Part 2: SonarQube – Static Analysis

NB! For some of the links in part 2 to work properly, you must be logged in to GitHub.

This part of the assignment is about getting familiar with the static analysis tool **SonarQube**. [1] There is a lot of documentation about SonarQube, but as an alternative, you may watch a couple of YouTube videos:

1. What is SonarQube?
2. What and Why is SonarQube?

For this part of the assignment you can choose to work with one of two options:

Option 1:
Study an already scanned project, and solve the following tasks based on the projects results shown **here.**
Difficulty: Normal

Option 2:
Run an analysis of your own project/code (either Java, C#, C, C++, Javascript, Python etc.). In order to analyze GitHub-projects you may follow the official documentation or a blogpost like How to Analyze GitHub Projects with SonarQube Cloud. Use the results from your analysis to solve the following tasks.
Difficulty: Hard

OBS: If you choose **Option 2**, SonarQube requires signing up with a GitHub/Bitbucket account, and it only permits you to scan open source projects (i.e. public project(s)).

[1] SonarQube/SonarQube Documentation – `https://docs.sonarqube.org/latest/`

Regardless of the chosen option, you should be able to see the following page:

https://sonarcloud.io/explore/projects

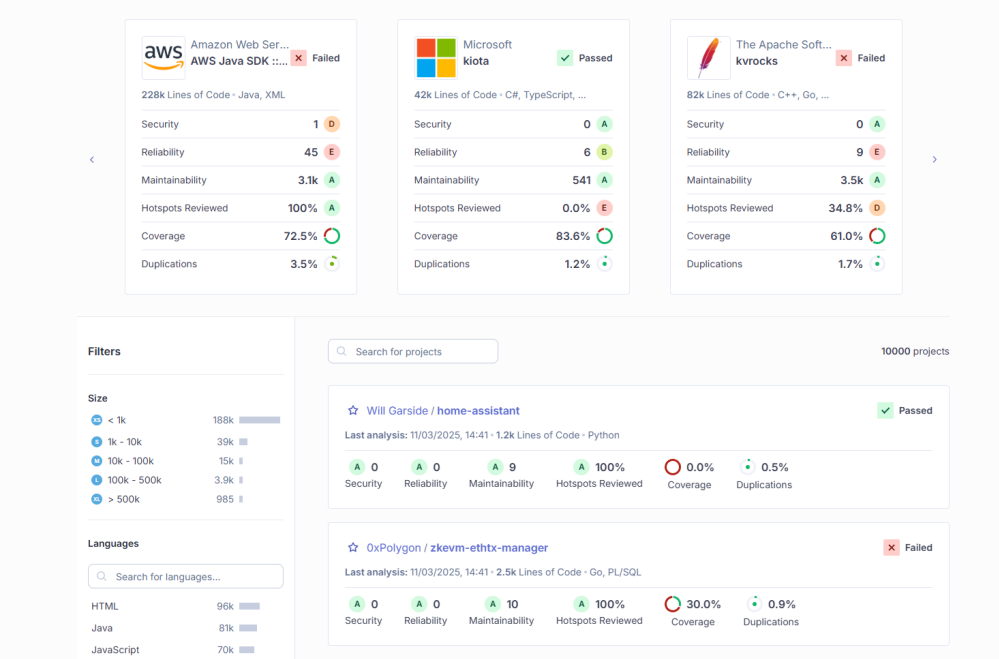


Figure 1: SonarQube Project Overview aka. Dashboard

Task 0.

0.1 **Specify** which of the following options you have chosen.

0.2 If you choose *Option 2*; **specify** the GitHub/Bitbucket URL.

Task 1.

1.1 What does the metrics say about the code/project in whole (e.g. quality gate)?

1.2 **Briefly explain** what the following six types of issues listed by the analyzer mean:

- Security
- Reliability
- Maintainability
- Hotspots reviewed
- Coverage
- Duplications

Task 2.

2.1 **Select and list** at least (four) 4 issues and **briefly explain why** the analyzer has reported the given issues.

2.2 For each of the listed issues, **how would you solve** the problem?

> ***Hint**: Use either textual description, or code/ pseudocode to describe the treatment.*