Static Code Analysis Procedure

Introduction

Static code analysis is an integral step in software development which must be employed by developers to validate their code before merging with the development branch. In this way, any bugs or security vulnerabilities present in their work can be identified and eliminated at an early stage of development. In view of this, we will be exploring SonarQube, an industry-standard static code analysis tool, in this document and be explaining its implementation in our local machines. This tool will be integrated in our Software Development Lifecycle (SDLC) for both internal and external projects. SonarQube is used in place of Sonar Cloud as we are unable secure permission from A*STAR ITSS for connecting Sonar Cloud plugin with Azure repository.

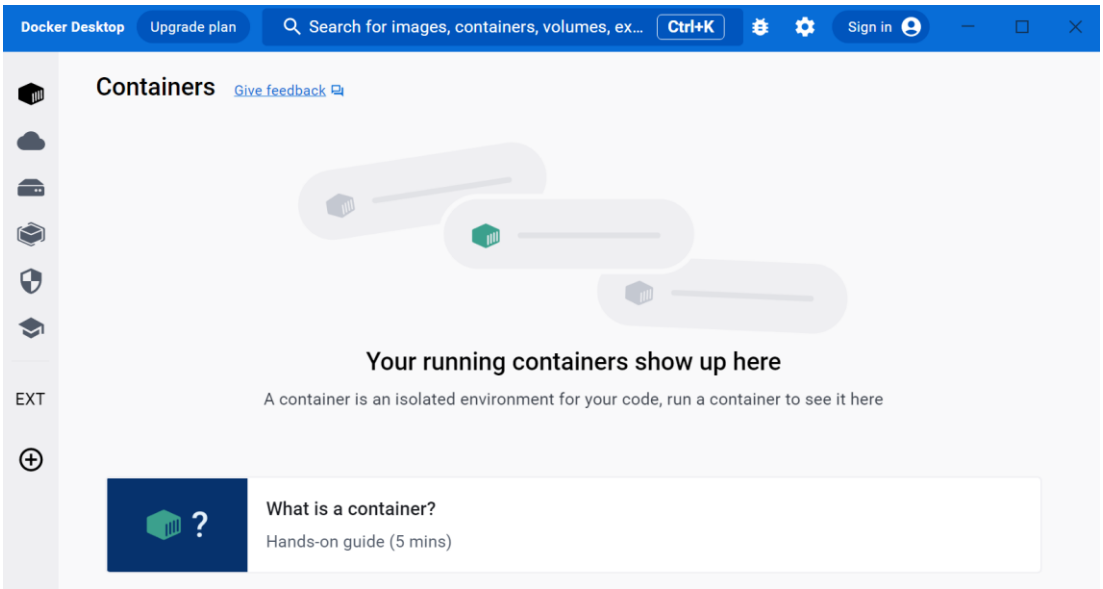
Description

SonarQube (formerly **Sonar**) is an open-source platform developed by SonarSource for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs and code smells on 29 programming languages. SonarQube offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, comments, bugs, and security recommendations.

Steps for installing and scanning

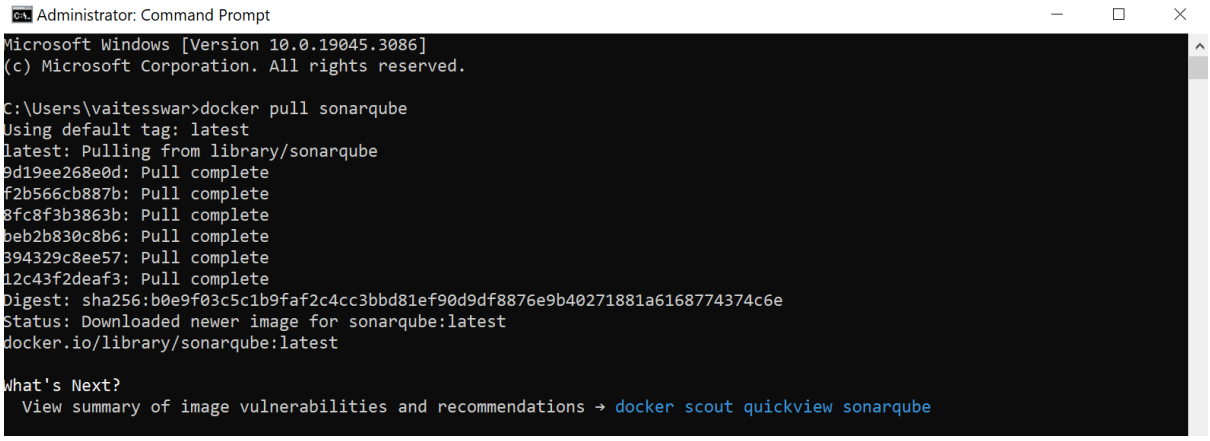
These steps are meant for installing SonarQube in a developer's local machine with Windows Operating System. Steps may vary for other operating systems. Please note that steps 1 to 6, 14 and 15 are only meant for installing SonarQube the first time.

1. Open Docker Desktop

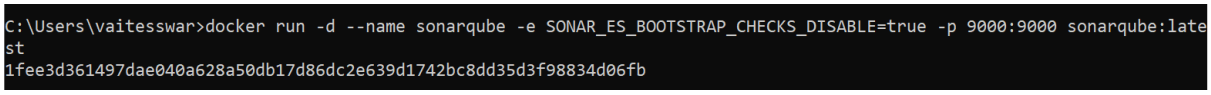


2. Open Command Prompt (run as Administrator)

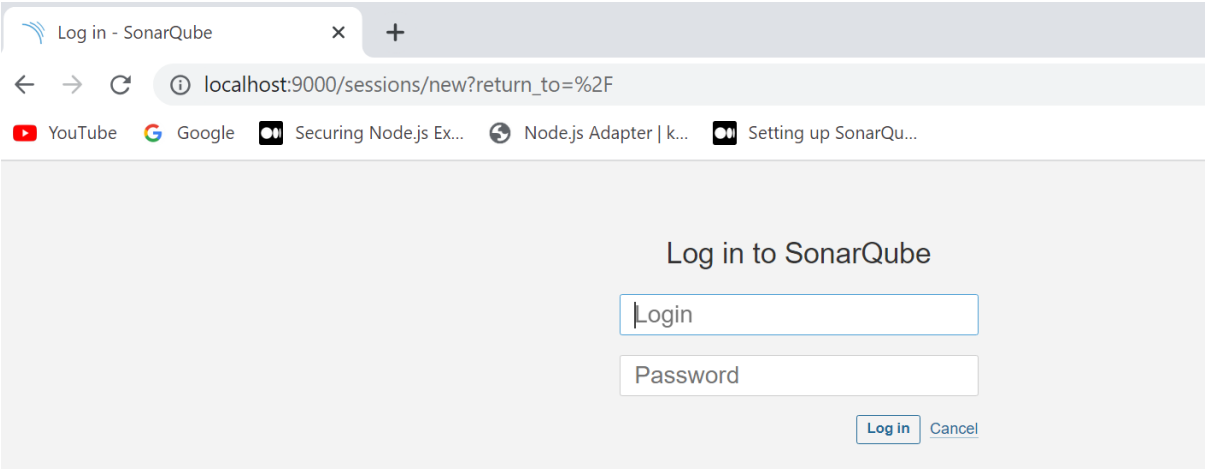
3. Run the command “docker pull sonarqube”



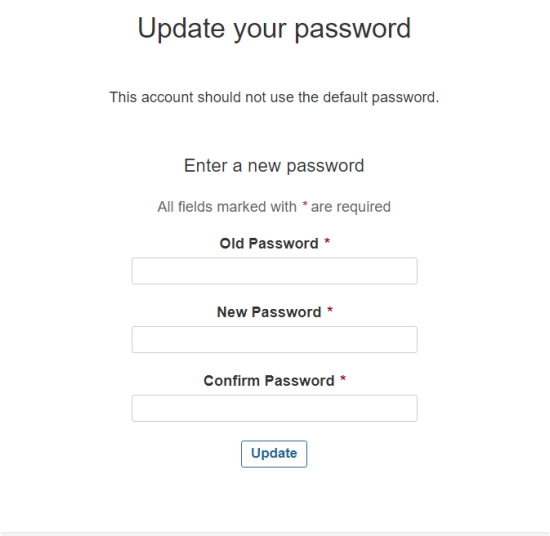
4. Run the command “docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest”



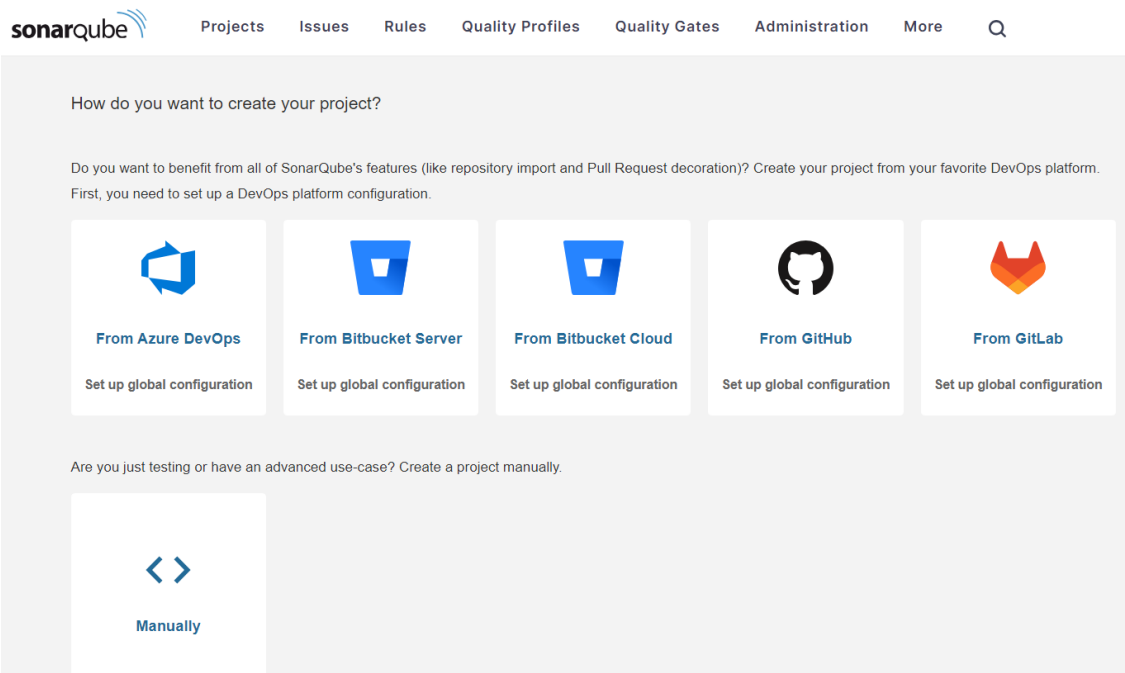
5. Log in to http://localhost:9000/ (username: admin, password: admin)



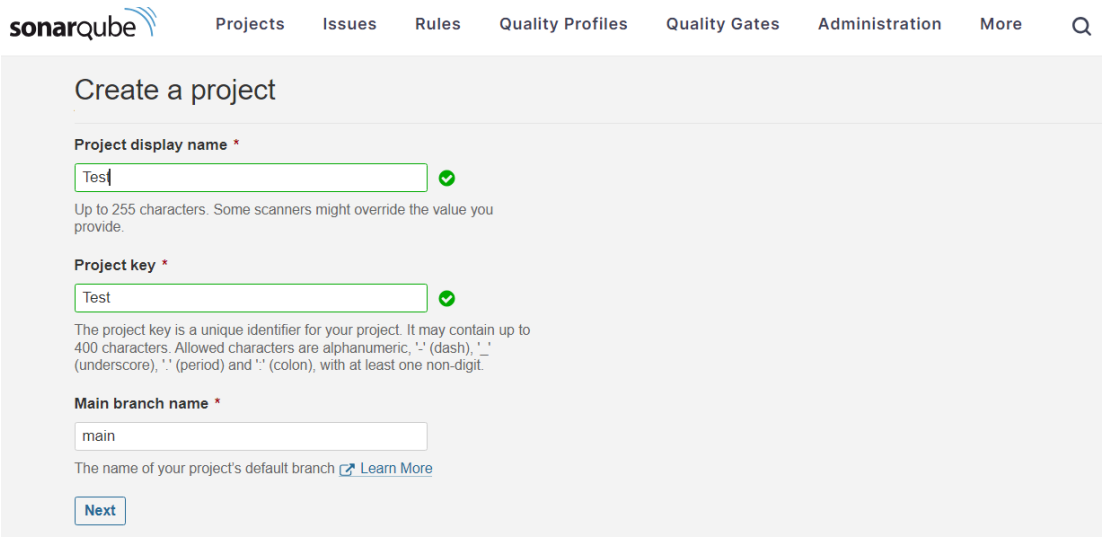
6. Change to desired password.



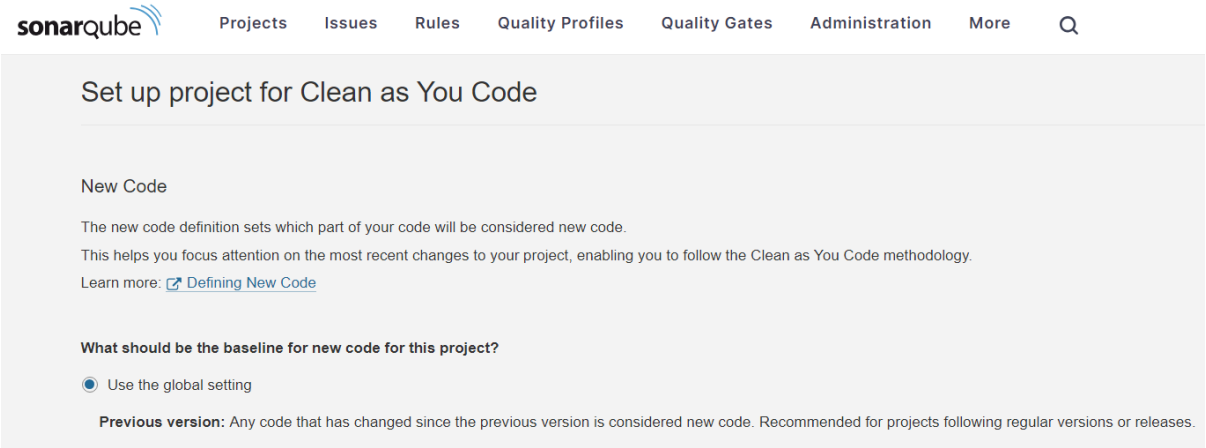
7. Choose “Manually”.



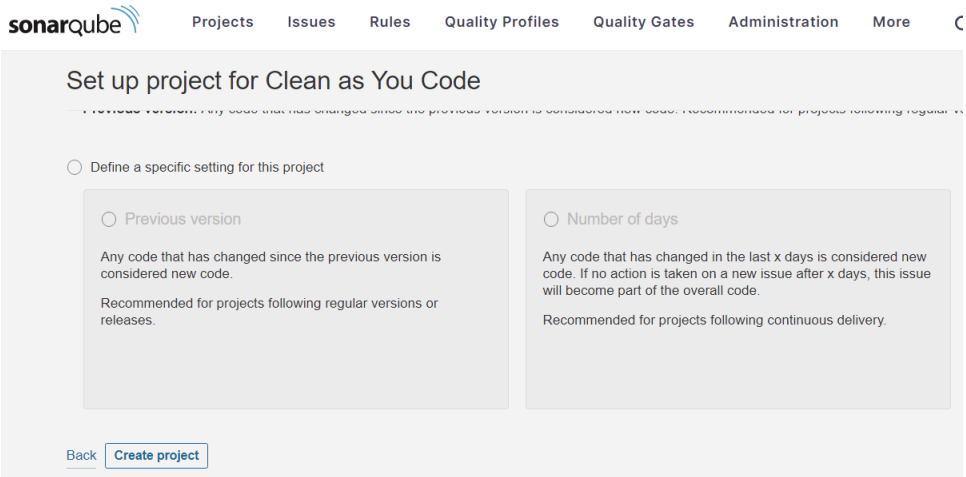
8. Assign a project display name and project key.



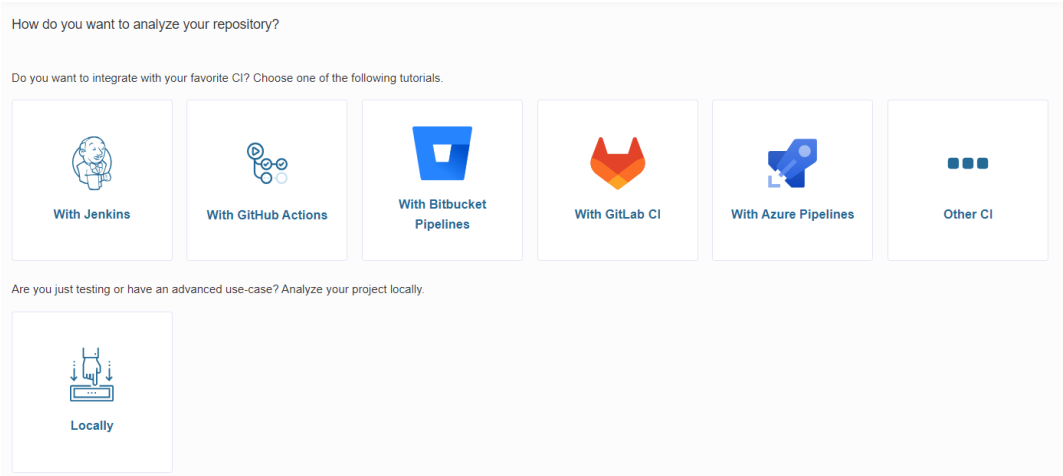
9. Select “Use the global setting” option.



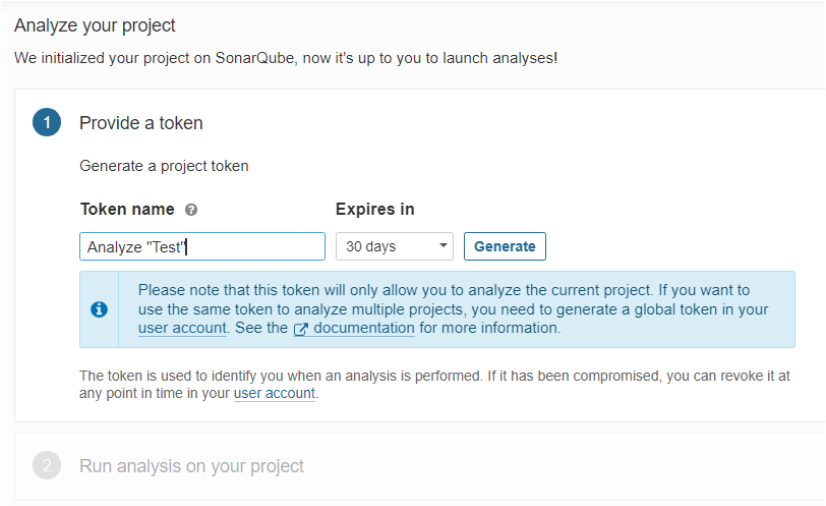
10. Click “Create project” button at bottom of the page.



11. Choose “Manually”.

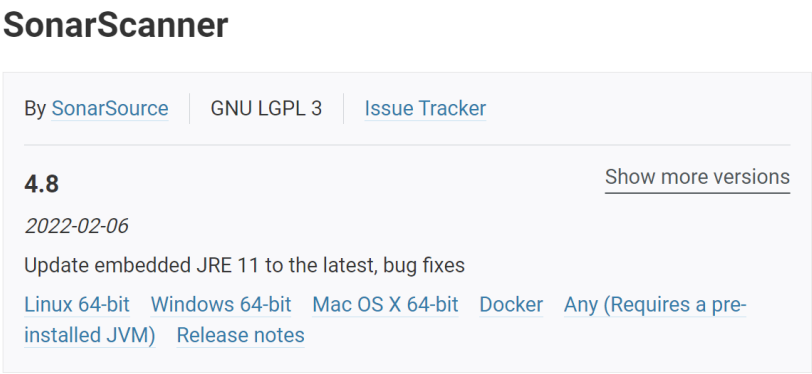


12. Generate token and click “Continue”.

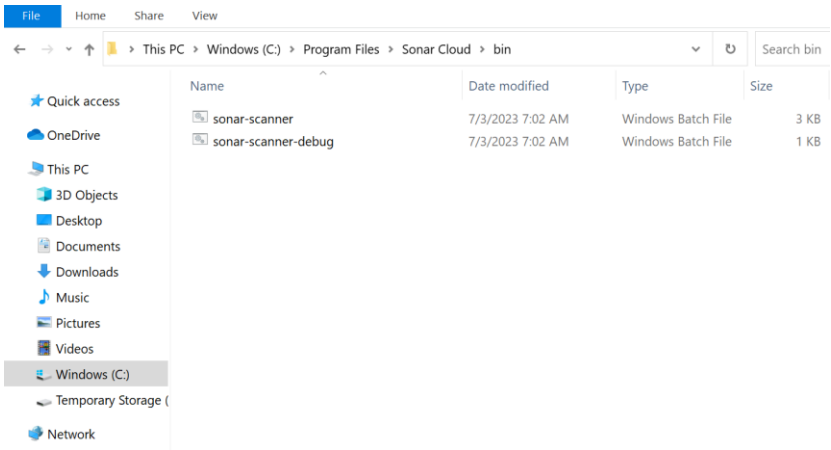


13. Choose the necessary options.

14. Download Sonar Scanner (.zip file) from “https://docs.sonarqube.org/10.1/analyzing-source-code/scanners/sonarscanner/” and extract it.



15. Transfer the extracted folder to “Program Files” and rename it to the desired new folder name. In this case, it is renamed as “Sonar Cloud”.



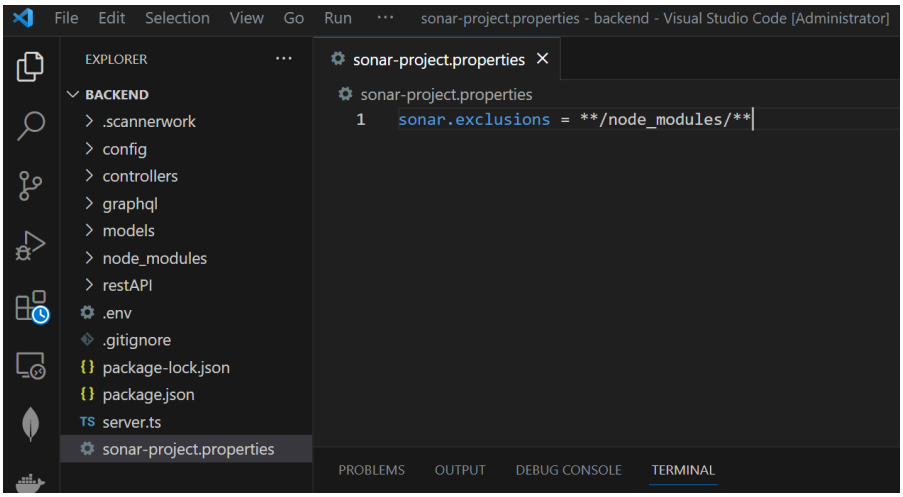
16. Go to command prompt and set the path to the sonar-scanner.bat file as follows which is found in bin folder. The command is “set PATH=%PATH%;"<bin folder path>"”.

```
C:\Users\vaitesswar>set PATH=%PATH%;"C:\Program Files\Sonar Cloud\bin"
```

17. Change the location in command prompt to project folder (cd <PROJECT_PATH>).

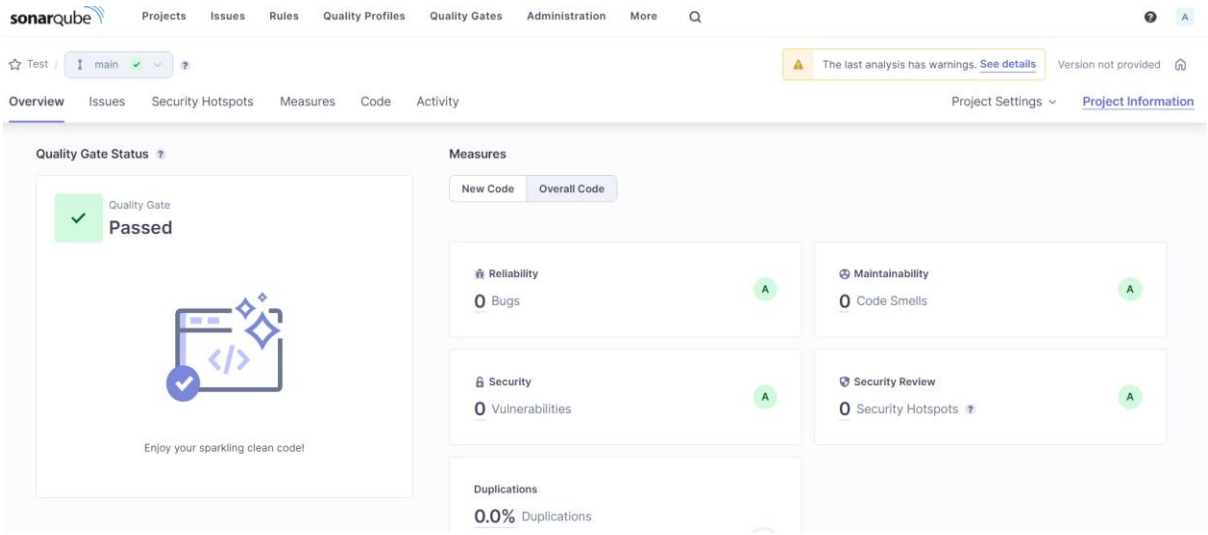
```
C:\Users\vaitesswar>cd C:\Users\vaitesswar\Desktop\patientDoctor_application\backend
```

18. Add sonar-project.properties in project folder and enter "sonar.exclusions = **/node_modules/**". This ensures that node modules are **not included** for scanning.



19. Run the command given in SonarQube page with token in command prompt. An example is shown below.

20. Upon completion, the SonarQube page will automatically refresh to display the results.



21. If issues are found by the tool, the developer has to rectify them based on the corrections suggested by the tool until all issues are rectified. An example is illustrated below.