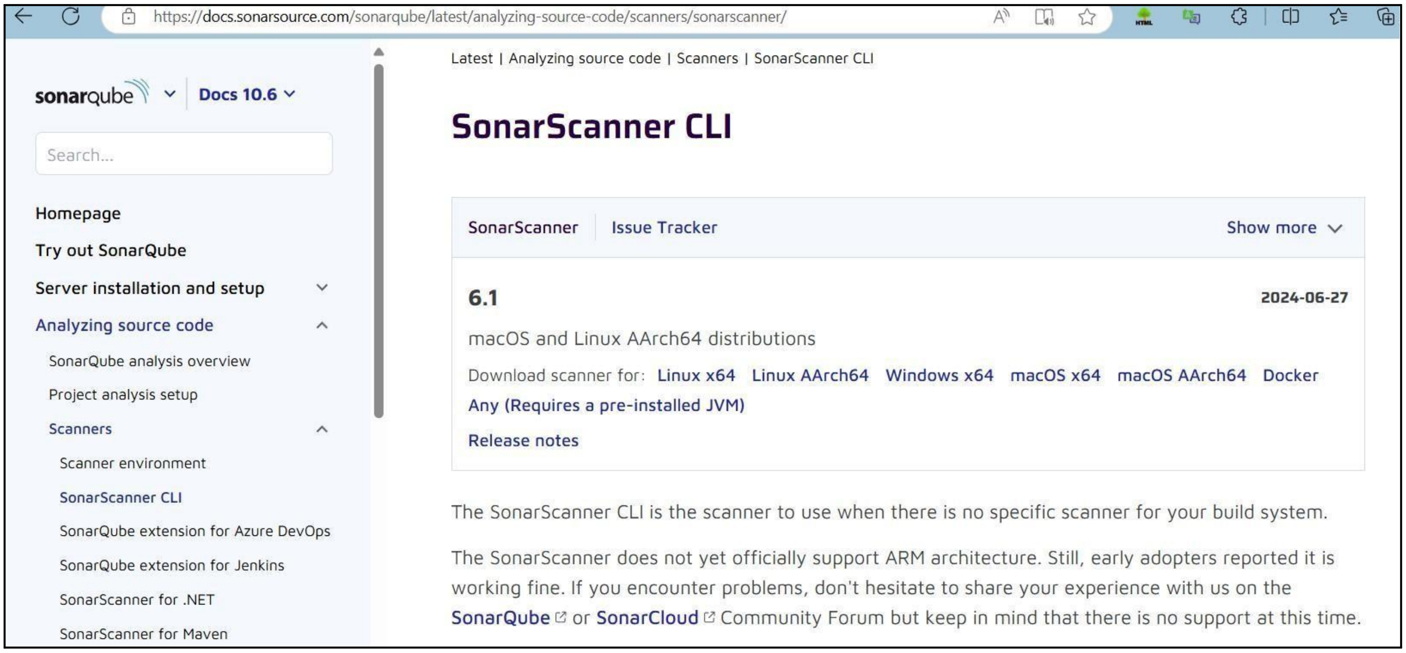
ADVANCE DEVOPS EXP 8

Name:Soham Satpute
Class:D15A
Roll No:52

Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

Step 1: Download sonar scanner

https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscanner/ Visit this link and download the sonarqube scanner CLI.


https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscanner/
sonarqube
Docs 10.6
Search...
Homepage
Try out SonarQube
Server installation and setup
Analyzing source code
SonarQube analysis overview
Project analysis setup
Scanners
Scanner environment
SonarScanner CLI
SonarQube extension for Azure DevOps
SonarQube extension for Jenkins
SonarScanner for .NET
SonarScanner for Maven
Latest | Analyzing source code | Scanners | SonarScanner CLI
SonarScanner
Issue Tracker
Show more

SonarScanner CLI

6.1 2024-06-27

macOS and Linux AArch64 distributions

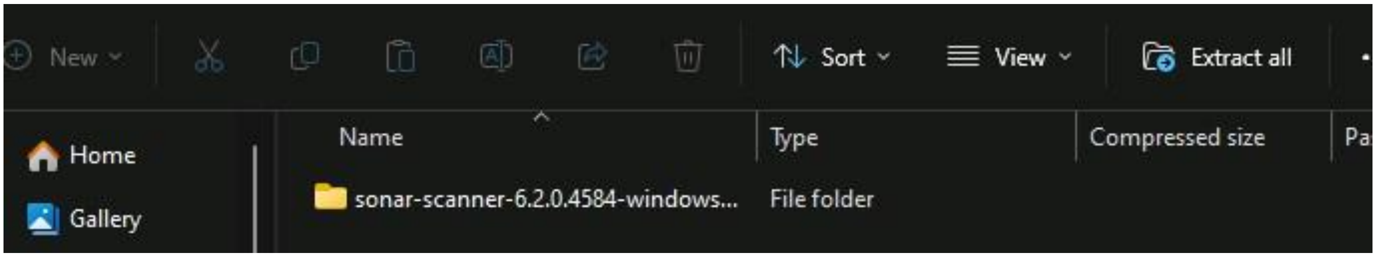
Download scanner for: Linux x64 Linux AArch64 Windows x64 macOS x64 macOS AArch64 Docker Any (Requires a pre-installed JVM)

Release notes

The SonarScanner CLI is the scanner to use when there is no specific scanner for your build system.

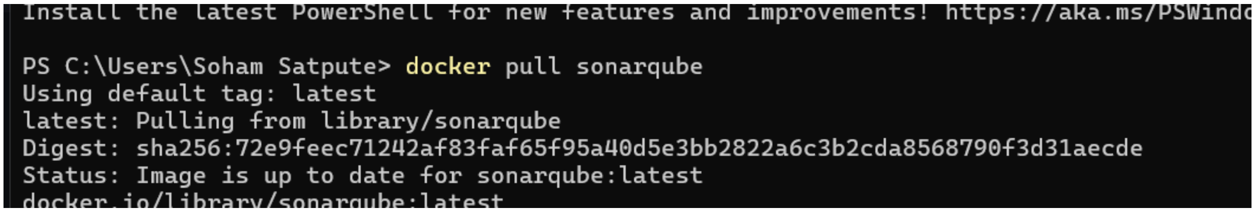
The SonarScanner does not yet officially support ARM architecture. Still, early adopters reported it is working fine. If you encounter problems, don't hesitate to share your experience with us on the SonarQube or SonarCloud Community Forum but keep in mind that there is no support at this time.

Extract the downloaded zip file in a folder.



Name	Type	Compressed size	Pa
sonar-scanner-6.2.0.4584-windows...	File folder		

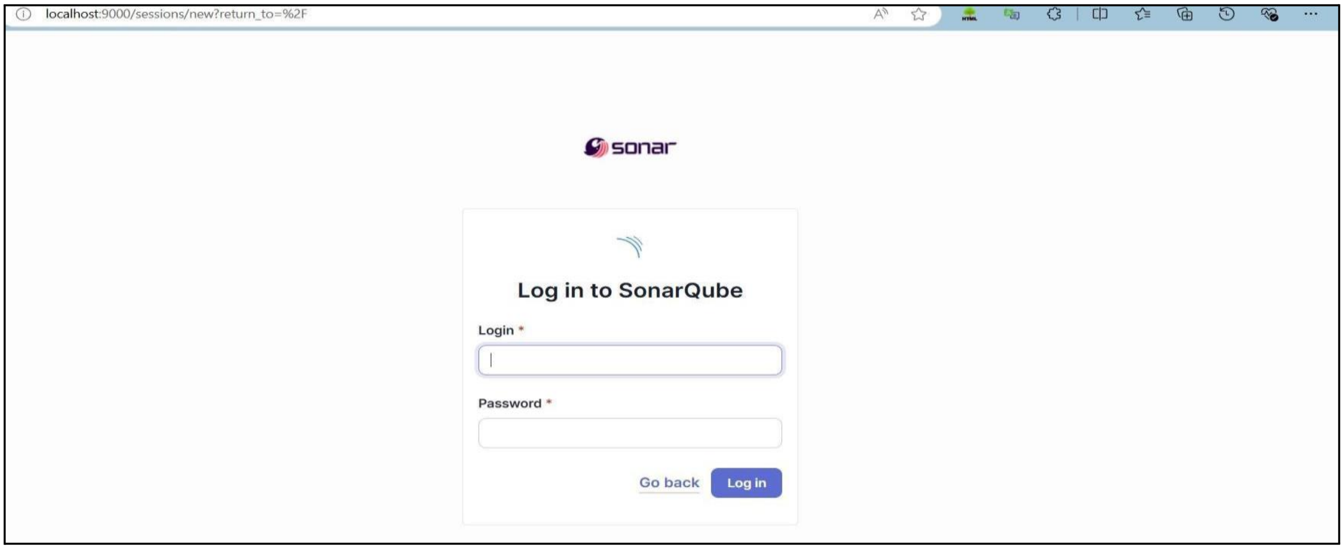
1. Install sonarqube image Command: **docker pull sonarqube**



```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindo

PS C:\Users\Soham Satpute> docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Image is up to date for sonarqube:latest
docker.io/library/sonarqube:latest
```

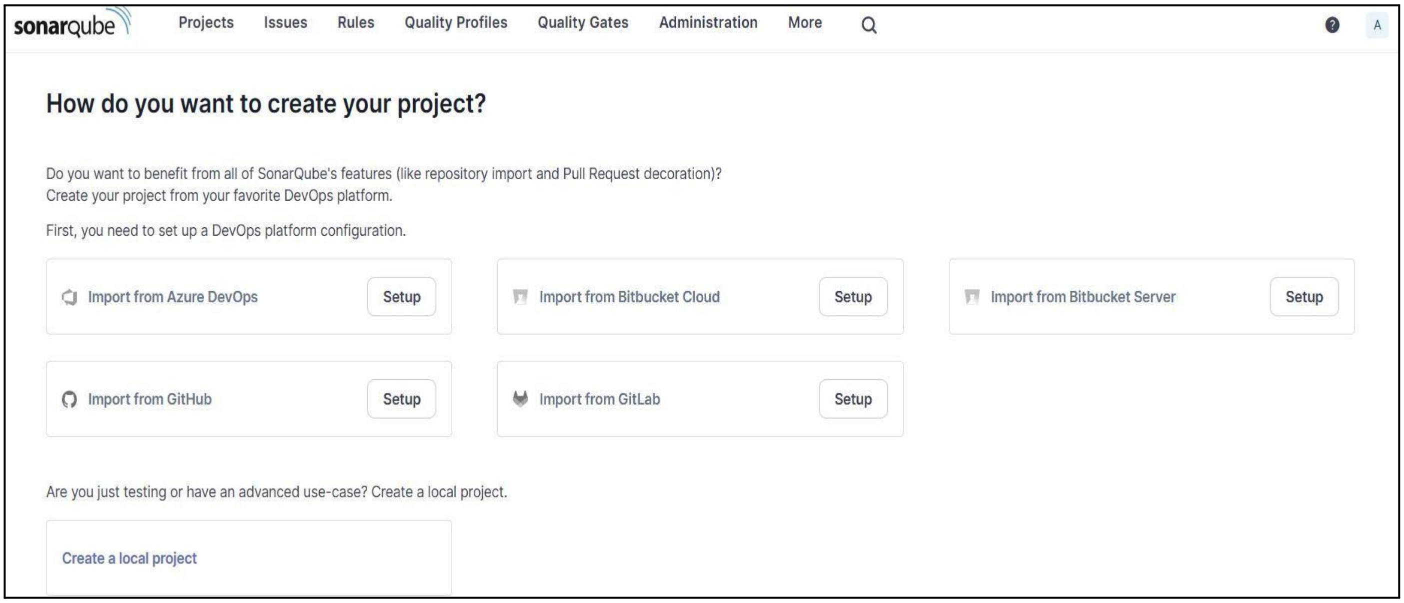
2. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.



localhost:9000/sessions/new?return_to=%2F

Log in to SonarQube

3. Login to SonarQube using username admin and password admin.



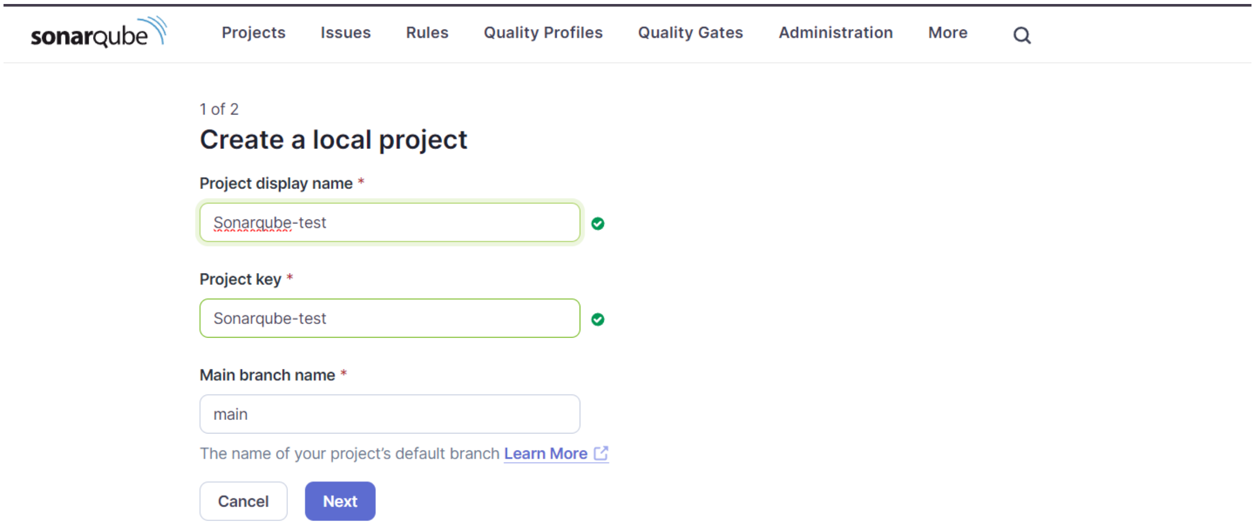
How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)?
Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Are you just testing or have an advanced use-case? Create a local project.

4. Create a manual project in SonarQube with the name sonarqube



1 of 2

Create a local project

Project display name *

Sonarqube-test

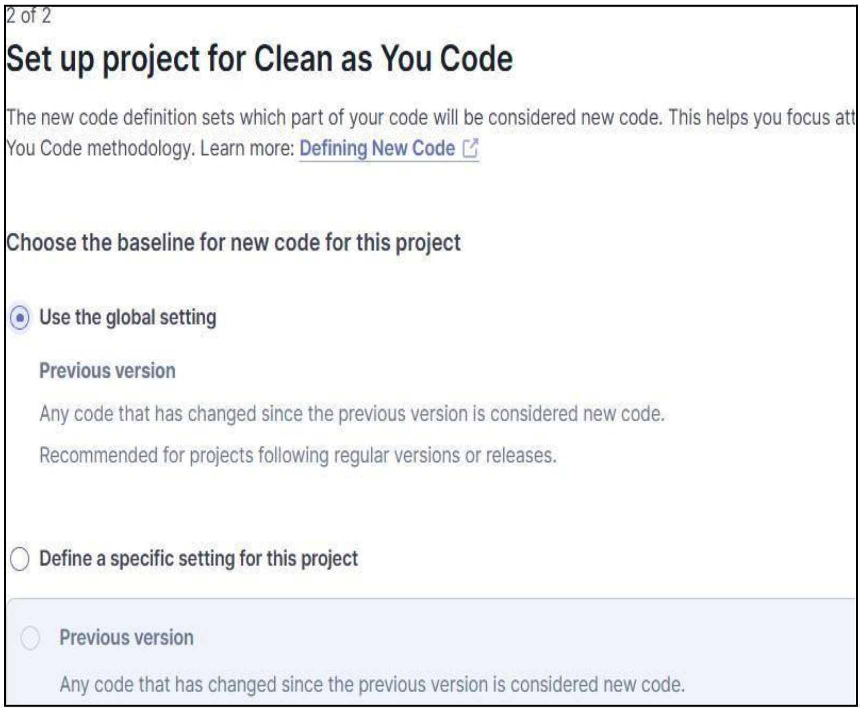
Project key *

Sonarqube-test

Main branch name *

main

The name of your project's default branch Learn More



2 of 2

Set up project for Clean as You Code

The new code definition sets which part of your code will be considered new code. This helps you focus att
You Code methodology. Learn more: Defining New Code

Choose the baseline for new code for this project

● Use the global setting

Previous version

Any code that has changed since the previous version is considered new code.

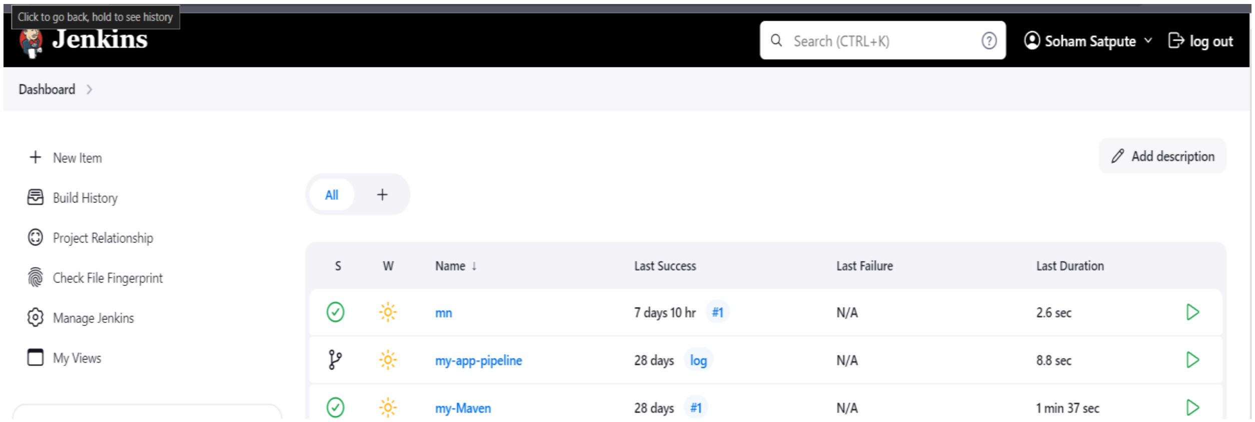
Recommended for projects following regular versions or releases.

○ Define a specific setting for this project

○ Previous version

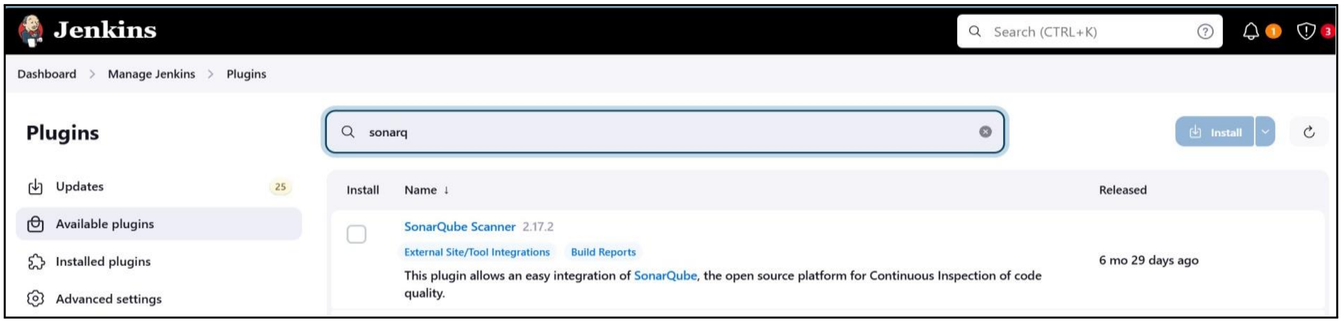
Any code that has changed since the previous version is considered new code.

5. Open up Jenkins Dashboard on localhost, port 8080 or whichever port it is at for you.

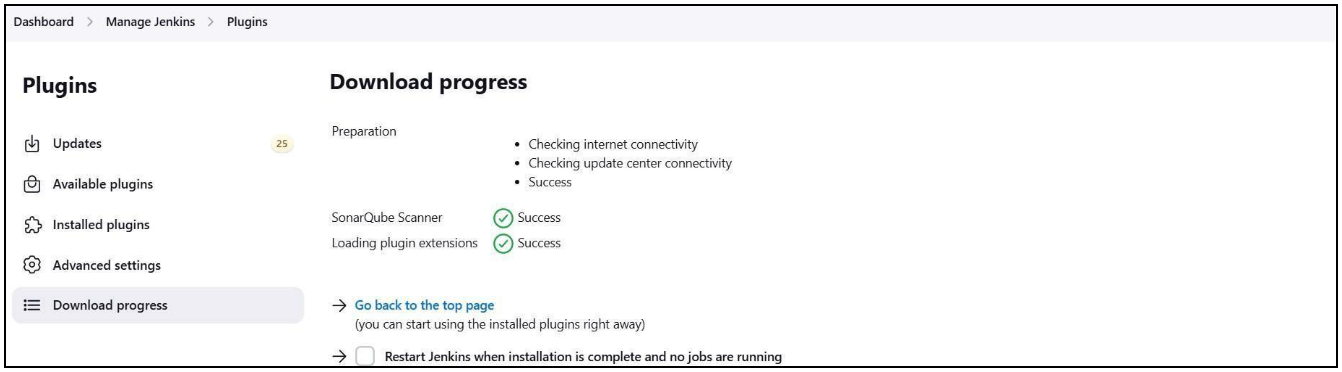


S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☼	mn	7 days 10 hr #1	N/A	2.6 sec
	☼	my-app-pipeline	28 days log	N/A	8.8 sec
✓	☼	my-Maven	28 days #1	N/A	1 min 37 sec

6. Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.



Install	Name ↓	Released
□	SonarQube Scanner 2.17.2 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.	6 mo 29 days ago



Download progress

Preparation
- Checking internet connectivity
- Checking update center connectivity
- Success

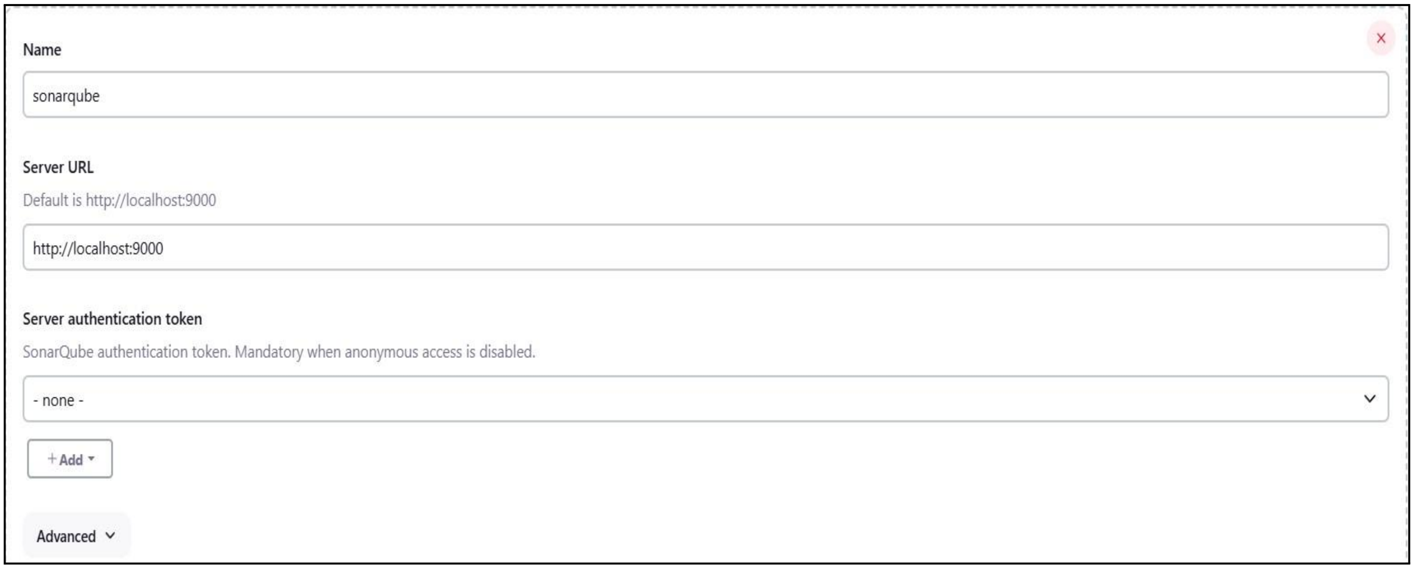
SonarQube Scanner ✓ Success
Loading plugin extensions ✓ Success

→ Go back to the top page
(you can start using the installed plugins right away)

→ □ Restart Jenkins when installation is complete and no jobs are running

7.Under Jenkins 'Manage Jenkins' then go to 'system', scroll and look for **SonarQube Servers** and enter
the details.
Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube> for me **adv_devops_7_sonarqube**
In **Server URL** Default is **http://localhost:9000**



Name

sonarqube

Server URL

Default is http://localhost:9000

http://localhost:9000

Server authentication token

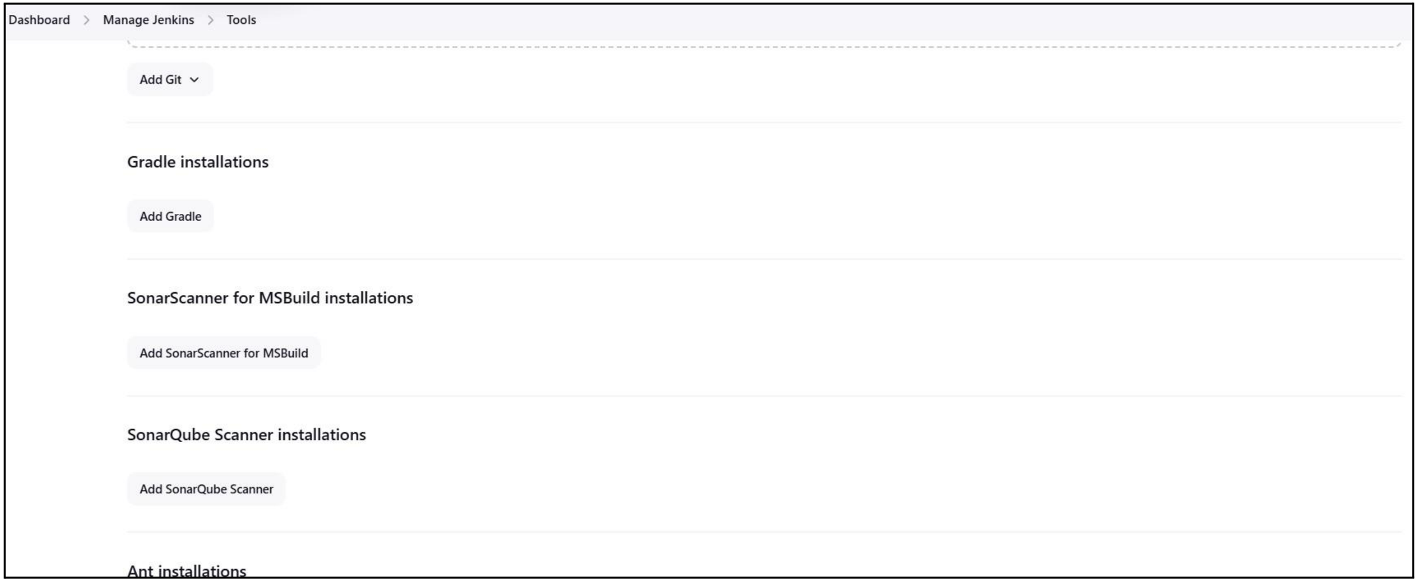
SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

8. Search for SonarQube Scanner under Global Tool Configuration.

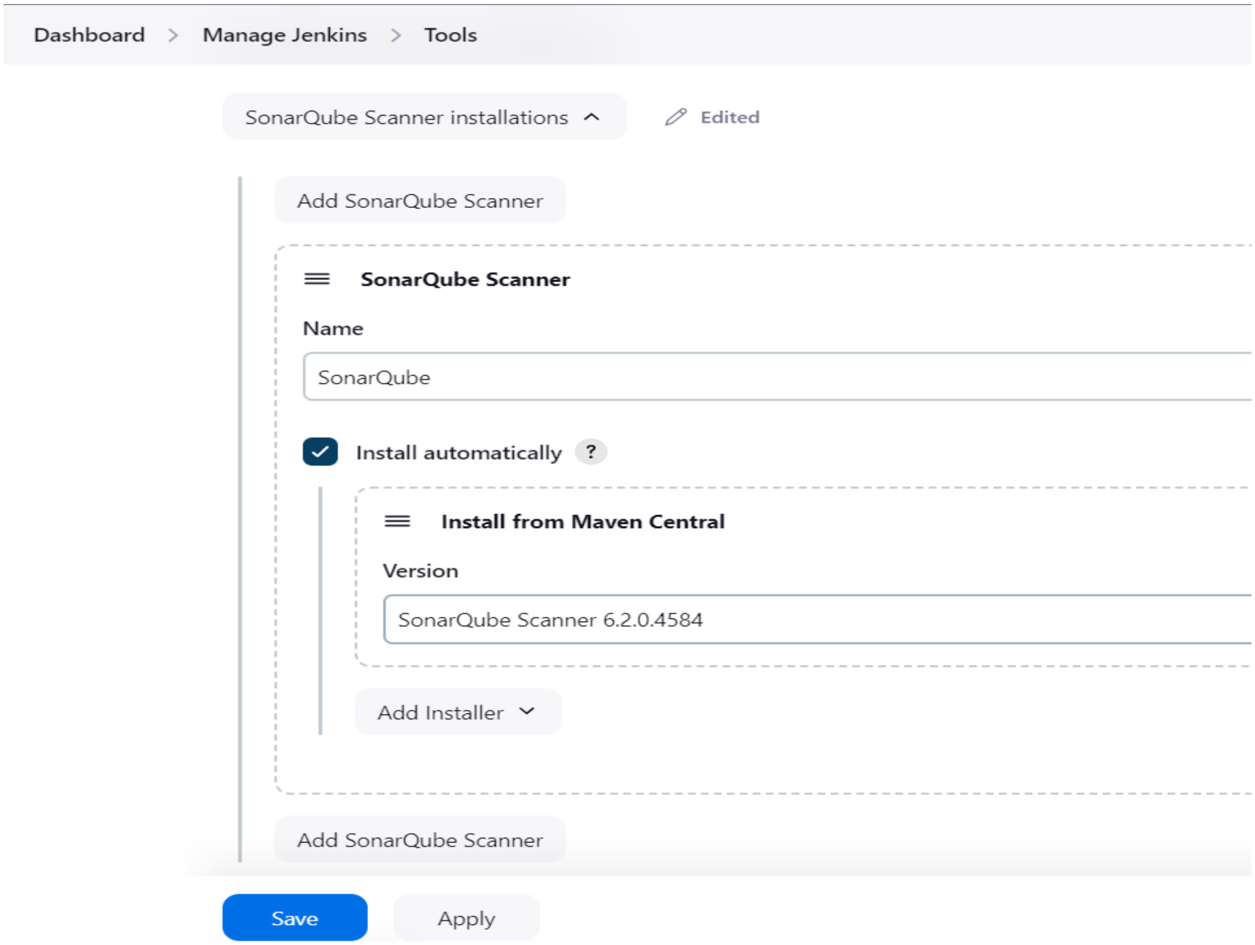
Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools



Dashboard > Manage Jenkins > Tools
Add Git
Gradle installations
Add Gradle
SonarScanner for MSBuild installations
Add SonarScanner for MSBuild
SonarQube Scanner installations
Add SonarQube Scanner
Ant installations

Check the “Install automatically” option. → Under name any name as identifier → Check



Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations — Edited

Add SonarQube Scanner

SonarQube Scanner

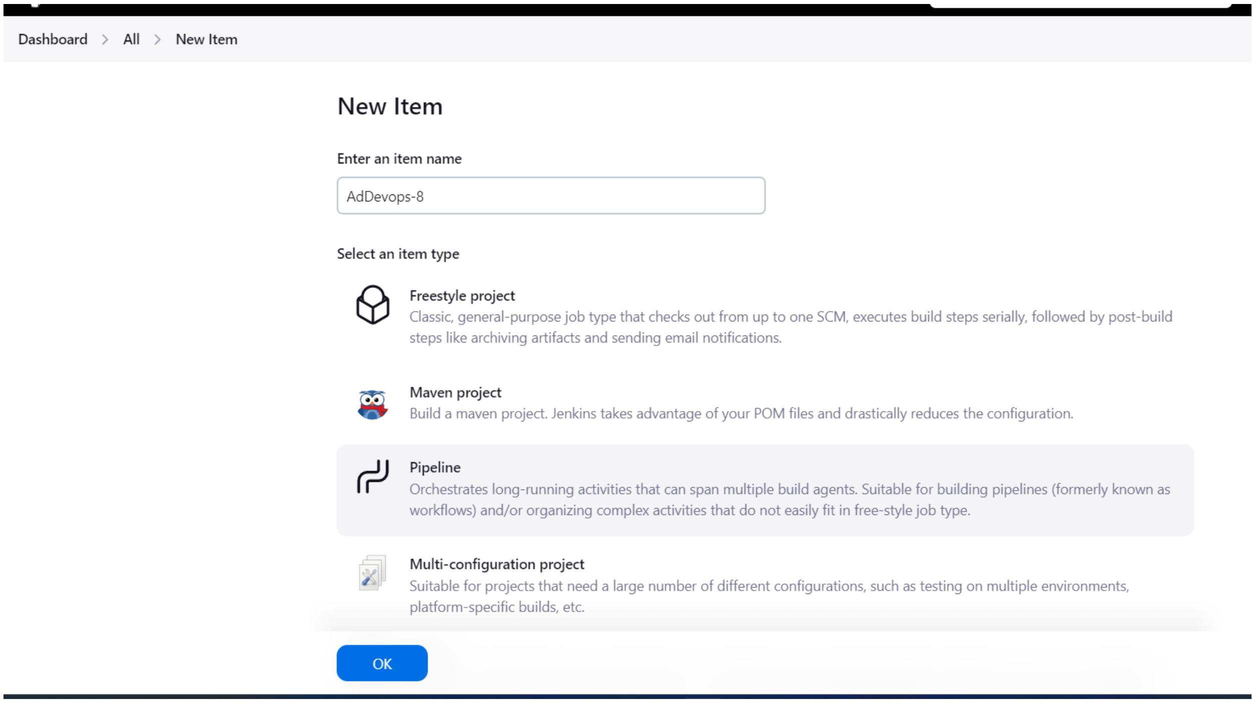
Name: SonarQube

☑ Install automatically

Install from Maven Central

Version: SonarQube Scanner 6.2.0.4584

9. After configuration, create a New Item → choose a pipeline project.



Dashboard > All > New Item

New Item

Enter an item name: AdDevops-8

Select an item type

Freestyle project
Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.

Maven project
Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

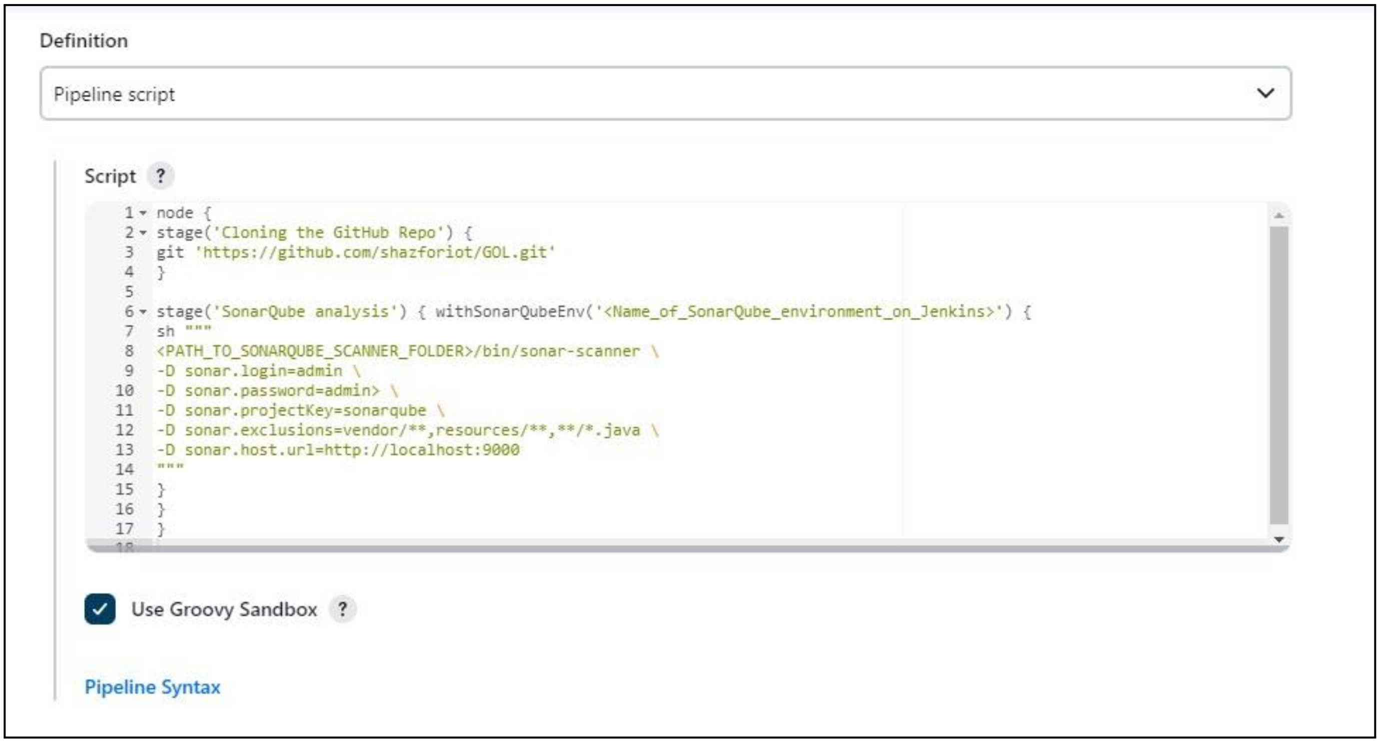
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

10. Under Pipeline script, enter the following:

```
      node {
  stage('Cloning the GitHub Repo') {
    git 'https://github.com/shazforiot/GOL.git'
  }

  stage('SonarQube analysis') {
    withSonarQubeEnv('<Name_of_SonarQube_environment_on_Jenki
    ns>') {
      sh """
        <PATH_TO_SONARQUBE_SCANNER_FOLDER>/bin/sonar-scanner \
        -D sonar.login=<SonarQube_USERNAME> \
        -D sonar.password=<SonarQube_PASSWORD> \
        -D sonar.projectKey=<Project_KEY> \
        -D sonar.exclusions=vendor/**,resources/**,**/*.java \
        -D sonar.host.url=<SonarQube_URL>(default: http://localhost:9000/)
      """
    }
  }
}
```

It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

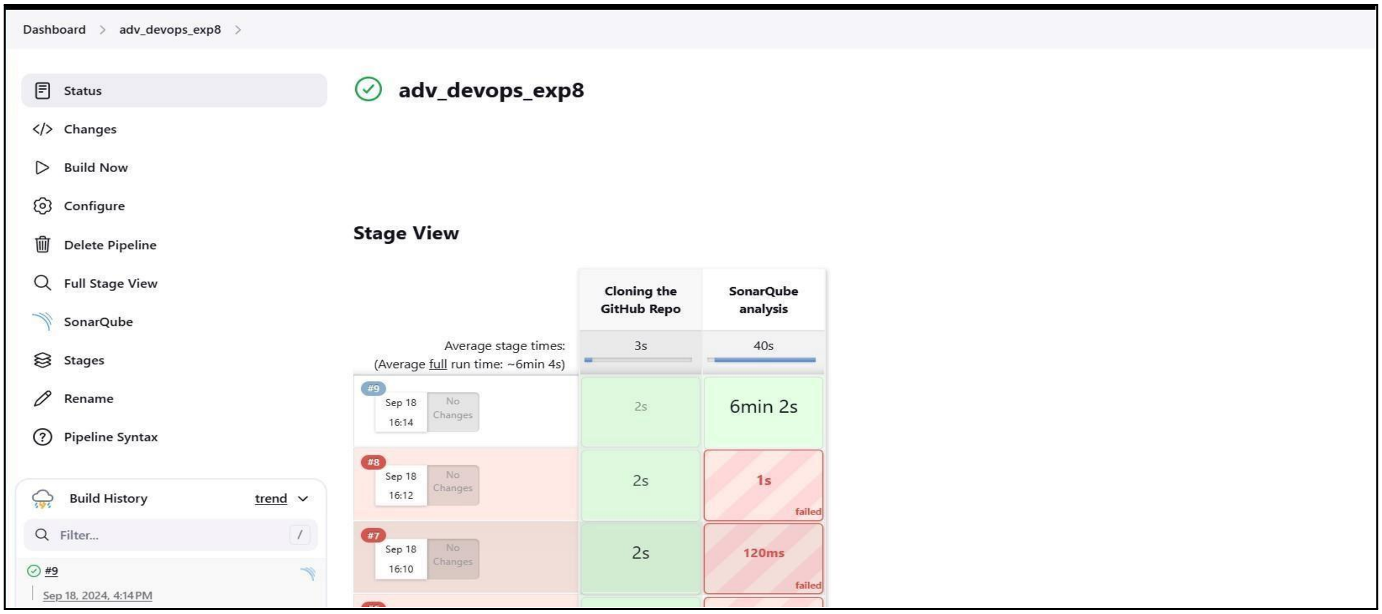


```
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}

stage('SonarQube analysis') { withSonarQubeEnv('<Name_of_SonarQube_environment_on_Jenkins>') {
sh """
<PATH_TO_SONARQUBE_SCANNER_FOLDER>/bin/sonar-scanner \
-D sonar.login=admin \
-D sonar.password=admin> \
-D sonar.projectKey=sonarqube \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://localhost:9000
"""
}
}
}
```

☑ Use Groovy Sandbox ?

11.Build project



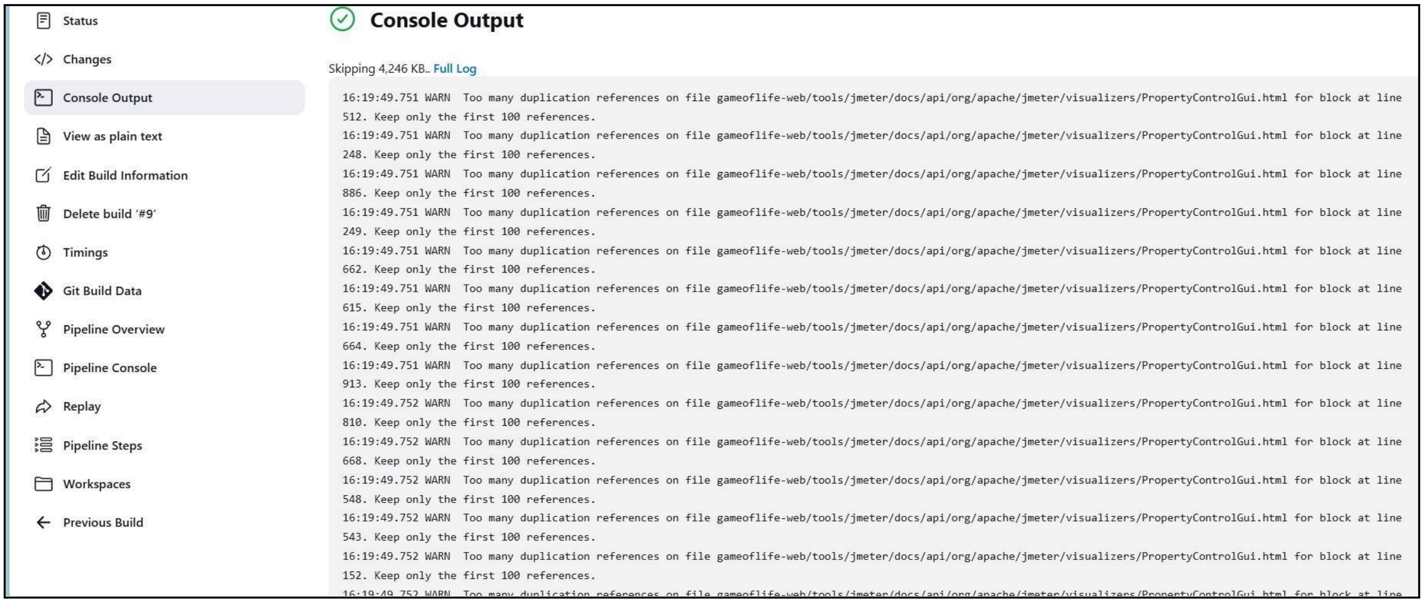
#9
Sep 18, 2024, 4:14 PM

adv_devops_exp8

Stage View

	Cloning the GitHub Repo	SonarQube analysis
Average stage times: (Average full run time: ~6min 4s)	3s	40s
#9 Sep 18 16:14 No Changes	2s	6min 2s
#8 Sep 18 16:12 No Changes	2s	1s failed
#7 Sep 18 16:10 No Changes	2s	120ms failed

12. Check console

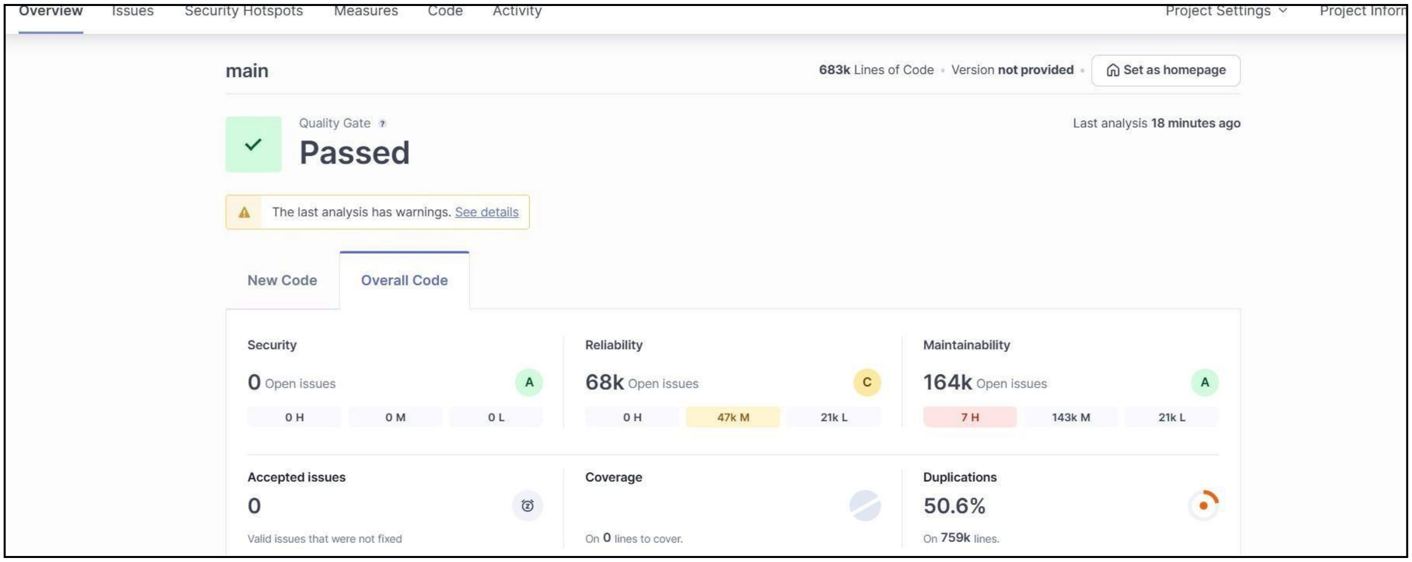


Console Output

Skipping 4,246 KB.. Full Log

```
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
512. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
248. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
886. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
249. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
662. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
615. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
664. Keep only the first 100 references.
16:19:49.751 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
913. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
810. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
668. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
548. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
543. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
152. Keep only the first 100 references.
16:19:49.752 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/visualizers/PropertyControlGui.html for block at line
```

13. Now, check the project in SonarQube



main

683k Lines of Code • Version not provided

Quality Gate

Passed

Last analysis 18 minutes ago

The last analysis has warnings. See details

Security

0 Open issues A

0 H | 0 M | 0 L

Reliability

68k Open issues C

0 H | 47k M | 21k L

Maintainability

164k Open issues A

7 H | 143k M | 21k L

Accepted issues

0

Valid issues that were not fixed

Coverage

On 0 lines to cover.

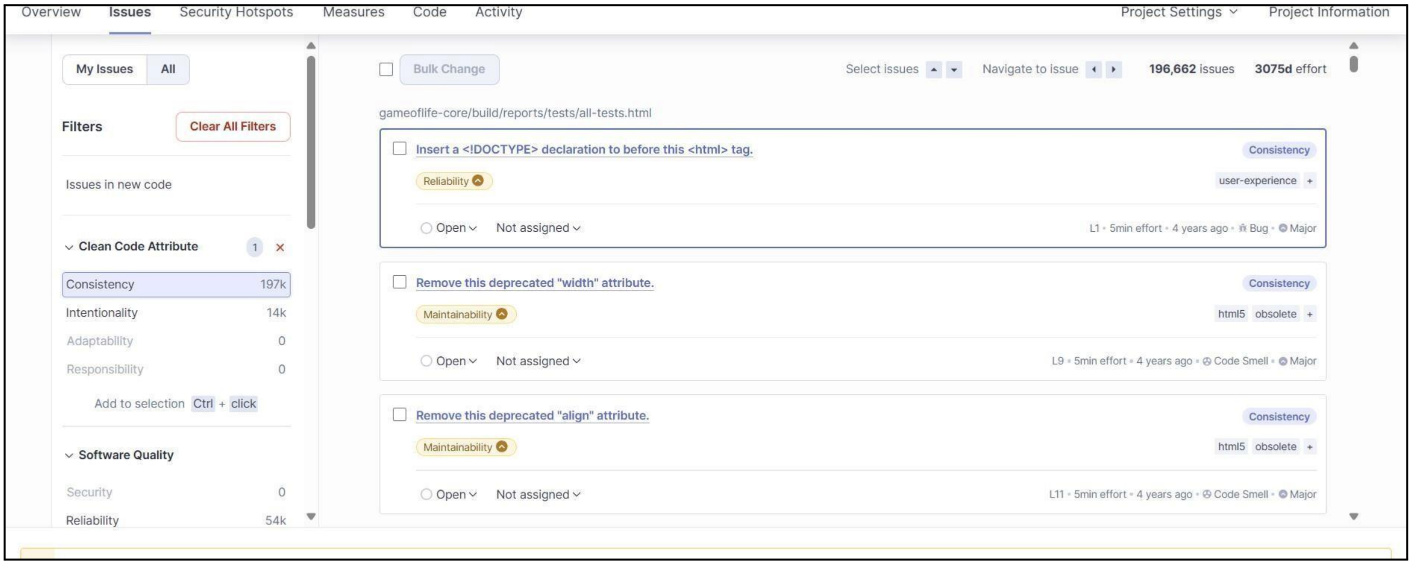
Duplications

50.6%

On 759k lines.

14. Code Problems

- Consistency



196,662 issues 3075d effort

Issues in new code

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

Security	0
Reliability	54k

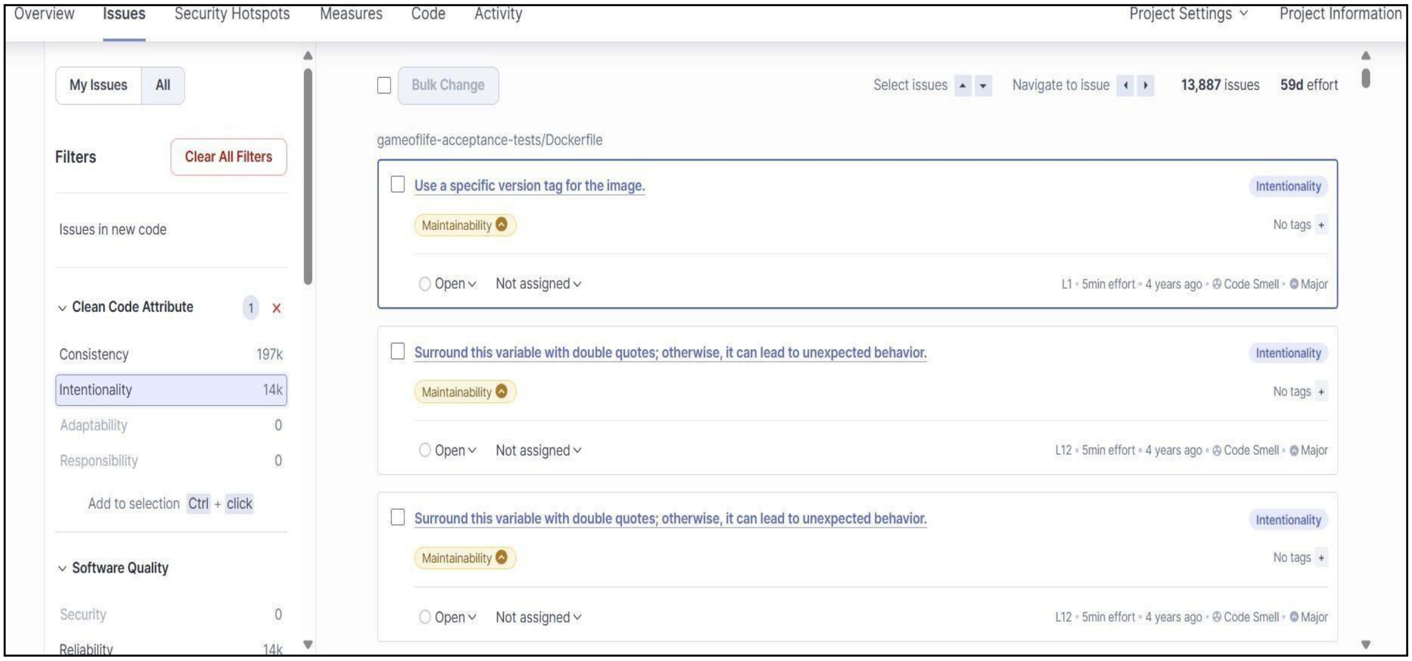
gameoflife-core/build/reports/tests/all-tests.html

□ Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency — Reliability — user-experience +
○ Open Not assigned — L1 • 5min effort • 4 years ago • Bug • Major

□ Remove this deprecated "width" attribute. — Consistency — Maintainability — html5 obsolete +
○ Open Not assigned — L9 • 5min effort • 4 years ago • Code Smell • Major

□ Remove this deprecated "align" attribute. — Consistency — Maintainability — html5 obsolete +
○ Open Not assigned — L11 • 5min effort • 4 years ago • Code Smell • Major

- Intentionality



13,887 issues 59d effort

Issues in new code

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

Security	0
Reliability	14k

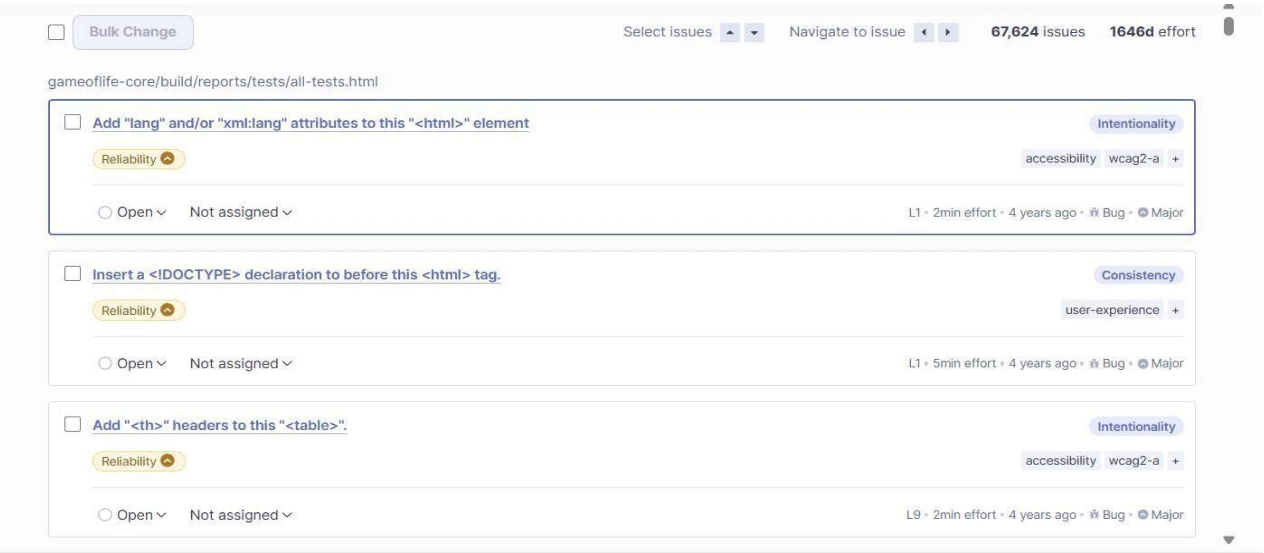
gameoflife-acceptance-tests/Dockerfile

□ Use a specific version tag for the image. — Intentionality — Maintainability — No tags +
○ Open Not assigned — L1 • 5min effort • 4 years ago • Code Smell • Major

□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags +
○ Open Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major

□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags +
○ Open Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major

- Bugs



67,624 issues **1646d** effort

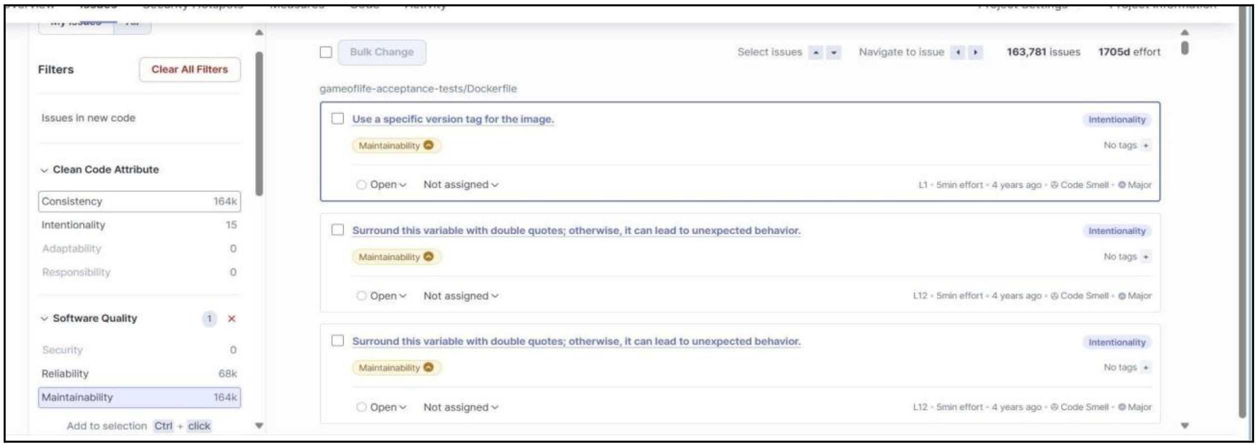
gameoflife-core/build/reports/tests/all-tests.html

□ Add "lang" and/or "xml:lang" attributes to this "<html>" element Intentionality
Reliability accessibility wcag2-a +
○ Open Not assigned L1 · 2min effort · 4 years ago · Bug · Major

□ Insert a <!DOCTYPE> declaration to before this <html> tag. Consistency
Reliability user-experience +
○ Open Not assigned L1 · 5min effort · 4 years ago · Bug · Major

□ Add "<th>" headers to this "<table>". Intentionality
Reliability accessibility wcag2-a +
○ Open Not assigned L9 · 2min effort · 4 years ago · Bug · Major

- Code Smells



Clean Code Attribute

Consistency	164k
Intentionality	15
Adaptability	0
Responsibility	0

Software Quality 1 ×

Security	0
Reliability	68k
Maintainability	164k

163,781 issues **1705d** effort

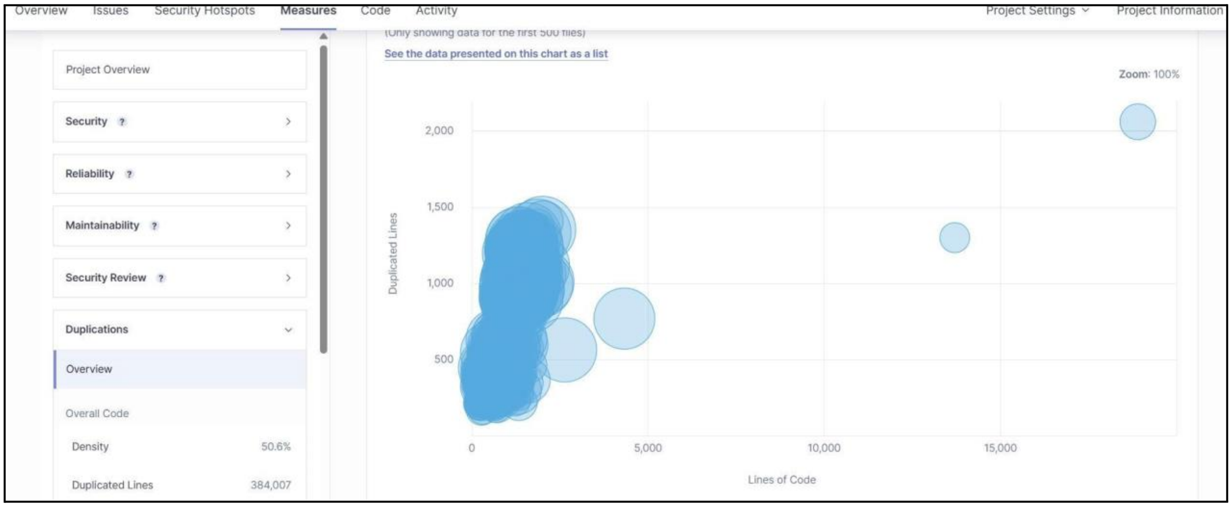
gameoflife-acceptance-tests/Dockerfile

□ Use a specific version tag for the image. Intentionality
Maintainability No tags +
○ Open Not assigned L1 · 5min effort · 4 years ago · Code Smell · Major

□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality
Maintainability No tags +
○ Open Not assigned L12 · 5min effort · 4 years ago · Code Smell · Major

□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality
Maintainability No tags +
○ Open Not assigned L12 · 5min effort · 4 years ago · Code Smell · Major

- Duplications



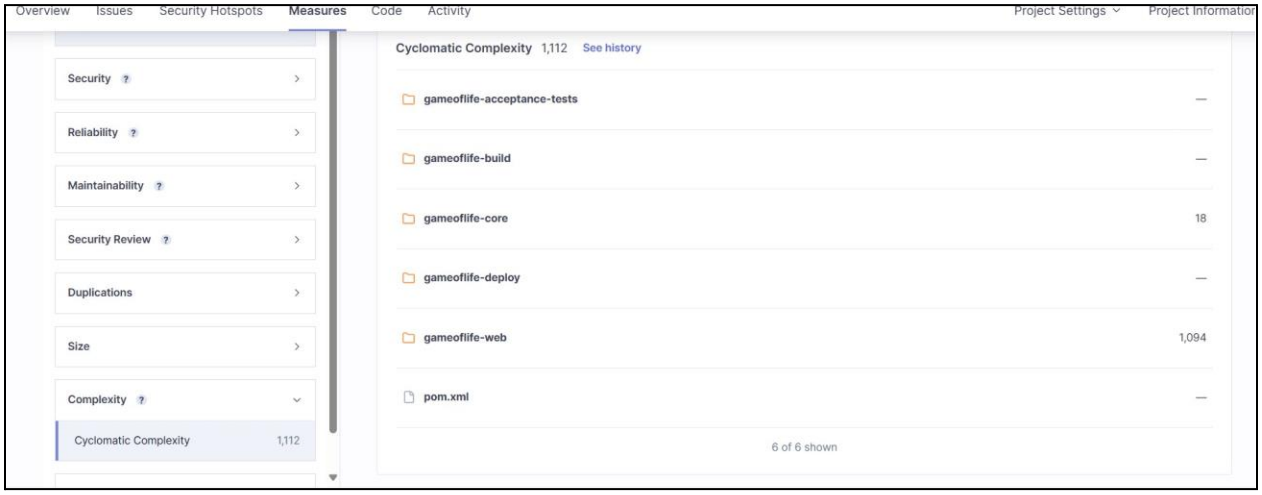
(Only showing data for the first 500 files)

See the data presented on this chart as a list

Overall Code

Density	50.6%
Duplicated Lines	384,007

- Cyclomatic Complexities



Cyclomatic Complexity 1,112

gameoflife-acceptance-tests	—
gameoflife-build	—
gameoflife-core	18
gameoflife-deploy	—
gameoflife-web	1,094
pom.xml	—

6 of 6 shown

In this way, we have integrated Jenkins with SonarQube for SAST.

p