

EXPERIMENT - 7

Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to Sonar Qube/Git Lab.

# Theory:

## SAST:

Static Application Security Testing is an automated process that analyzes source code or compiled versions of code to identify potential security vulnerabilities. It's "static" because it examines the code without executing it.

## Jenkins:

Jenkins is an open-source automation server that enables developers to reliably build, test, and deploy their software. It is a server-based system that runs in servlet containers such

as Apache Tomcat. It is an CI/CD tool used in most of the industries.

## SonarQube:

SonarQube is an open-source platform for continuous inspection of code quality, developed by SonarSource. It provides automated analysis and integration with various development tools, enabling developers to write clean, readable, and understandable code.

Integrating SAST into Jenkins allows for automated security checks as part of your build process. Also It can be integrated with SonarQube to provide detailed code analysis reports.

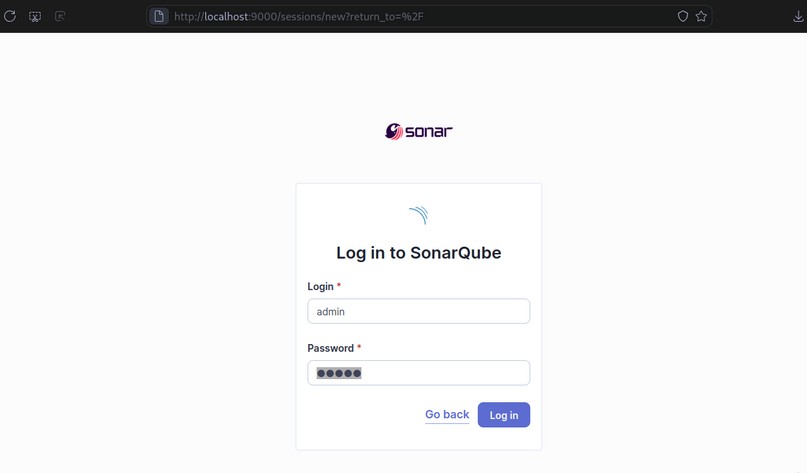
STEPS:

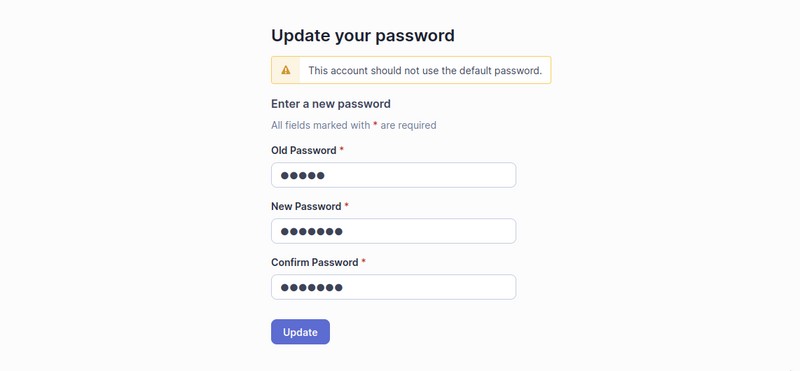
1. First you need to go with the installation part.

❯ docker run -d --name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest

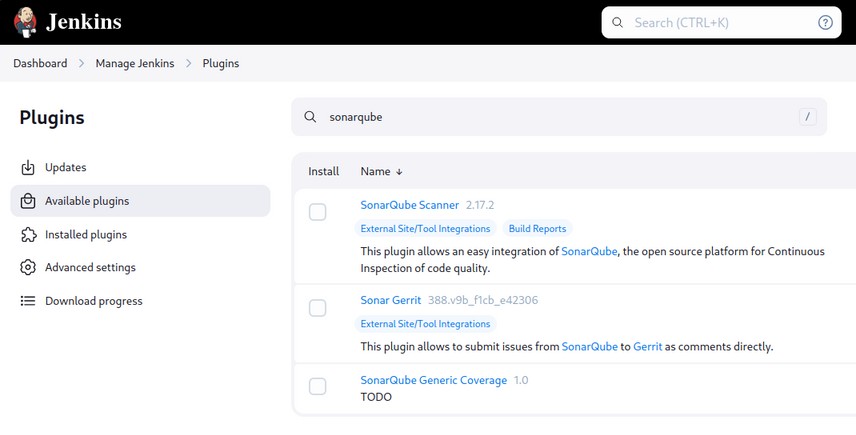
I have used docker, zip file also works well.

1. Then access it on localhost:9000

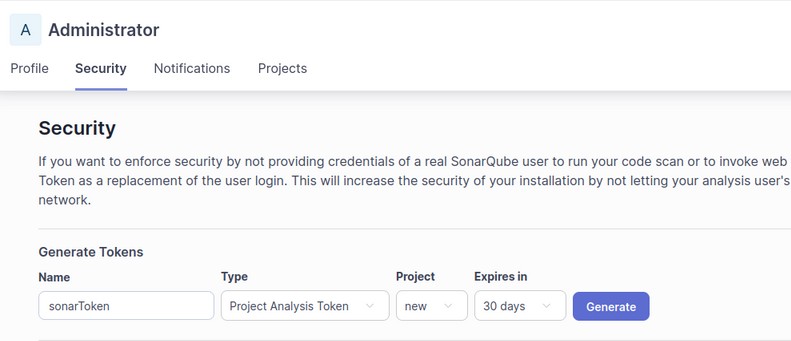
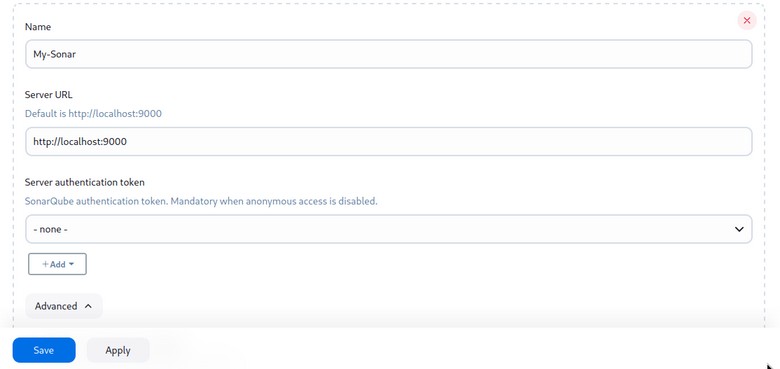




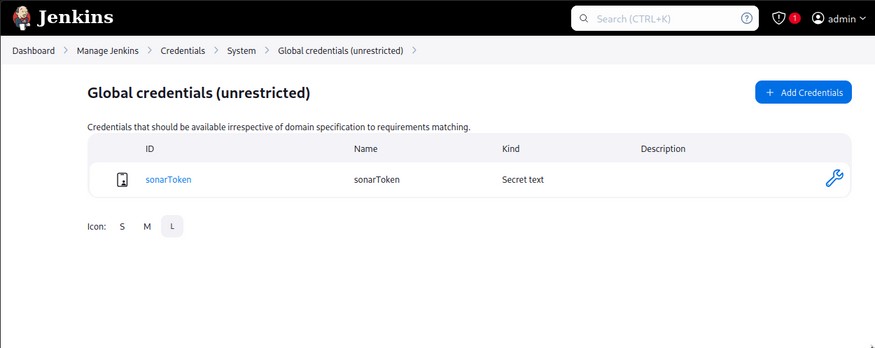
1. Now login to your jenkins dashboard and install SonarQube Scanner plugin.



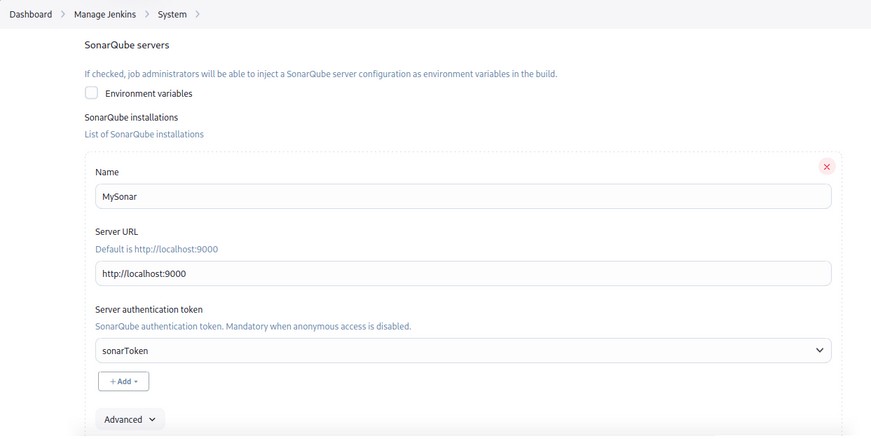
1. Then Go to SonarQube dashboard → Account settings → Secuity → Generate Token. (Make sure you have an project, if not then create)



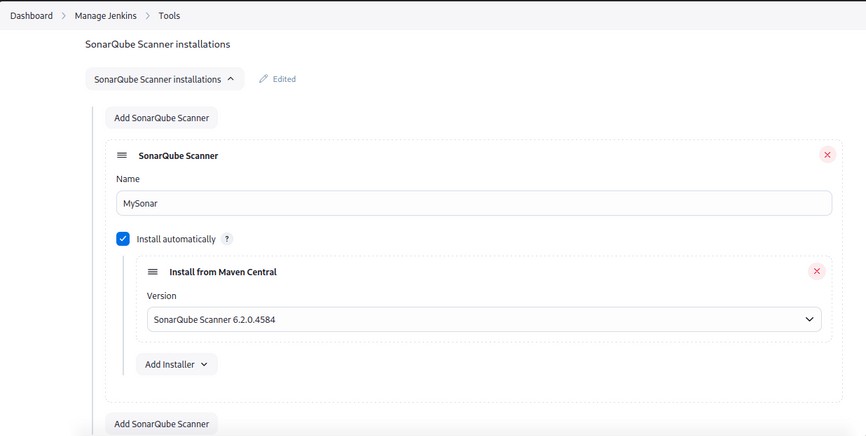
1. Once token is generated add it to Jenkins Credentials as a secret. (Global)



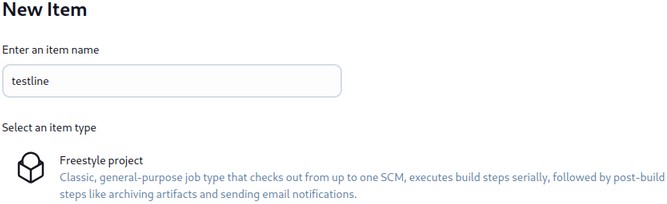
1. Then, Add your SonarQube server with jenkins, and add that credential here and save.



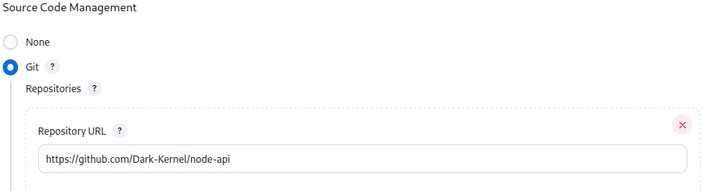
1. Now, setup the SonarQube scanner installations, If you want you can go with manual configuration or just tick “Install Automatically”.



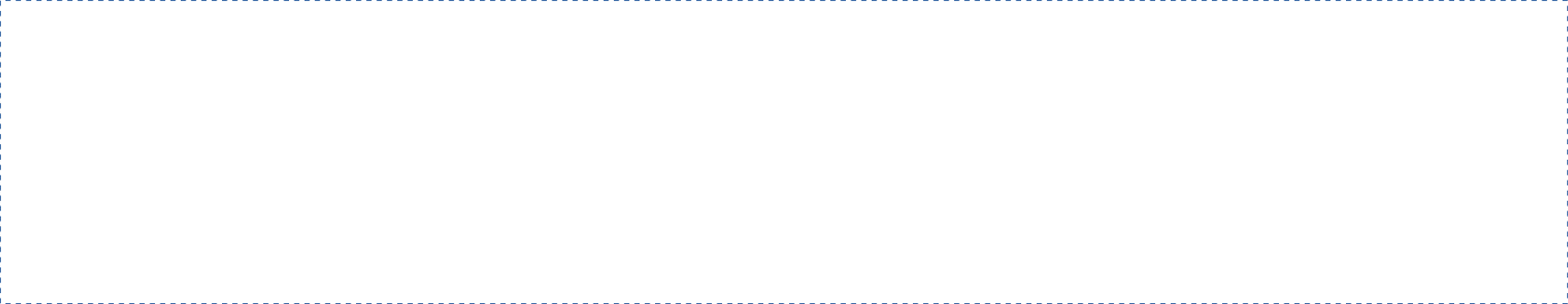
1. Start new item, with type “Freestyle project”.



1. Select your source code repository if it on any git server.



1. You need to create new file ‘sonar-project.properties’ with following configuration:

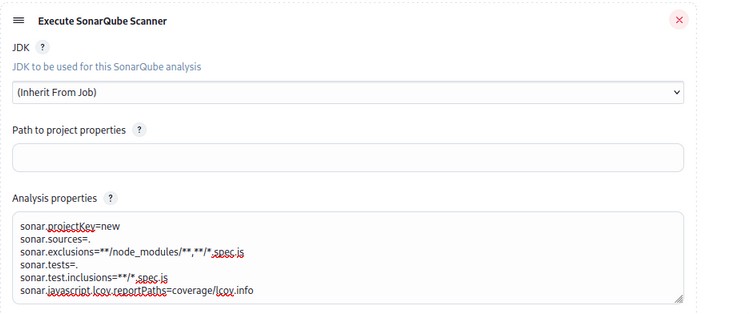


sonar.projectKey=new sonar.sources=.

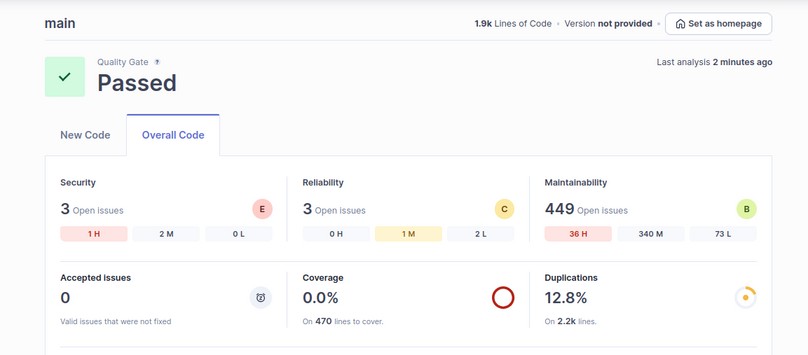
sonar.exclusions=\*\*/node\_modules--\*,\*\*/\*.spec.js sonar.tests=.

sonar.test.inclusions=\*\*/\*.spec.js sonar.javascript.lcov.reportPaths=coverage/lcov.info

Or just add it in Build step.



1. Build the project, then go to sonarQube project.



# Conclusion: Thus, we have successfully understood Static Analysis SAST process

## and learned to integrate Jenkins SAST to SonarQube/GitLab.