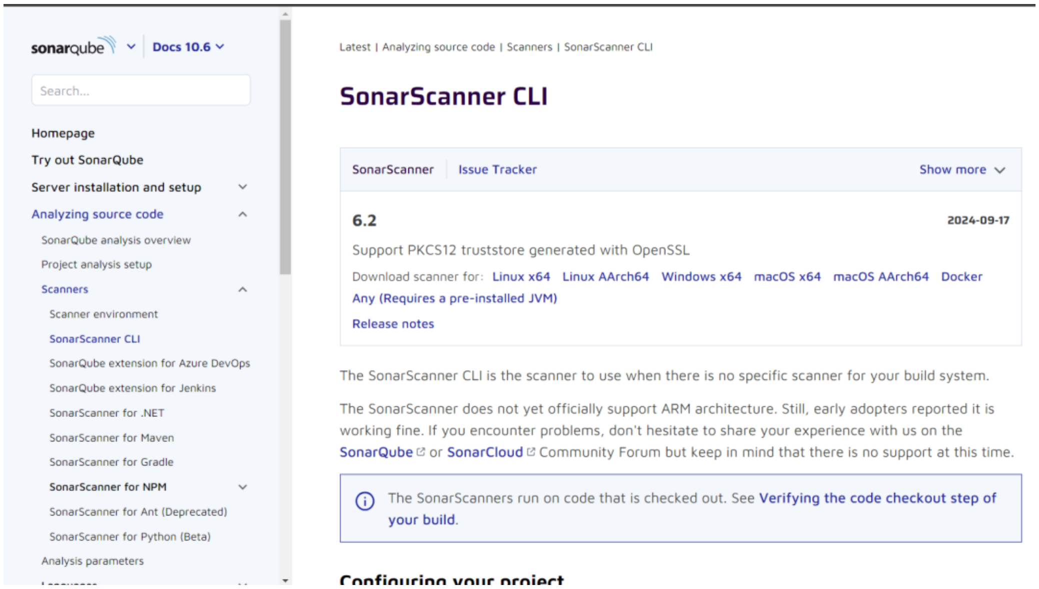
08 Advanced DevOps Lab

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: Download sonar scanner

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



SonarScanner CLI

6.2 2024-09-17

Support PKCS12 truststore generated with OpenSSL

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

Release notes

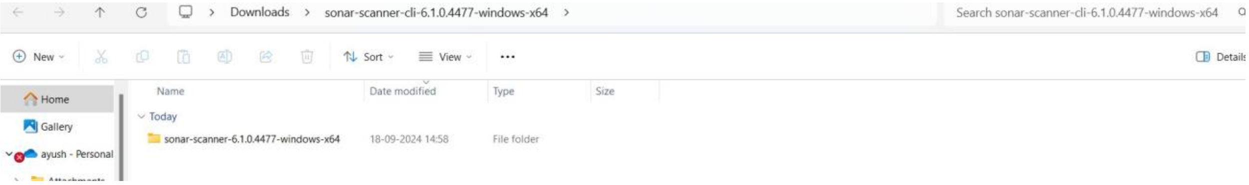
The SonarScanner CLI is the scanner to use when there is no specific scanner for your build system.

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.

The SonarScanners run on code that is checked out. See Verifying the code checkout step of your build.

Configuring your project

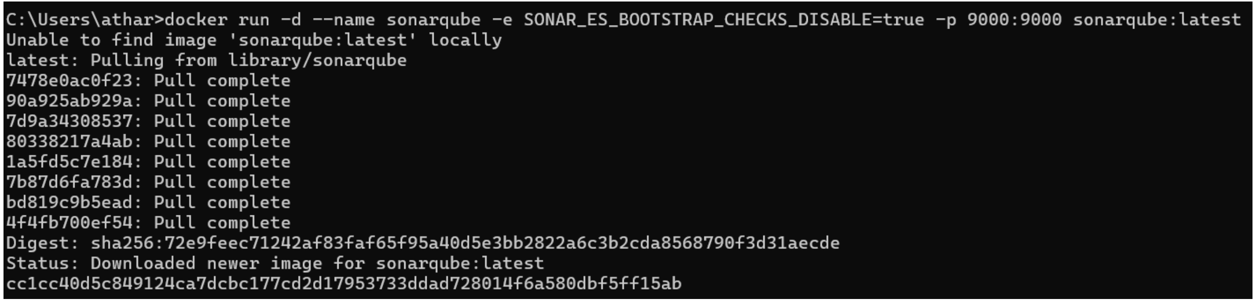
Extract the downloaded zip file in a folder.


Downloads
sonar-scanner-cli-6.1.0.4477-windows-x64
Search sonar-scanner-cli-6.1.0.4477-windows-x64
New
Sort
View
Details
Home
Gallery
ayush - Personal
Name
Date modified
Type
Size
Today

sonar-scanner-6.1.0.4477-windows-x64 18-09-2024 14:58 File folder

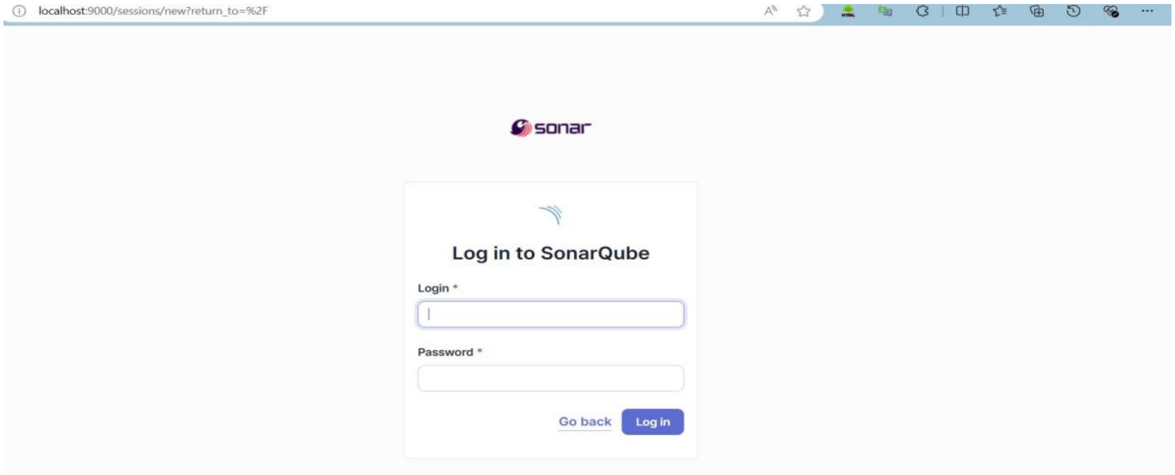
1. Install sonarqube image

Command: **docker pull sonarqube**



```
C:\Users\athar>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
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
cc1cc40d5c849124ca7dcbc177cd2d17953733ddad728014f6a580dbf5ff15ab
```

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



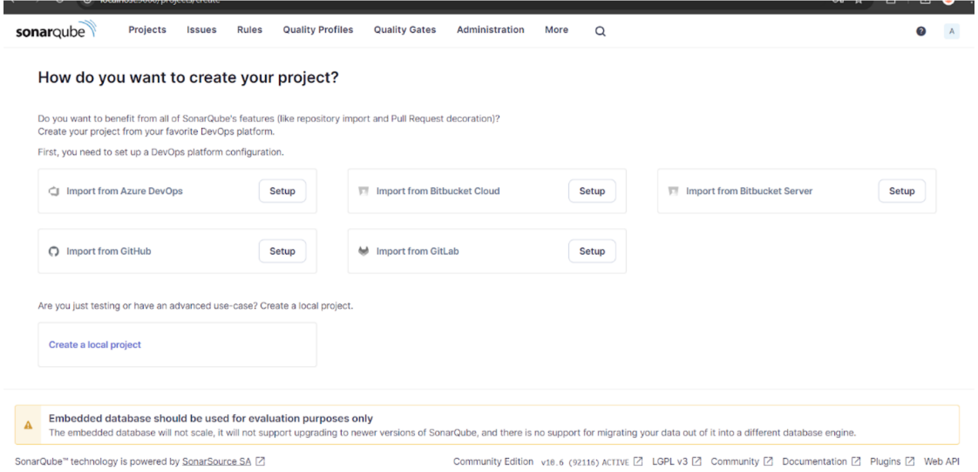
localhost:9000/sessions/new?return_to=%2F

Log in to SonarQube

Login *

Password *

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.

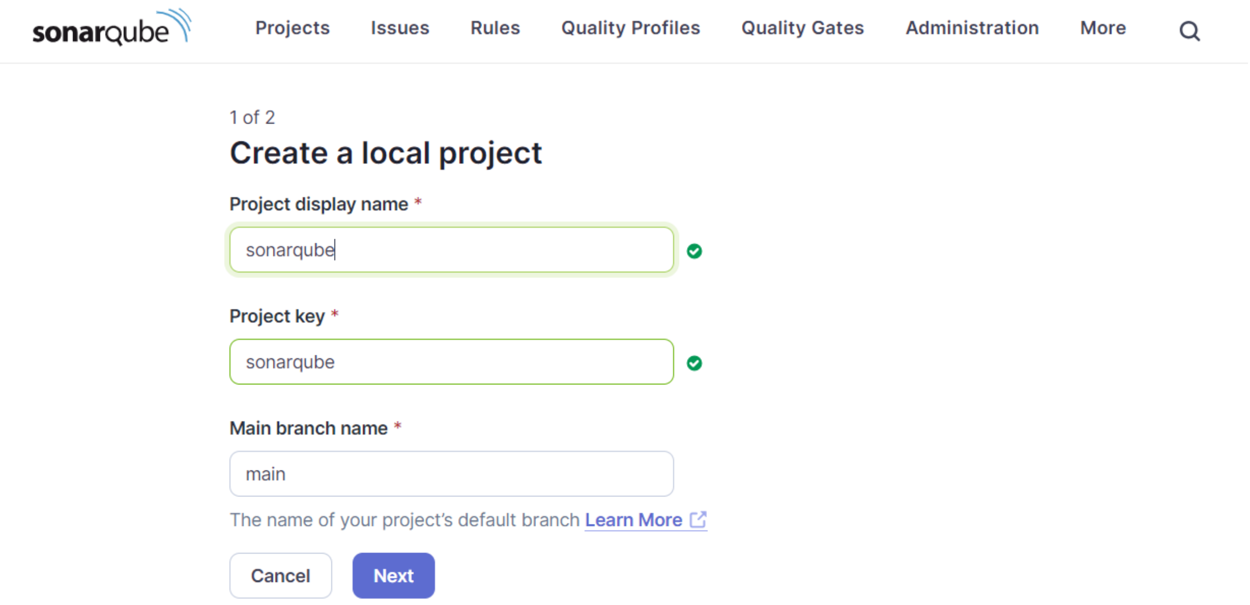
First, you need to set up a DevOps platform configuration.

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

Embedded database should be used for evaluation purposes only
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA Community Edition v10.6 (92116) ACTIVE LGPL v3 Community Documentation Plugins Web API

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



1 of 2

Create a local project

Project display name *

sonarqube

Project key *

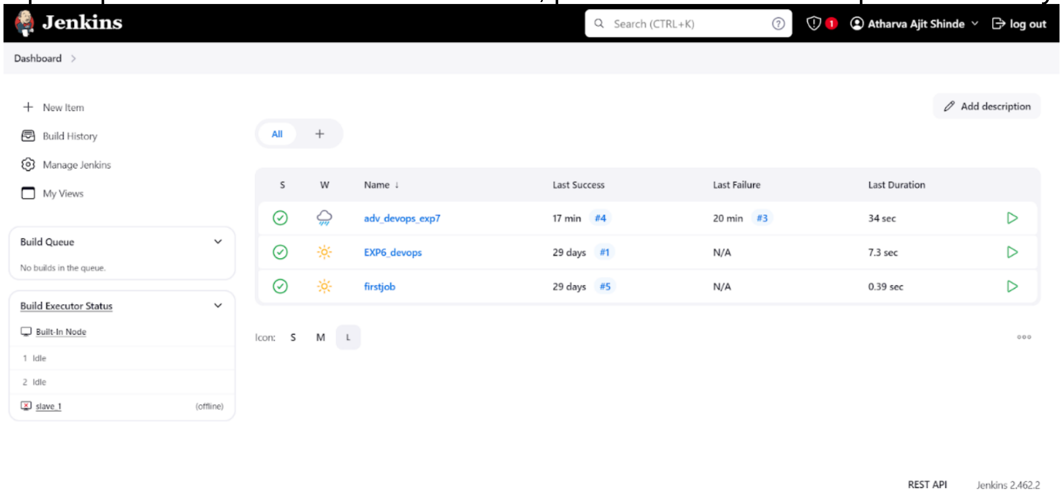
sonarqube

Main branch name *

main

The name of your project’s default branch Learn More

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



Build Queue

No builds in the queue.

Build Executor Status

Built-In Node

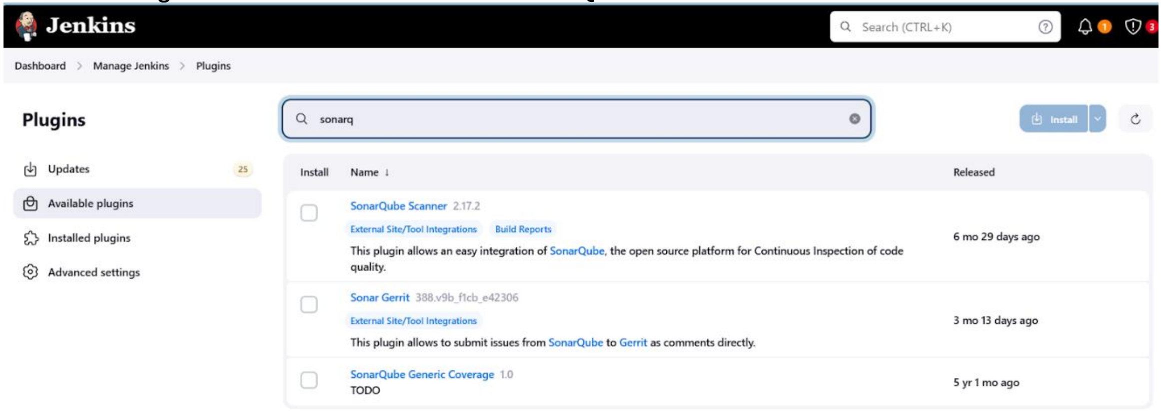
1 Idle

2 Idle

slave_1 (offline)

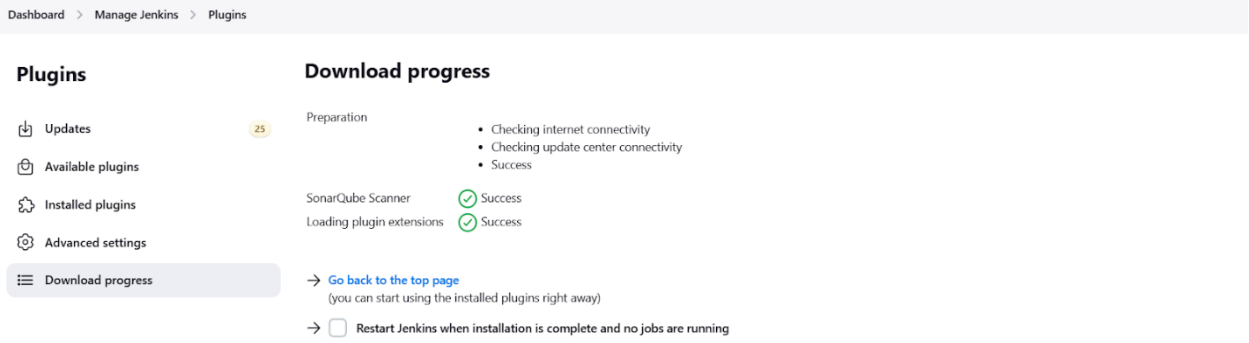
S	W	Name ↓	Last Success	Last Failure	Last Duration
✓		adv_devops_exp7	17 min #4	20 min #3	34 sec
✓	☀	EXP6_devops	29 days #1	N/A	7.3 sec
✓	☀	firstjob	29 days #5	N/A	0.39 sec

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



sonarq

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
□	Sonar Gerrit 388.v9b_f1cb_e42306 External Site/Tool Integrations This plugin allows to submit issues from SonarQube to Gerrit as comments directly.	3 mo 13 days ago
□	SonarQube Generic Coverage 1.0 TODO	5 yr 1 mo ago



Download progress

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

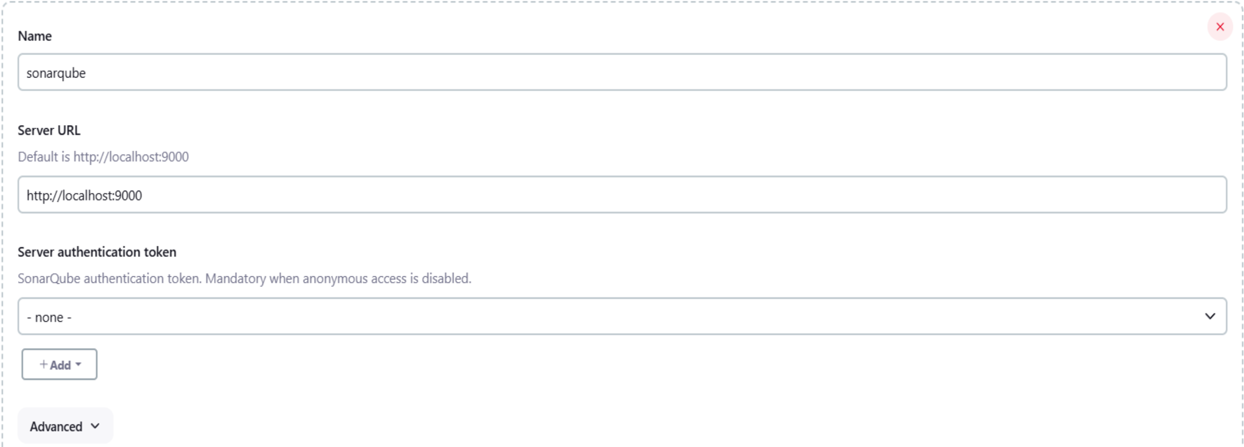
SonarQube Scanner ✓ Success
Loading plugin extensions ✓ Success

→ 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

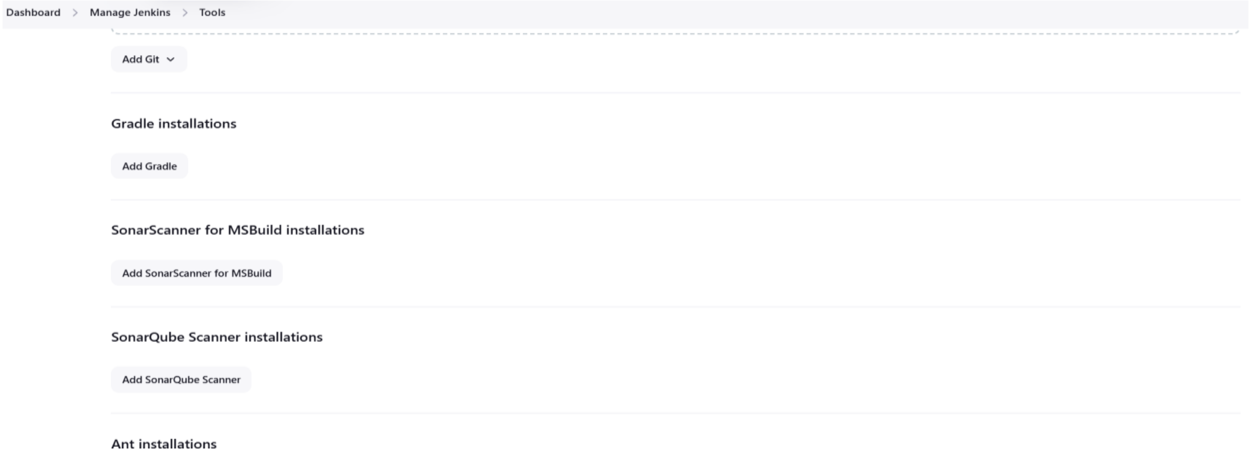
Server authentication token

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

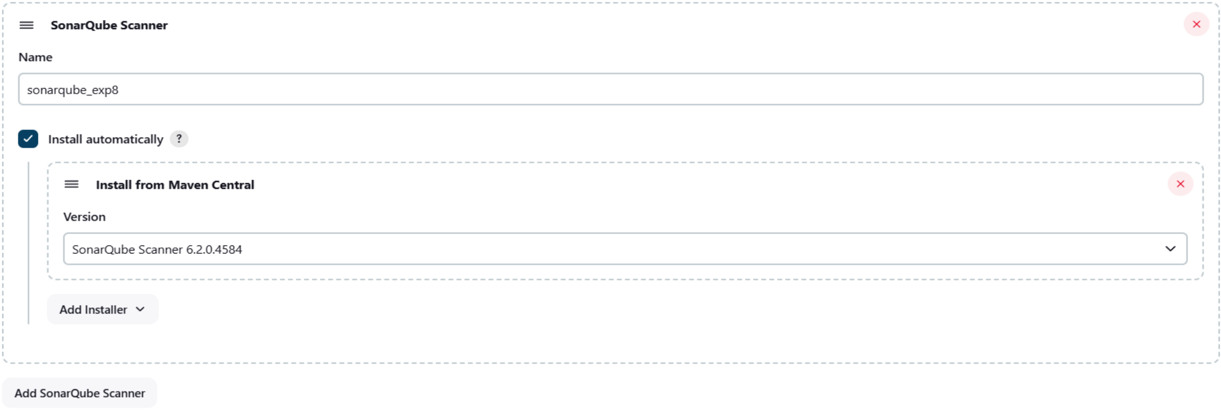
SonarScanner for MSBuild installations

Add SonarScanner for MSBuild

SonarQube Scanner installations

Ant installations

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



SonarQube Scanner

Name

sonarqube_exp8

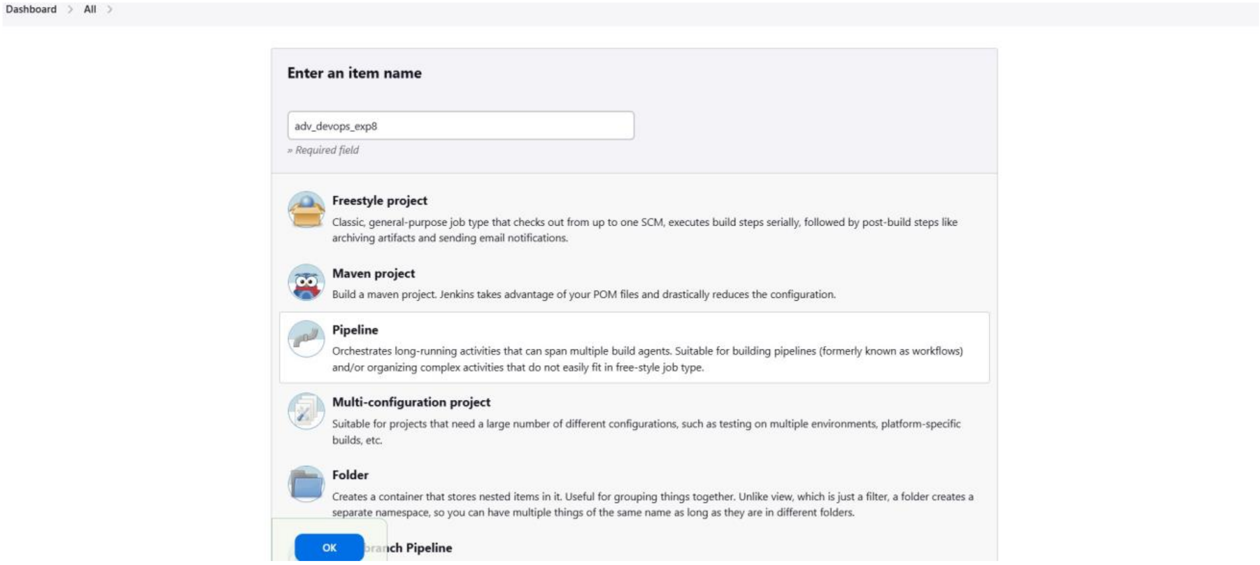
☑ Install automatically ?

Install from Maven Central

Version

SonarQube Scanner 6.2.0.4584

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



Enter an item name

adv_devops_exp8

» Required field

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.

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.

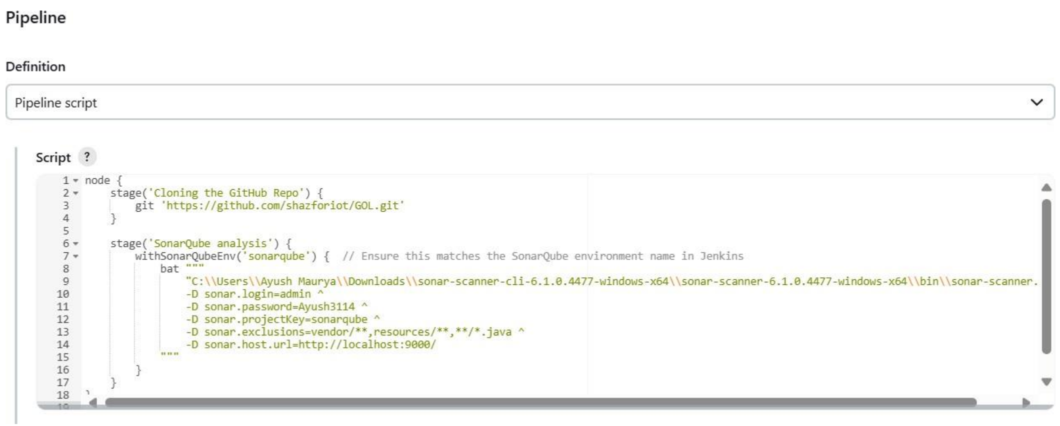
ranch Pipeline

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/)
            """
        }
    }
}
```

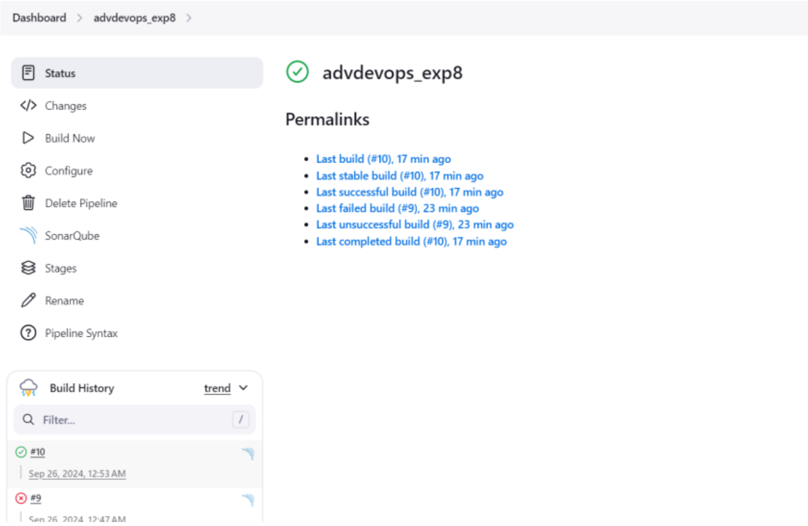
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.



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

    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {  // Ensure this matches the SonarQube environment name in Jenkins
            bat """
                "C:\\Users\\Ayush Maurya\\Downloads\\sonar-scanner-cli-6.1.0.4477-windows-x64\\sonar-scanner-6.1.0.4477-windows-x64\\bin\\sonar-scanner.
                -D sonar.login=admin ^
                -D sonar.password=Ayush3114 ^
                -D sonar.projectKey=sonarqube ^
                -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
                -D sonar.host.url=http://localhost:9000/
            """
        }
    }
}
```

11. Build project



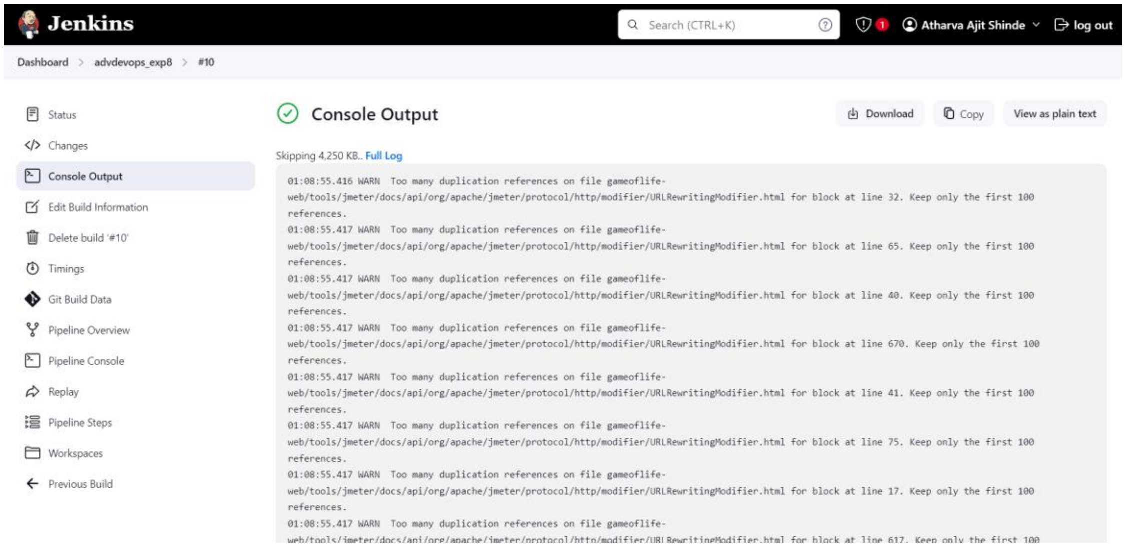
advdevops_exp8

Permalinks

- Last build (#10), 17 min ago
- Last stable build (#10), 17 min ago
- Last successful build (#10), 17 min ago
- Last failed build (#9), 23 min ago
- Last unsuccessful build (#9), 23 min ago
- Last completed build (#10), 17 min ago

#10
Sep 26, 2024, 12:53 AM
#9
Sep 26, 2024, 12:47 AM

12. Check console

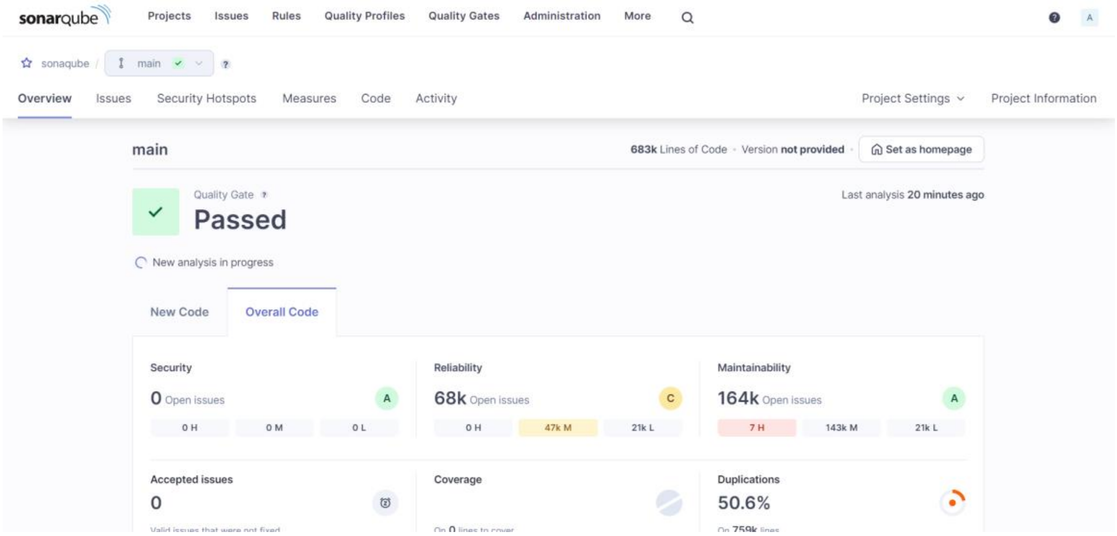


Console Output

Skipping 4,250 KB.. Full Log

```
01:08:55.416 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 32. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 65. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 40. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 670. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 41. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 75. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 17. Keep only the first 100
references.
01:08:55.417 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/modifier/URLRewritingModifier.html for block at line 617. Keep only the first 100
```

13. Now, check the project in SonarQube



main

683k Lines of Code · Version not provided

Quality Gate

Passed

Last analysis 20 minutes ago

New analysis in progress

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

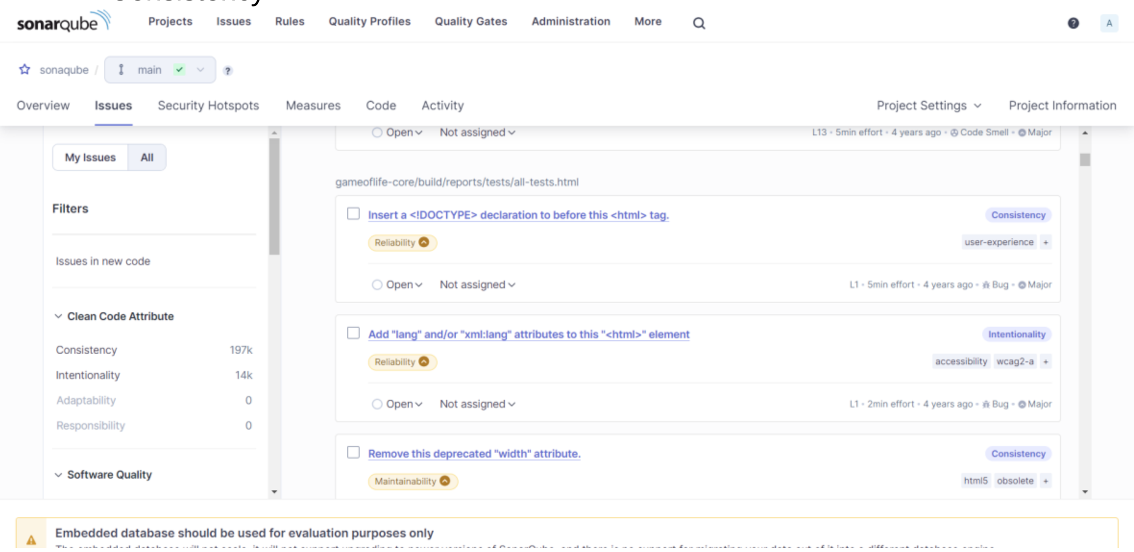
Accepted issues: 0 — Valid issues that were not fixed

Coverage — On 0 lines to cover

Duplications: 50.6% — On 759k lines

14. Code Problems

- Consistency



Clean Code Attribute	
Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

○ Open ⌄ Not assigned ⌄ — L13 · 5min effort · 4 years ago · Code Smell · Major

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

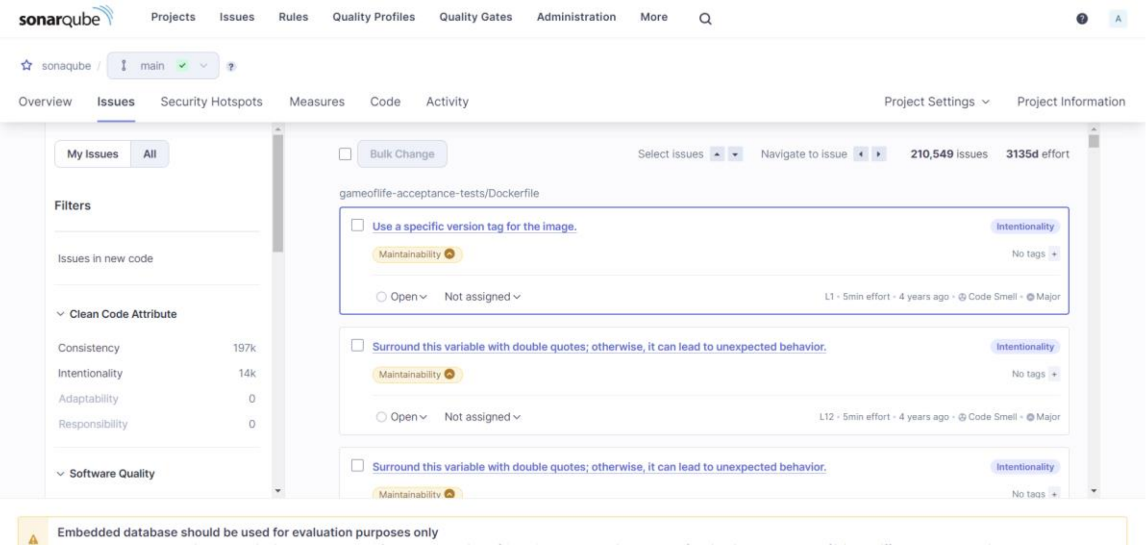
□ Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency
Reliability — user-experience +
○ Open ⌄ Not assigned ⌄ — L1 · 5min effort · 4 years ago · Bug · Major

□ 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

□ Remove this deprecated "width" attribute. — Consistency
Maintainability — html5 obsolete +

Embedded database should be used for evaluation purposes only

- Intentionality



Clean Code Attribute	
Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

210,549 issues 3135d effort

gameoflife-acceptance-tests/Dockerfile

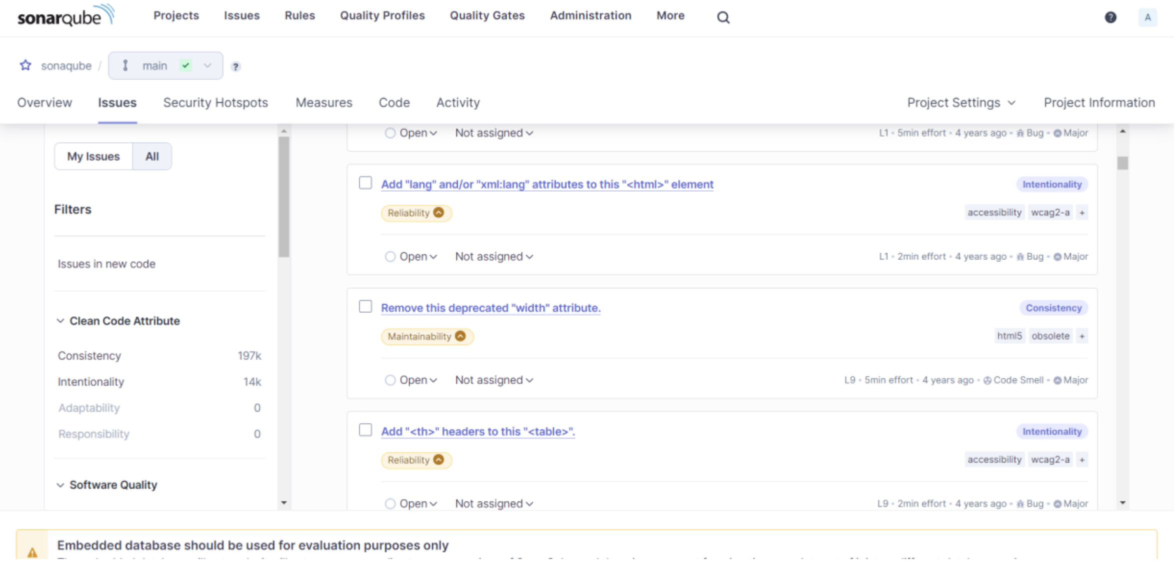
□ Use a specific version tag for the image. — Intentionality
Maintainability — No tags +
○ Open ⌄ Not assigned ⌄ — L1 · 5min effort · 4 years ago · Code Smell · Major

□ 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 +

Embedded database should be used for evaluation purposes only

- Bugs



sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

sonaqube / main ✓

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

My Issues | All

Filters

Issues in new code

Clean Code Attribute

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Software Quality

○ Open Not assigned L1 · 5min effort · 4 years ago · Bug · Major

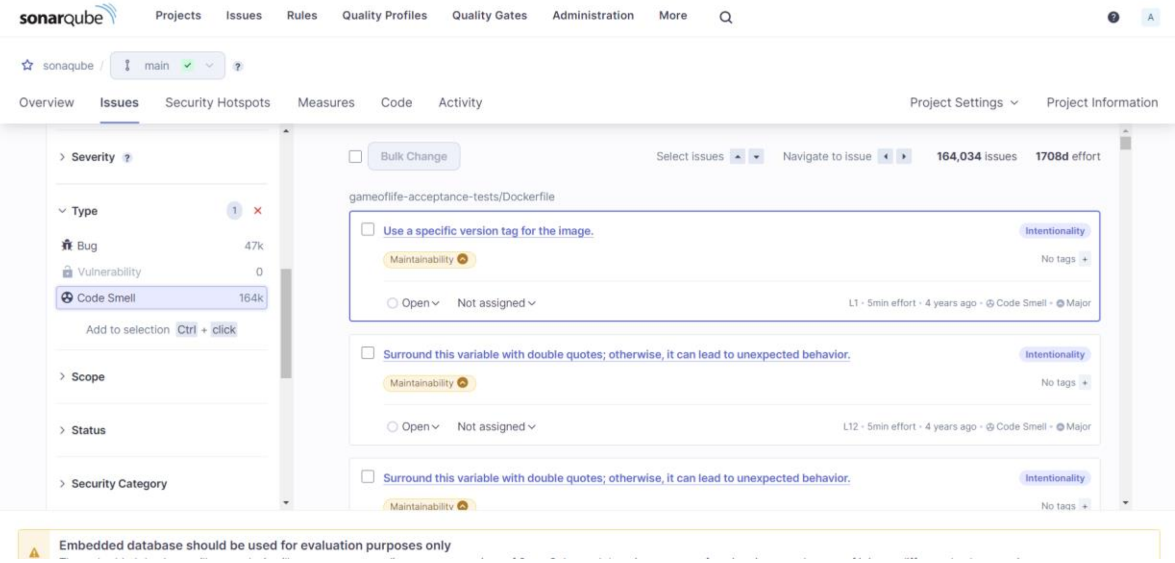
☐ Add "lang" and/or "xml:lang" attributes to this "<html>" element Intentionality
Reliability accessibility wcag2-a +
○ Open Not assigned L1 · 2min effort · 4 years ago · Bug · Major

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

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

Embedded database should be used for evaluation purposes only

- Code Smells



sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

sonaqube / main ✓

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

Severity

Type 1 ✕

Bug	47k
Vulnerability	0
Code Smell	164k

Add to selection Ctrl + click

Scope

Status

Security Category

☐ Bulk Change Select issues Navigate to issue **164,034** issues **1708d** effort

gameoflife-acceptance-tests/Dockerfile

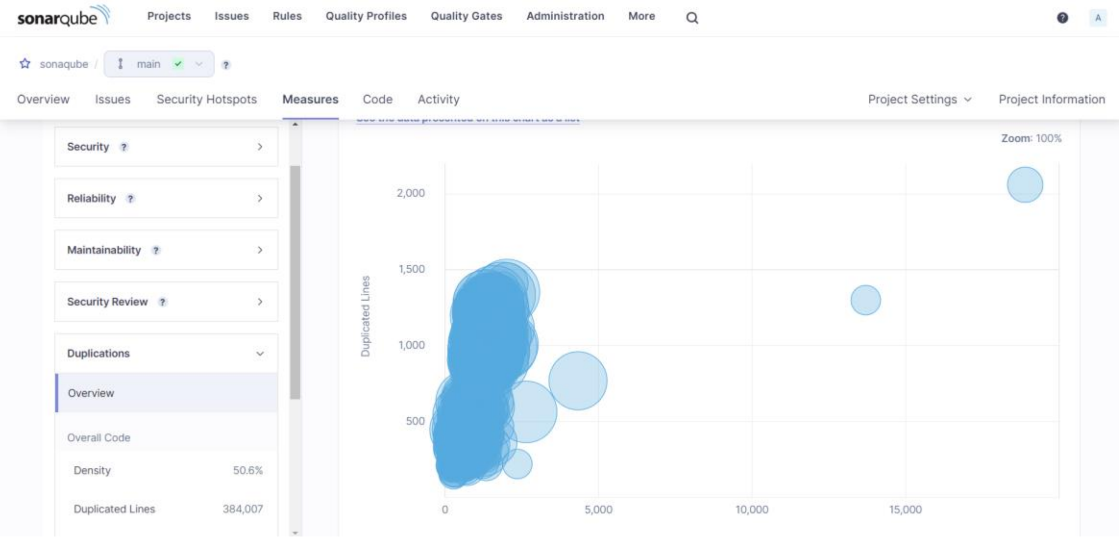
☐ Use a specific version tag for the image. Intentionality
Maintainability No tags +
○ Open Not assigned L1 · 5min effort · 4 years ago · Code Smell · Major

☐ 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 +

Embedded database should be used for evaluation purposes only

- Duplications



sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

sonaqube / main ✓

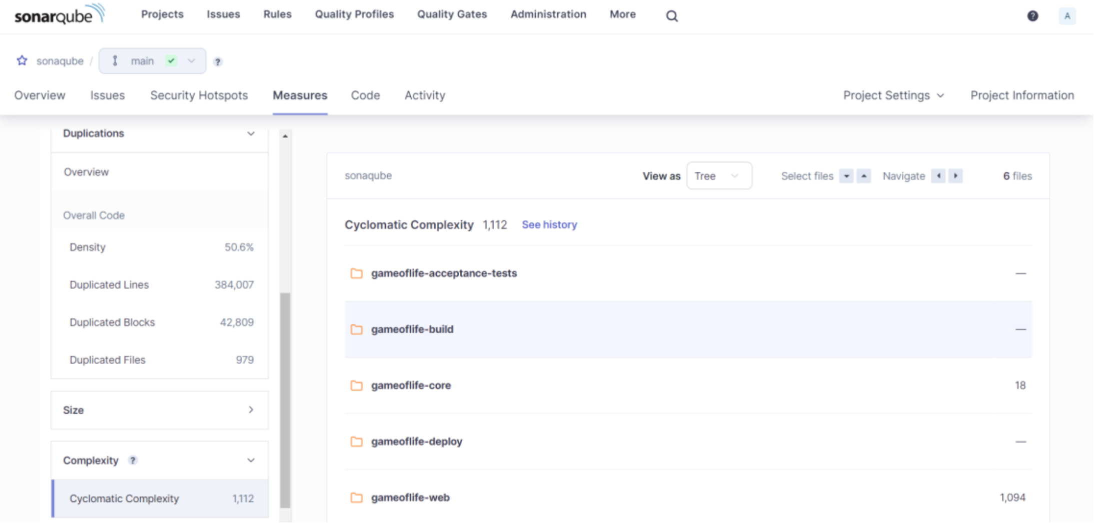
Overview Issues Security Hotspots **Measures** Code Activity Project Settings Project Information

Security
Reliability
Maintainability
Security Review
Duplications
Overview

Overall Code

Density	50.6%
Duplicated Lines	384,007

- Cyclomatic Complexities



Duplications

Overview

Overall Code

Density	50.6%
Duplicated Lines	384,007
Duplicated Blocks	42,809
Duplicated Files	979

Size

Complexity

Cyclomatic Complexity	1,112

sonaqube — 6 files

Cyclomatic Complexity 1,112

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

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

Conclusion:

In this experiment, we integrated Jenkins with SonarQube to enable automated code quality checks within our CI/CD pipeline. We started by deploying SonarQube using Docker, setting up a project, and configuring it to analyze code quality. Next, we configured Jenkins by installing the SonarQube Scanner plugin, adding SonarQube server details, and setting up the scanner tool. We then developed a Jenkins pipeline to automate the process of cloning a GitHub repository and running SonarQube analysis on the code. This integration helps ensure continuous monitoring of code quality, detecting issues such as bugs, code smells, and security vulnerabilities throughout the development process.