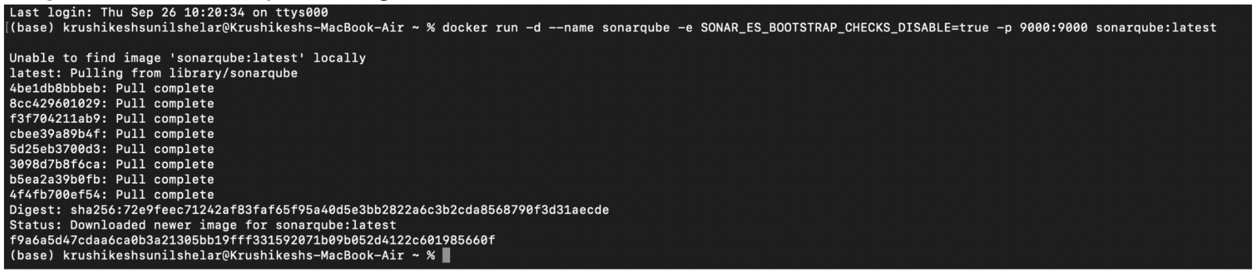
08 Advanced DevOps Lab

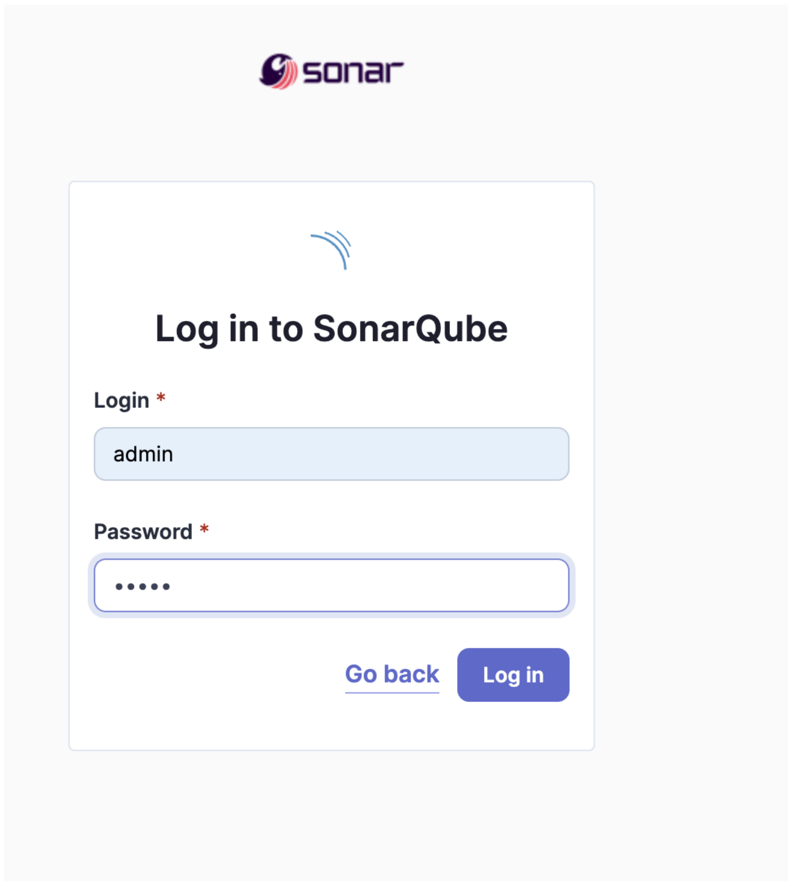
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

Step 1: Install sonarqube image



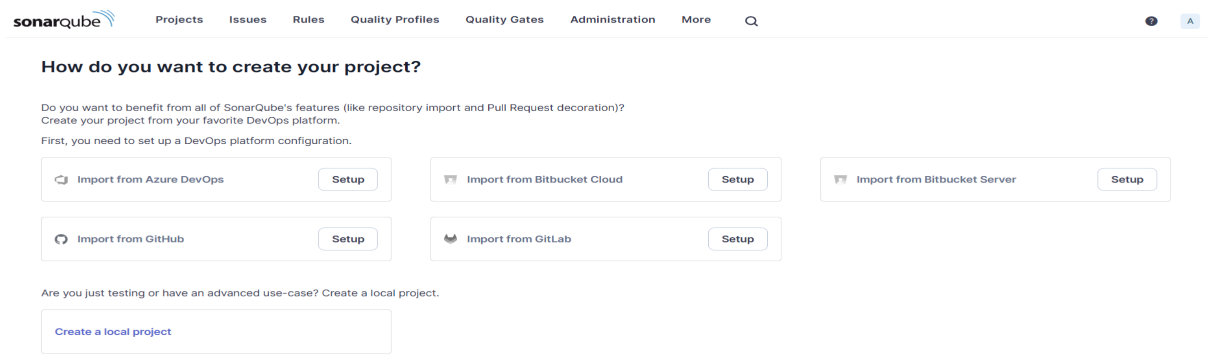
```
Last login: Thu Sep 26 10:20:34 on ttys000
(base) krushikeshsunilshelar@Krushikeshs-MacBook-Air ~ % docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
4be1db8bbbeb: Pull complete
8cc429601029: Pull complete
f3f704211ab9: Pull complete
cbee39a89b4f: Pull complete
5d25eb3700d3: Pull complete
3098d7b8f6ca: Pull complete
b5ea2a39b0fb: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
f9a6a5d47cdaa6ca0b3a21305bb19fff331592071b09b052d4122c601985660f
(base) krushikeshsunilshelar@Krushikeshs-MacBook-Air ~ % 
```

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



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

Krushikesh Shelar 51. D15-C


sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

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.

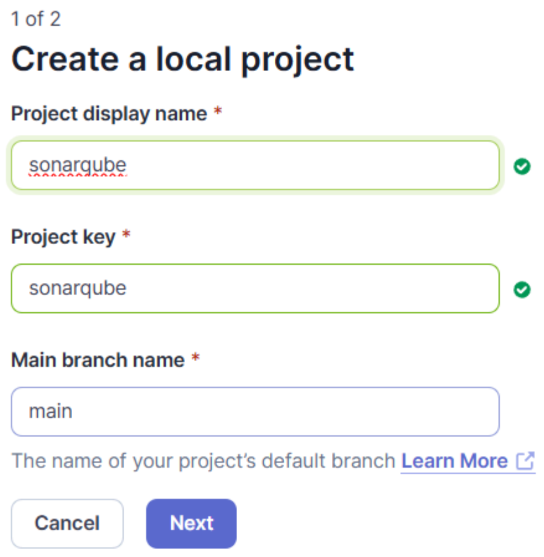
First, you need to set up a DevOps platform configuration.

Import from Azure DevOps — Setup	Import from Bitbucket Cloud — Setup	Import from Bitbucket Server — Setup
Import from GitHub — Setup	Import from GitLab — Setup	

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

Create a local project

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


1 of 2

Create a local project

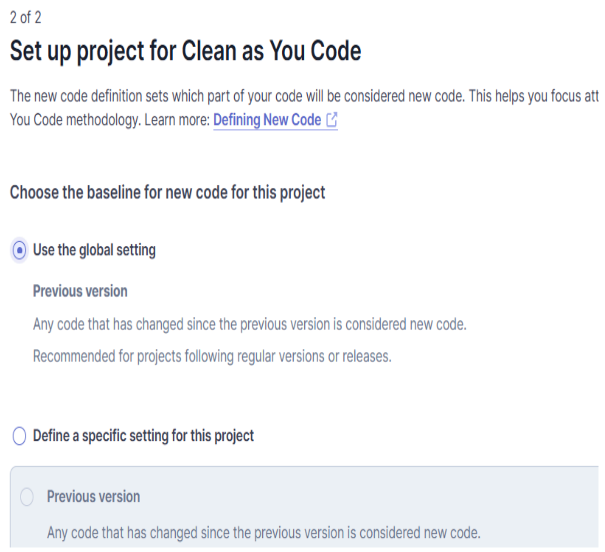
Project display name *: sonarqube

Project key *: sonarqube

Main branch name *: main

The name of your project's default branch Learn More

Cancel Next


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.

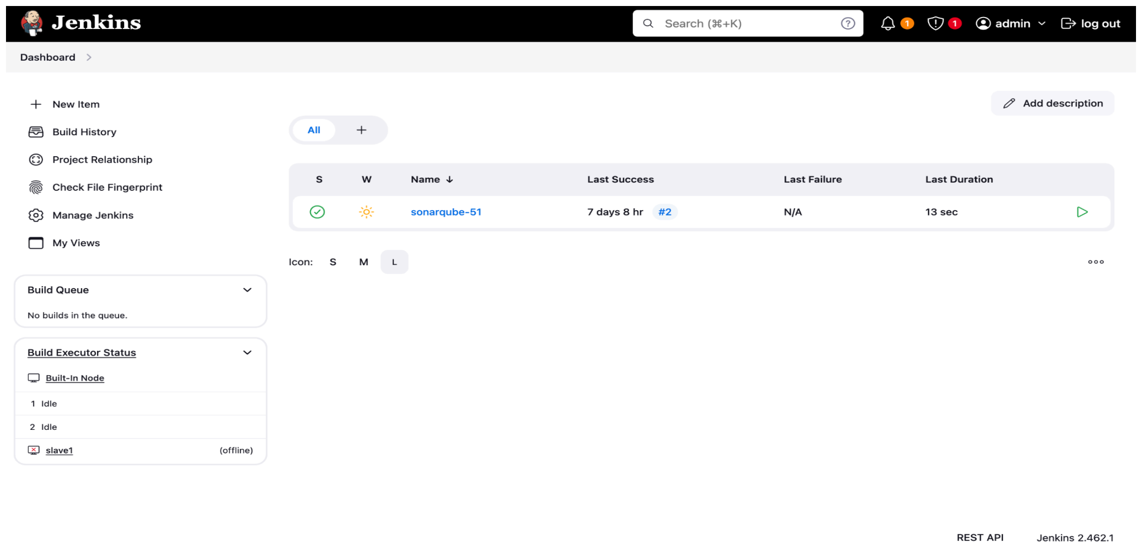
Recommended for projects following regular versions or releases.

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.


Jenkins Search (⌘+K) admin log out

Dashboard >

New Item
Build History
Project Relationship
Check File Fingerprint
Manage Jenkins
My Views

Add description

All +

S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	sonarqube-51	7 days 8 hr #2	N/A	13 sec

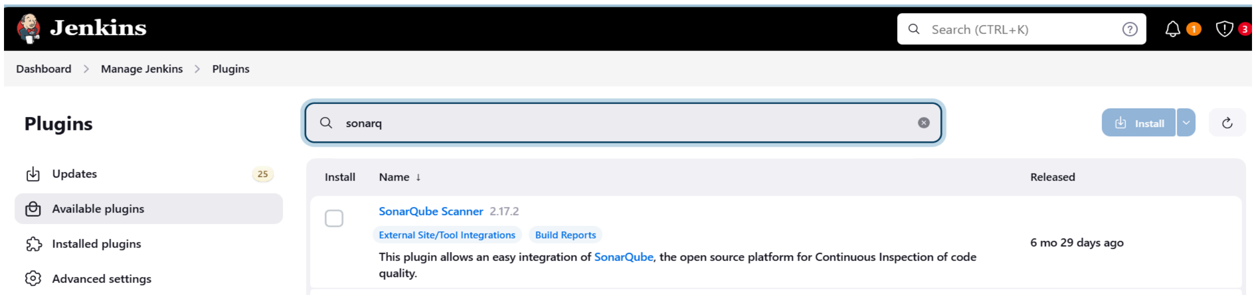
Icon: S M L

Build Queue
No builds in the queue.

Build Executor Status
Built-In Node
1 Idle
2 Idle
slave1 (offline)

REST API Jenkins 2.462.1

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



Jenkins

Search (CTRL+K)

Dashboard > Manage Jenkins > Plugins

Plugins

sonarq

Install

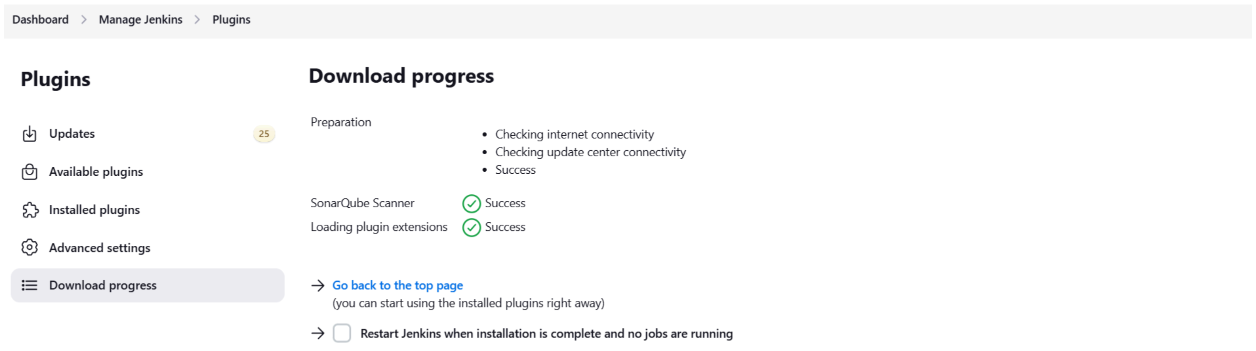
Updates 25

Available plugins

Installed plugins

Advanced settings

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



Dashboard > Manage Jenkins > Plugins

Plugins

Updates 25

Available plugins

Installed plugins

Advanced settings

Download progress

Download progress

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

SonarQube Scanner ✓ Success

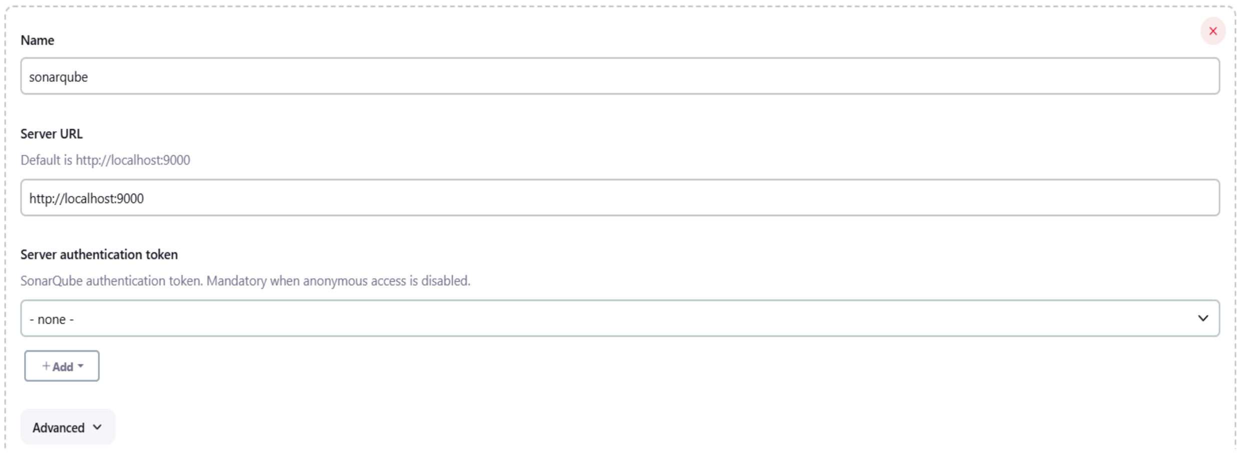
Loading plugin extensions ✓ Success

→ 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 **sonarqube**
In **Server URL** Default is **http://localhost:9000**



Name

sonarqube

Server URL

Default is http://localhost:9000

http://localhost:9000

Server authentication token

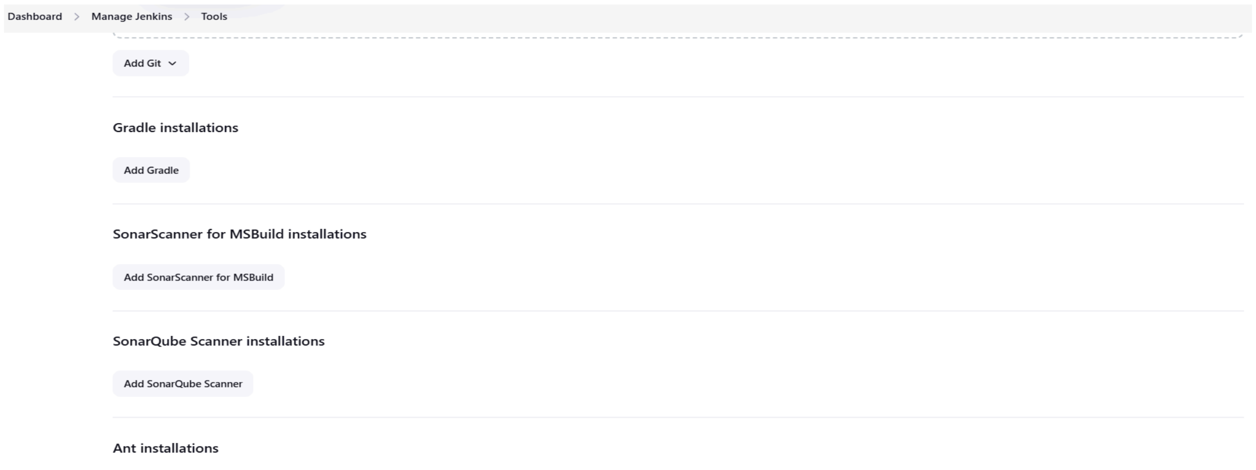
SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

+ Add

Advanced

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

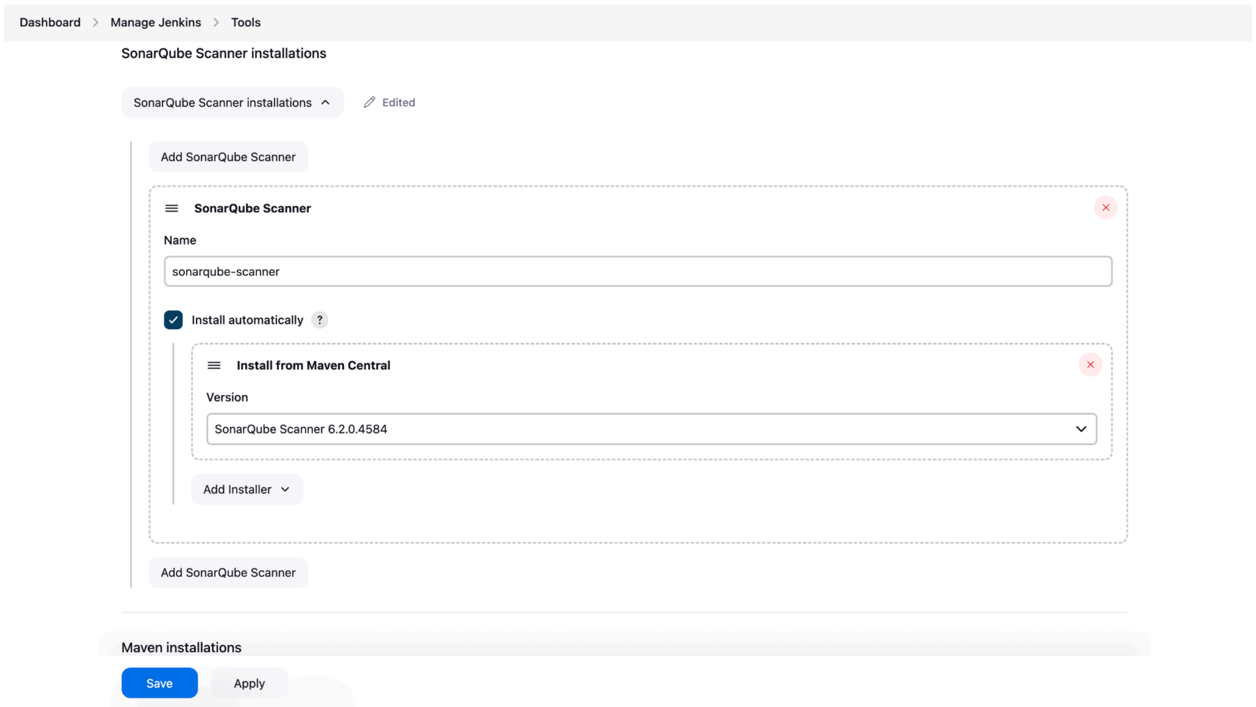
Add SonarScanner for MSBuild

SonarQube Scanner installations

Add SonarQube Scanner

Ant installations

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


Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations

SonarQube Scanner installations — Edited

Add SonarQube Scanner

SonarQube Scanner

Name: sonarqube-scanner

☑ Install automatically

Install from Maven Central

Version: SonarQube Scanner 6.2.0.4584

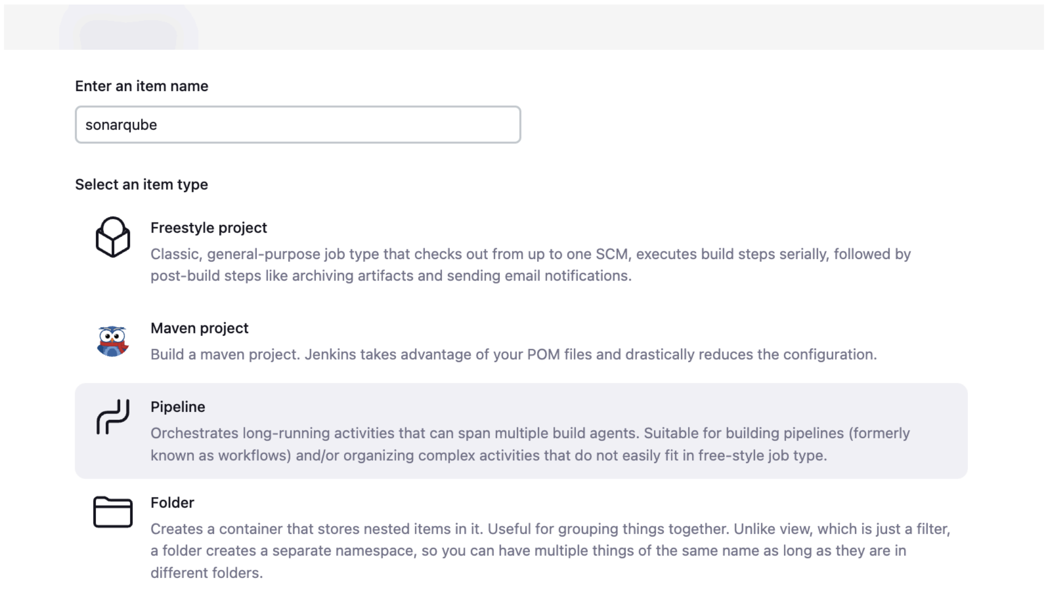
Add Installer

Add SonarQube Scanner

Maven installations

Save Apply

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


Enter an item name

sonarqube

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.

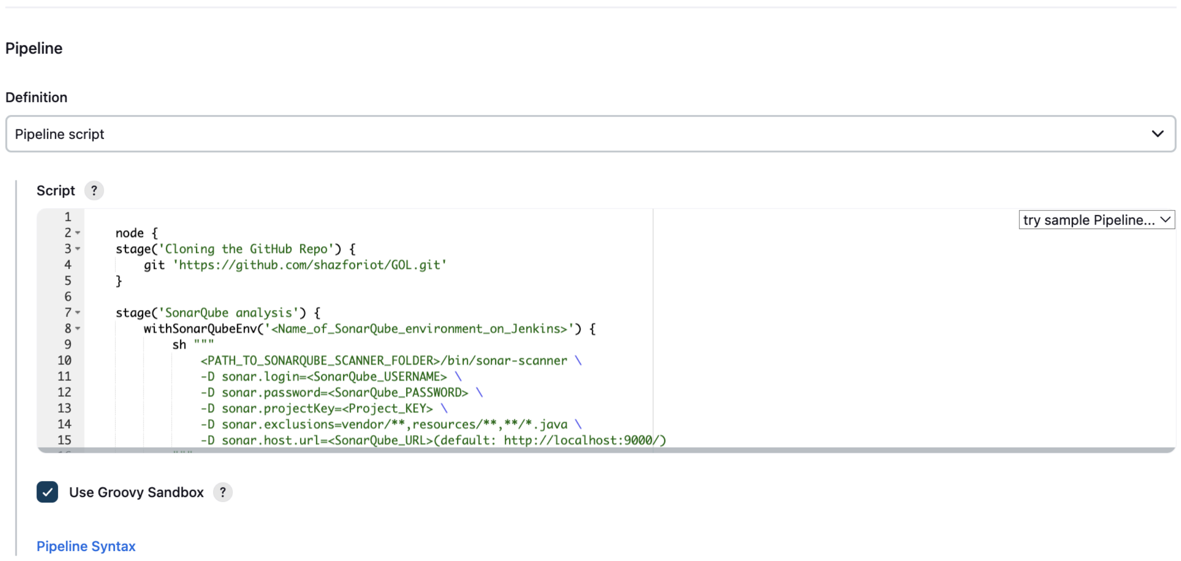
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

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_Jenkins>') {
      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.

Krushikesh Shelar 51. D15-C



Pipeline

Definition

Pipeline script

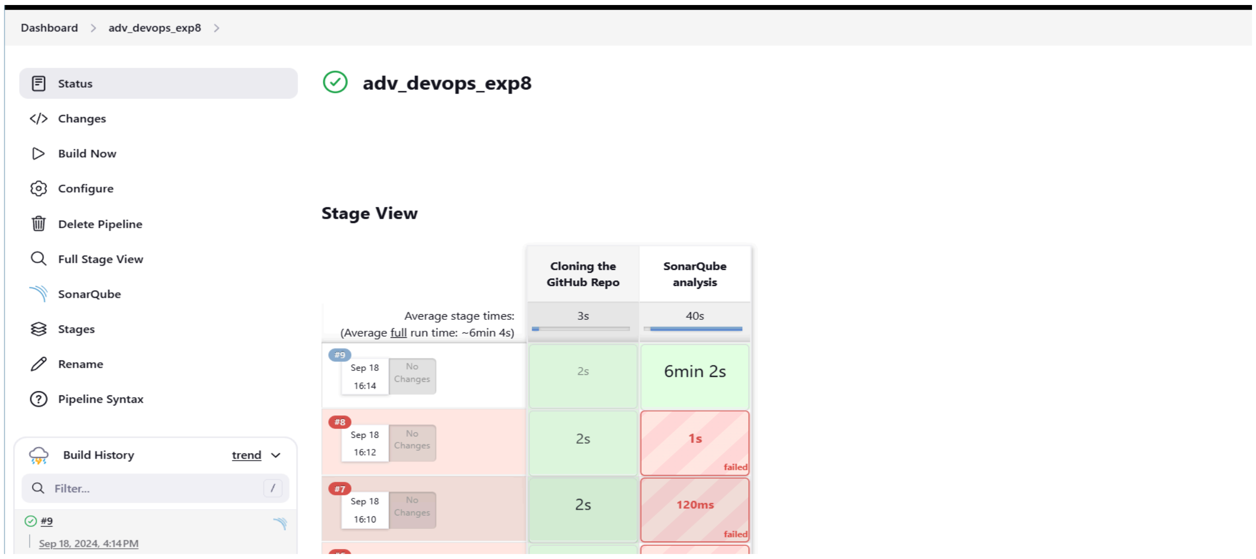
Script

```
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=<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/)
```

Use Groovy Sandbox: ✓

Pipeline Syntax

11. Build project



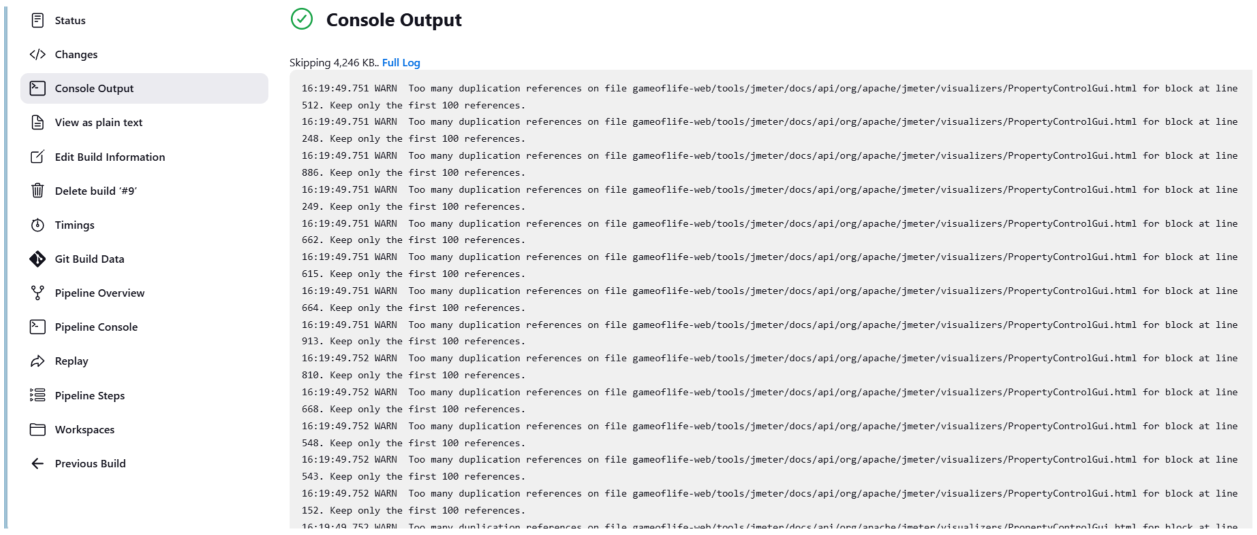
adv_devops_exp8

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

Krushikesh Shelar 51. D15-C

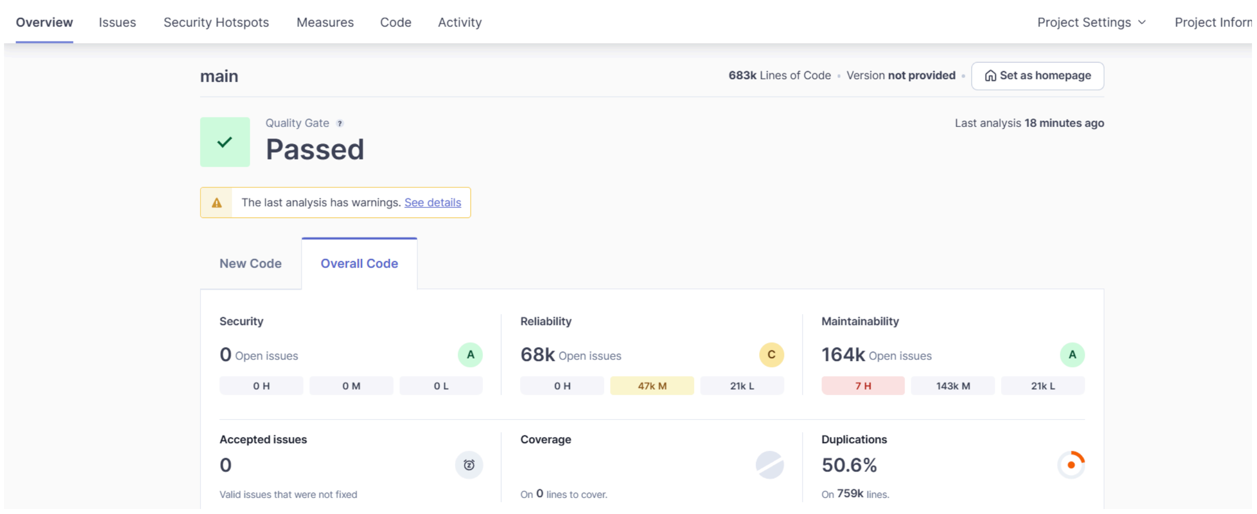

Status
Changes
Console Output
View as plain text
Edit Build Information
Delete build '#9'
Timings
Git Build Data
Pipeline Overview
Pipeline Console
Replay
Pipeline Steps
Workspaces
Previous Build

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.
```

13. Now, check the project in SonarQube



main — 683k Lines of Code • Version not provided • Set as homepage

Quality Gate
Passed
Last analysis 18 minutes ago

The last analysis has warnings. See details

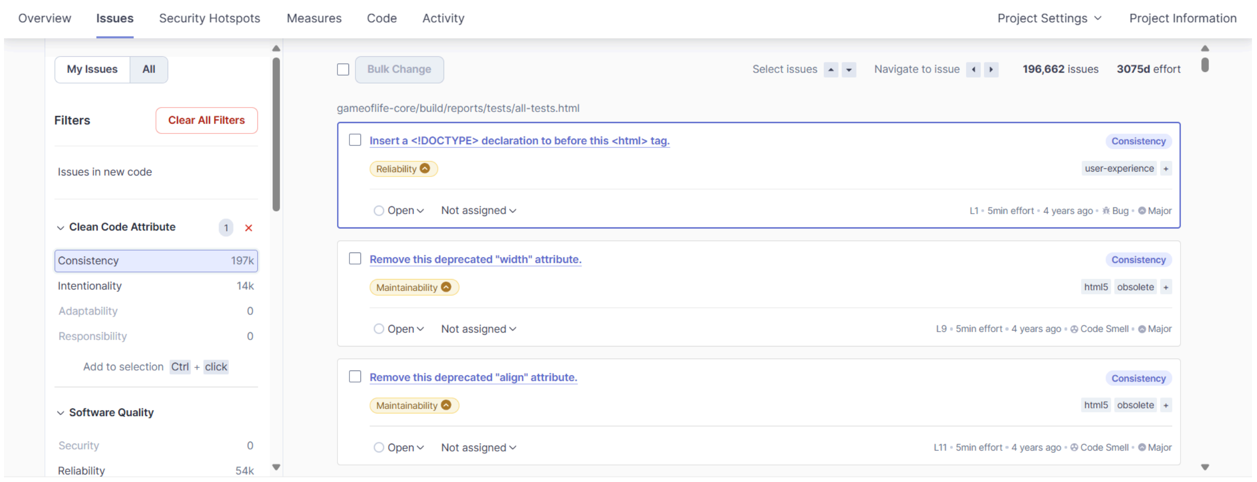
New Code | Overall Code

Security	Reliability	Maintainability
0 Open issues (A)	68k Open issues (C)	164k Open issues (A)
0 H, 0 M, 0 L	0 H, 47k M, 21k L	7 H, 143k M, 21k L

Accepted issues	Coverage	Duplications
0		50.6%
Valid issues that were not fixed	On 0 lines to cover.	On 759k lines.

14. Code Problems

- Consistency



Filters — Clear All Filters

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

196,662 issues 3075d effort

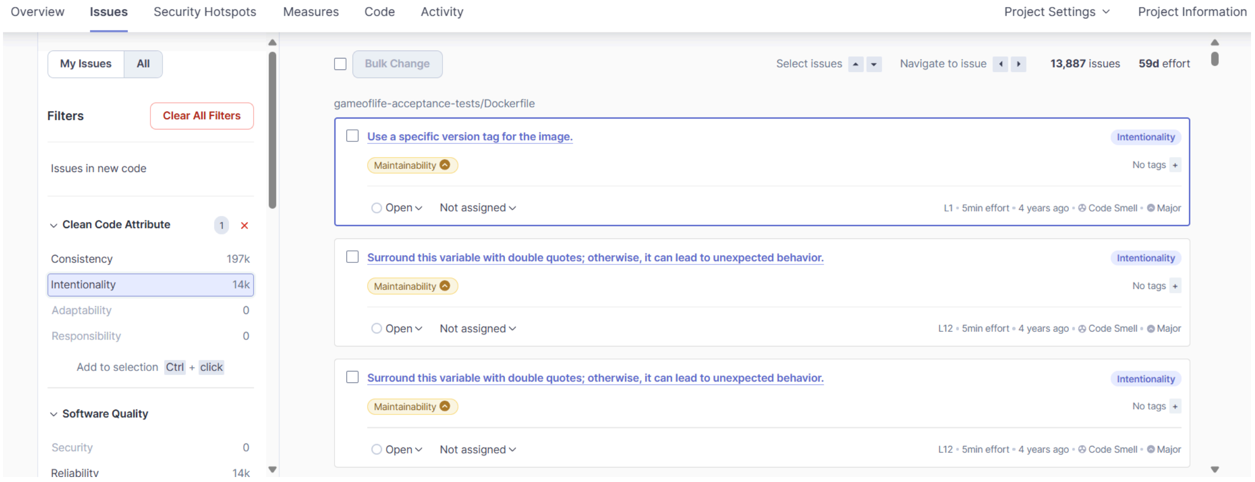
gameoflife-core/build/reports/tests/all-tests.html

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


Overview | Issues | Security Hotspots | Measures | Code | Activity | Project Settings | Project Information

My Issues | All

Filters — Clear All Filters

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

Bulk Change | Select issues | Navigate to issue | 13,887 issues | 59d effort

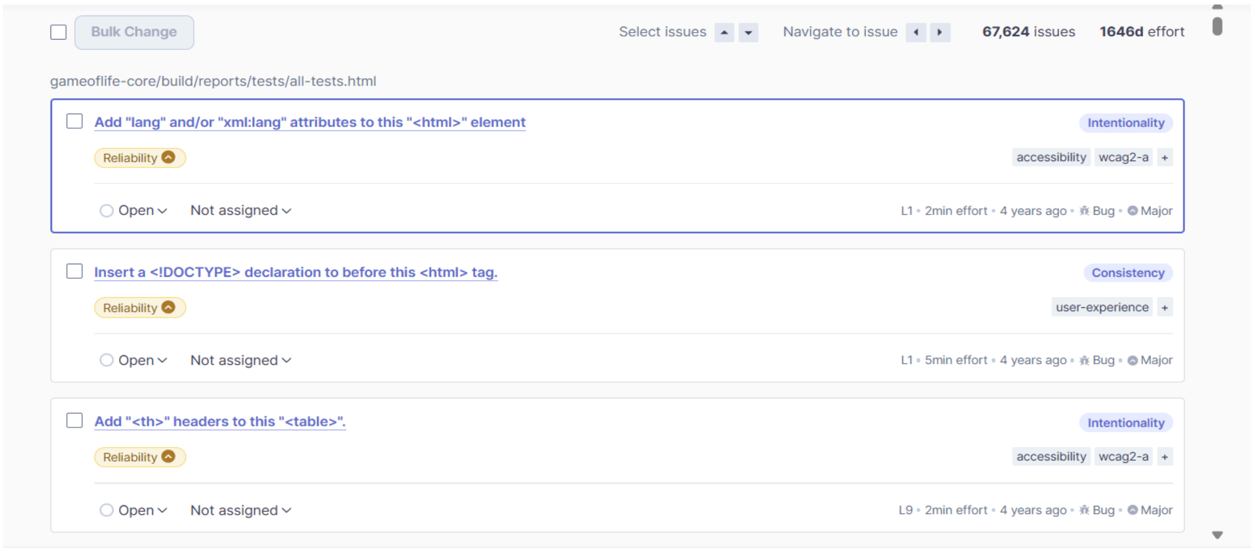
gameoflife-acceptance-tests/Dockerfile

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

- Bugs


Bulk Change | Select issues | Navigate to issue | 67,624 issues | 1646d effort

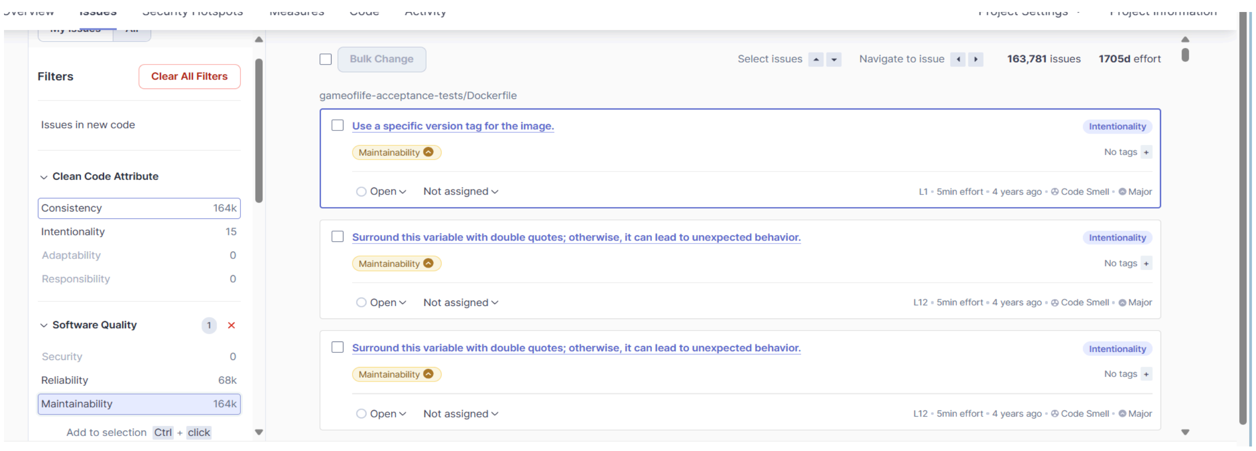
gameoflife-core/build/reports/tests/all-tests.html

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


Overview | Issues | Security Hotspots | Measures | Code | Activity | Project Settings | Project Information

Filters — Clear All Filters

Issues in new code

Clean Code Attribute

Consistency	164k
Intentionality	15
Adaptability	0
Responsibility	0

Software Quality 1

Security	0
Reliability	68k
Maintainability	164k

Add to selection Ctrl + click

Bulk Change | Select issues | Navigate to issue | 163,781 issues | 1705d effort

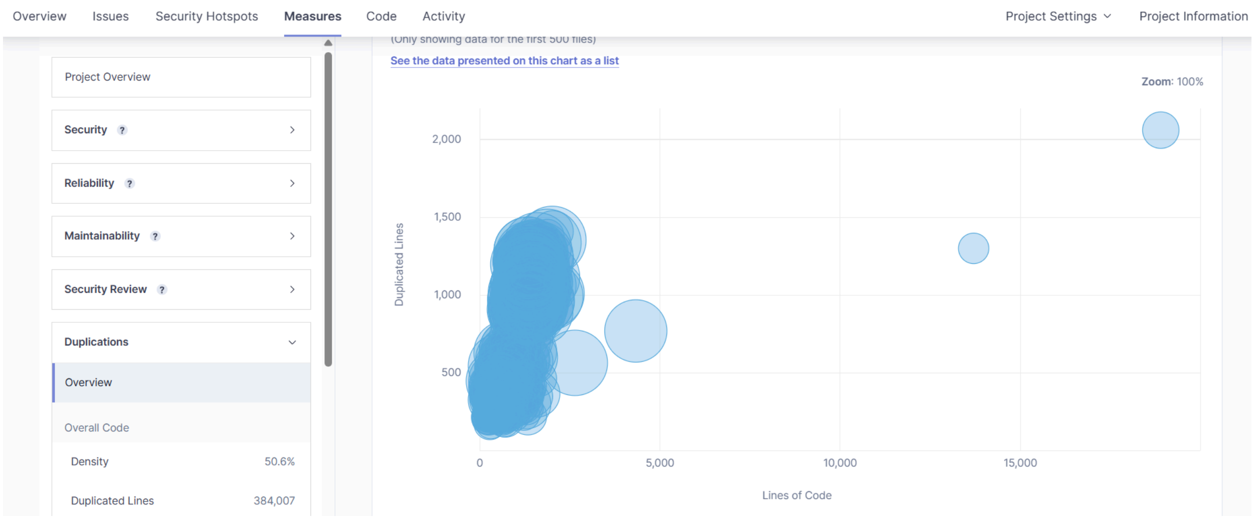
gameoflife-acceptance-tests/Dockerfile

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

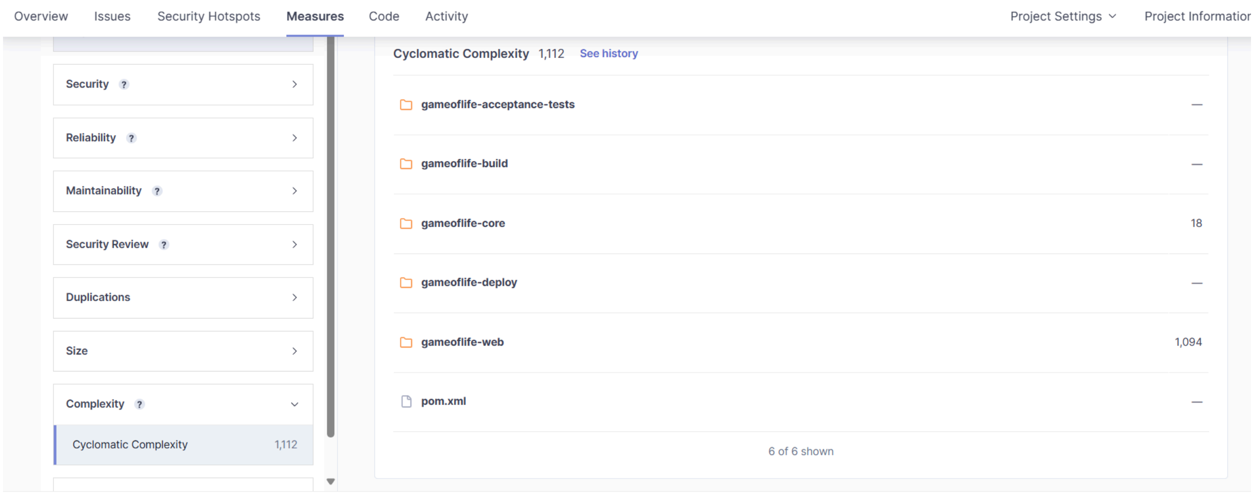
Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags — Open — Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major

- Duplications



Density	50.6%
Duplicated Lines	384,007

- Cyclomatic Complexities



Cyclomatic Complexity 1,112

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.

Conclusion:

In this experiment, we integrated Jenkins with SonarQube to automate code quality checks in our CI/CD pipeline. We deployed SonarQube using Docker, set up a project for analysis, and configured Jenkins with the SonarQube Scanner plugin. We then created a Jenkins pipeline to clone a GitHub repository and run SonarQube analysis on the code. This integration ensures continuous monitoring of code quality, helping to identify bugs, code smells, and security vulnerabilities throughout the development process.