD**, **Snyk**, **SonarQube** and many more 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 tools:**

[SonarQube](https://docs.sonarsource.com/sonarcloud/improving/sonarlint/) is a **Static code analysis tools** that analyses bytecode and detect a wide range of problems based on the concept of bug patterns. [Snyk](https://snyk.io/) is a security code analysis tool and can check code as it’s being written for security issues. Since we will be working with a Java project and VS-Code, we will use the extensions available in VS Code for Sonar and Synk. For this lab you will have to demonstrate how you **used SonarQube for IDE and Snyk Security and analyse two bugs found.**

**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 is a sample project for this lab, therefore it should not be looked at as a complete system. You can download the code from GitHub: <https://github.com/mariagriffin/BillingSystemStudentCode>

## **2. Tasks**

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

* Install (if not already installed) **SonarQube**, and **Snyk** 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

#### **2.2 Use SonarQube and Snyk**

* Use SonarQube and Snyk to identify issues in the code.

## **3. Fix some of the issues in the code**

* Look out for: Database security error
* == instead of .equals()
* Try/Catch
* Exceptions