* SonarQube: SonarQube empowers all developers to write cleaner and safer code. SonarQube is **an open-source automatic code review tool to detect bugs, vulnerabilities and code smell in your code**. ... Well, as I told in the description, SonarQube is an open-source automatic code review tool to detect bugs, vulnerabilities, and code smells in your code

##Benefits:

* Sustainability - Reduces complexity, possible vulnerabilities, and code duplications, optimising the life of applications.
* Increase productivity - Reduces the scale, cost of maintenance, and risk of the application; as such, it removes the need to spend more time changing the code.

SonarQube is a **Code Quality Assurance tool that collects and analyzes source code**, and provides reports for the code quality of your project.

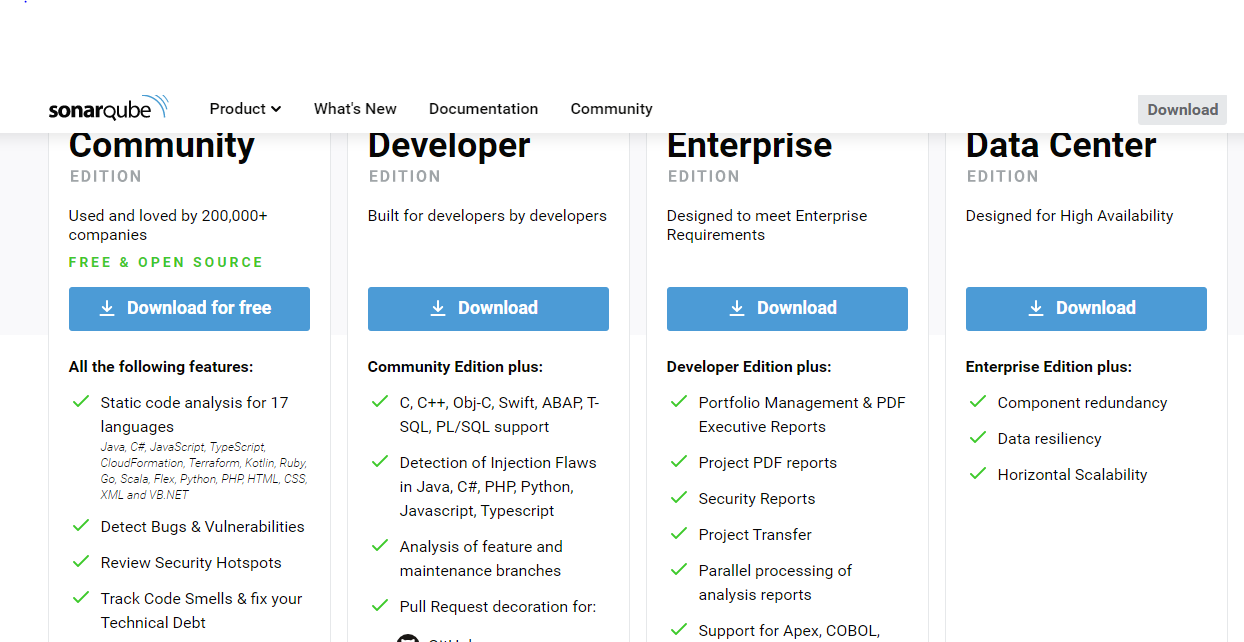
The JaCoCo-Maven plugin is used **to generate code coverage reports**. Source code with high code coverage has more of its code executed during testing.

SonarScanner is **a separate client type application that** in connection with the SonarQube server will run project analysis and then send the results to the SonarQube server to process it.

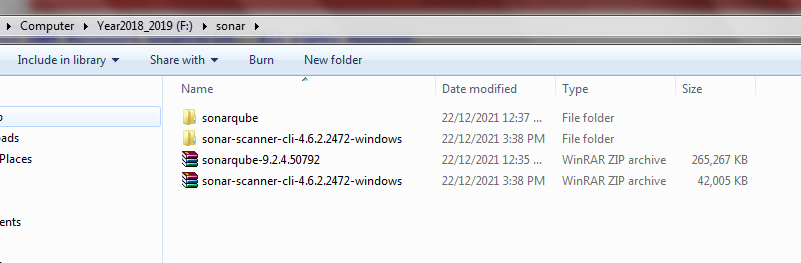
SonarQube Installation:

Step-1) [Download](https://www.sonarqube.org/downloads/)the SonarQube Community Edition.

<https://www.sonarqube.org/downloads/>



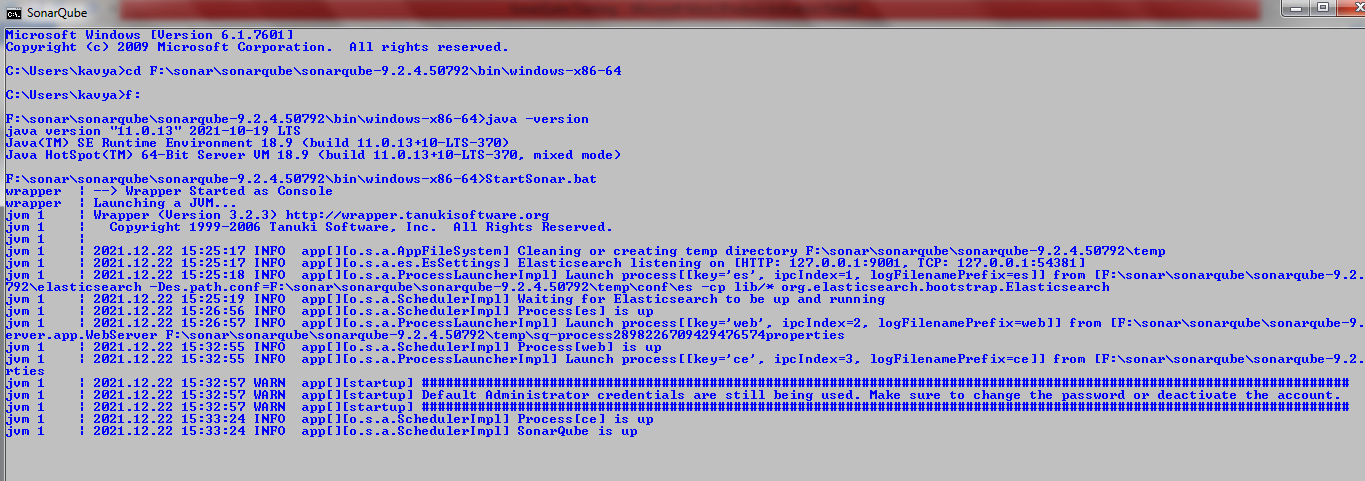
Step 2) As a non-root user, unzip it, let’s say in **C:\sonarqube** or **/opt/sonarqube**.



Step 3) Go to path as per your OS and start SonarQube using StartSonar.bat/sh

Below is the snapshot for the same:

F:\sonar\sonarqube\sonarqube-9.2.4.50792\bin\windows-x86-64>StartSonar.bat

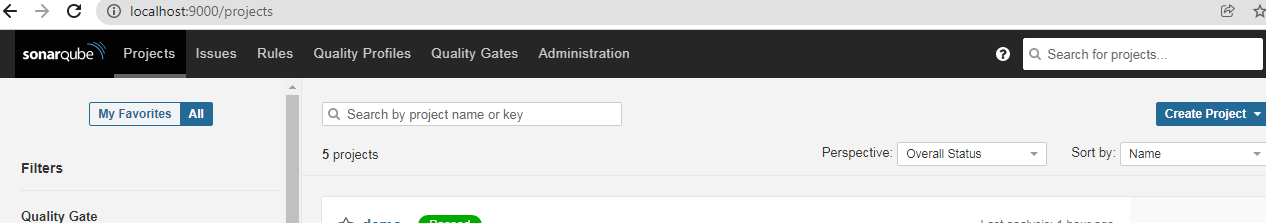


Step 4) Open browser and[**http://localhost:9000/**](http://localhost:9000/) (9000 is default) you will be navigated to below window, with System Administrator credentials (login=**admin**, password=**admin**).

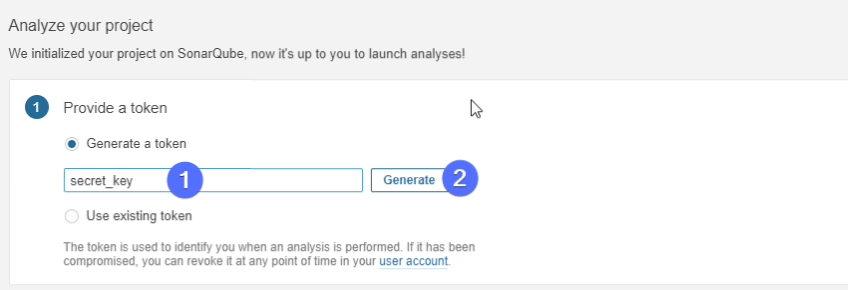
For any configuration changes go to **conf** folder and **sonar.properties**file.

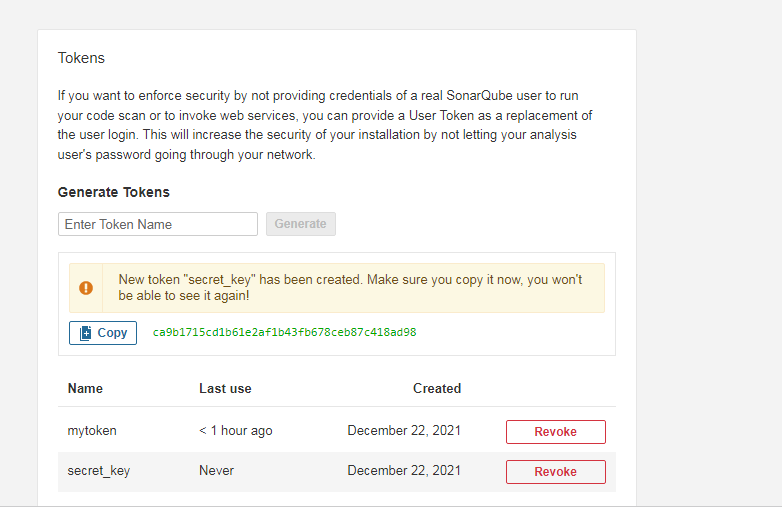
Here you can configure database, LDAP, webserver, SSO authentication, logging, etc…, e.g. for port — under web-server section I have added **sonar.web.port=9001**

<http://localhost:9000/projects>



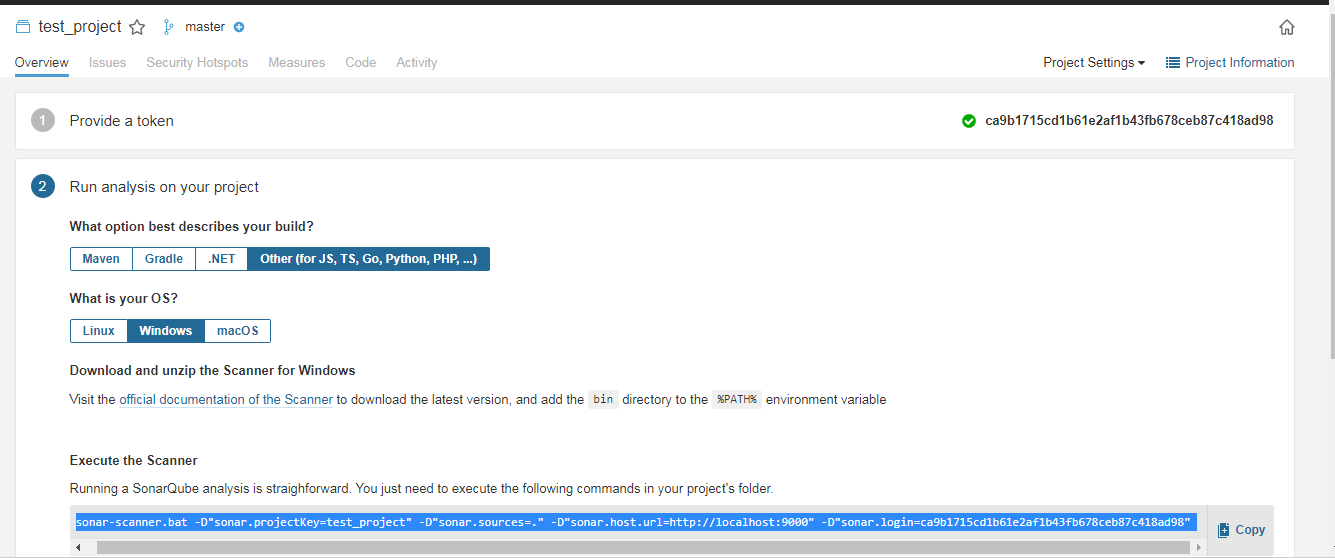
5) Key Creations:



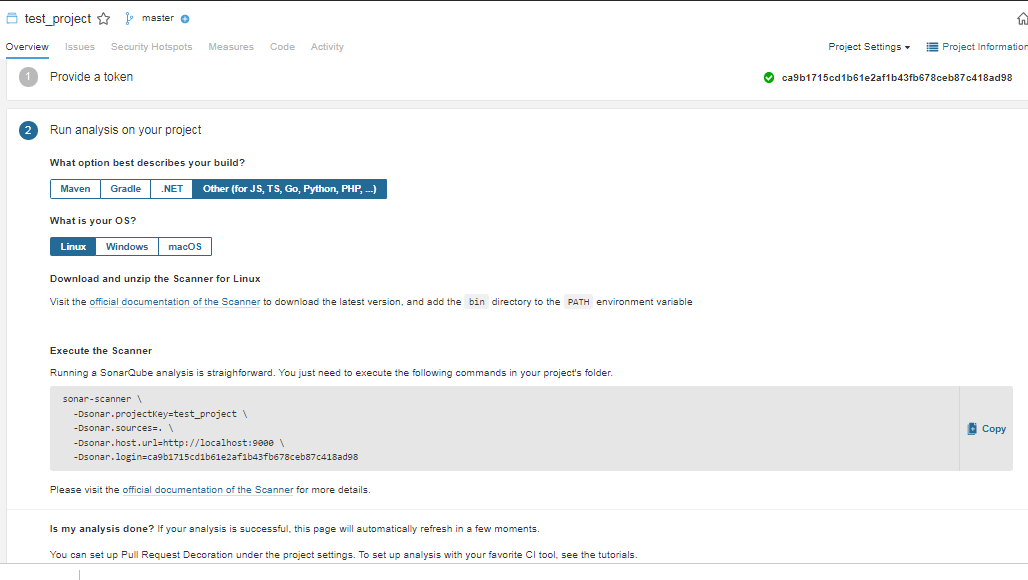


6) As per our OS/Code we need to execute command.

Windows:

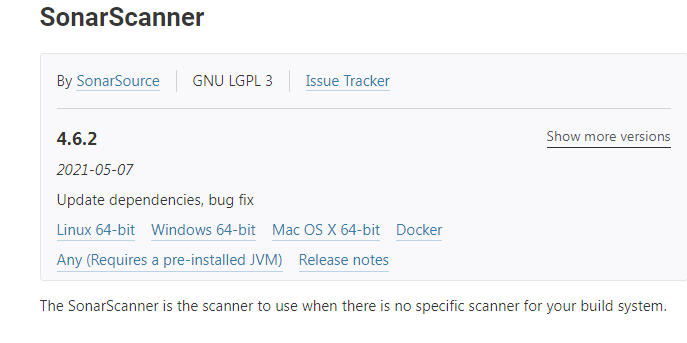


Linux:



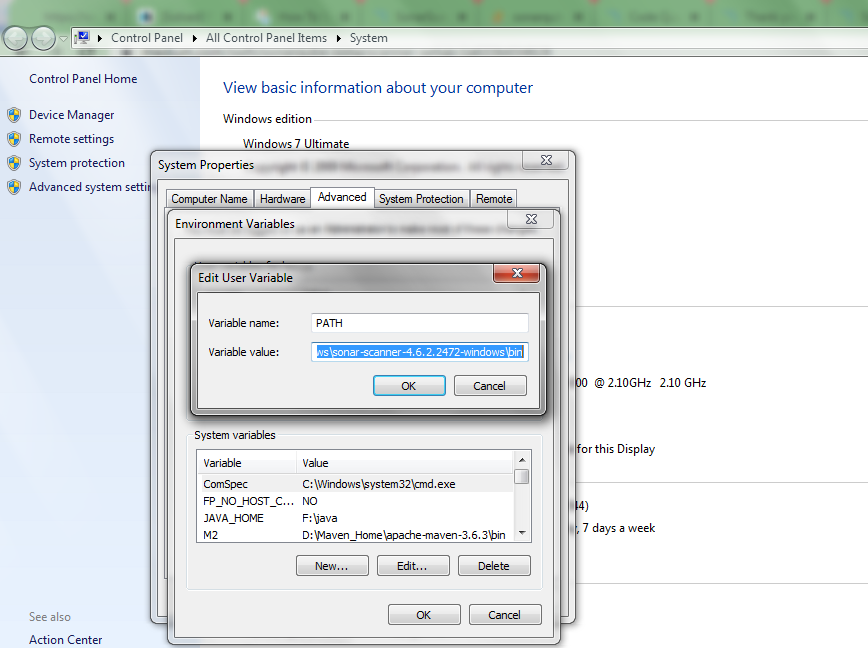
7) Sonar Scanner Setup:

<https://docs.sonarqube.org/latest/analysis/scan/sonarscanner/>



8) After completion of download of sonar scanner, extract the file. (I’ve extracted in the download folder)

**Window** — Register the sonar-scanner path in environment variable.

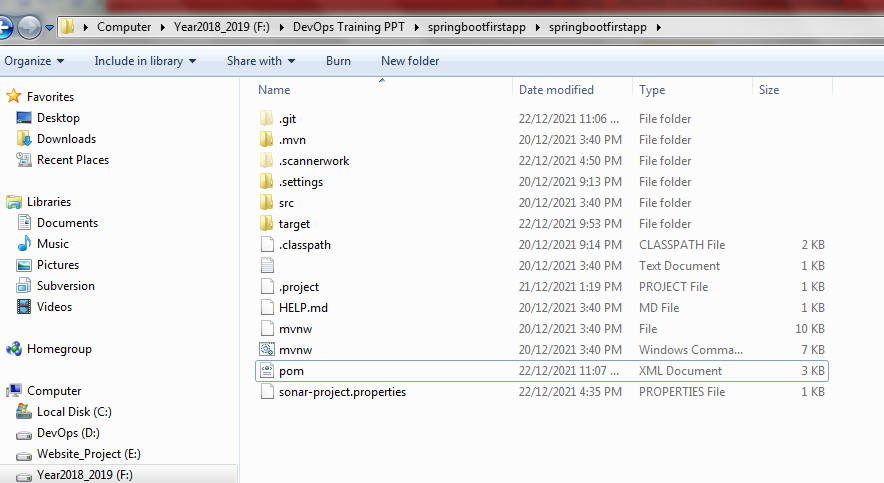


Save the following properties in your project-folder —

with file name **sonar-project.properties**

sonar.projectKey=TLH\_PROJECT\_SQ\_V1  
sonar.projectName=TLH\_PROJECT\_SQ\_V1  
sonar.login = ba4fd\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
sonar.scm.provider = svn  
sonar.projectVersion=1.0  
sonar.sources=src  
sonar.exclusions=node\_modules/\*\*,src/environments/\*\*,\*\*/\*.spec.ts,dist/\*\*,\*\*/docs/\*\*,\*\*/\*.js,e2e/\*\*,coverage/\*\*,TLH-distributions/\*\*,src/bsb-theme/css/\*\*  
sonar.ts.tslint.configPath=tslint.json  
sonar.typescript.lcov.reportPaths=coverage/lcov.info

Add the sonar-project.properties at root level of project.



Now open your project path in Terminal or CMD. Run the following command

sonar-scanner.bat

We can add profile in pom.xml file as well.





On executing below command we can see coverage on sonar dashboard

