

Experiment No: 8

AIM: Create a Jenkins CI/CD 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.

PREREQUISITES:

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

The screenshot shows the SonarScanner CLI documentation page. The left sidebar contains a navigation menu with links to 'Homepage', 'Try out SonarQube', 'Server installation and setup', 'Analyzing source code', 'Scanners', 'Scanner environment', 'SonarScanner CLI', 'SonarQube extension for Azure DevOps', 'SonarQube extension for Jenkins', 'SonarScanner for .NET', 'SonarScanner for Maven', 'SonarScanner for Gradle', 'SonarScanner for NPM', 'SonarScanner for Ant (Deprecated)', and 'SonarScanner for Python (Beta)'. The main content area is titled 'SonarScanner CLI' and shows the version '6.1' with a release date of '2024-06-27'. It lists download links for 'Linux x64', 'Linux AArch64', 'Windows x64', 'macOS x64', 'macOS AArch64', and 'Docker'. A note states 'Any (Requires a pre-installed JVM)'. Below this, it says 'Release notes'. A paragraph explains that the SonarScanner CLI is the scanner to use when there is no specific scanner for your build system. It also mentions that the SonarScanner does not yet officially support ARM architecture. A warning box at the bottom states: 'The SonarScanners run on code that is checked out. See Verifying the code checkout step of your build.'

Step 2: Docker Run docker -v command .If docker is not installed so install it

```
C:\Users\Sandesh>docker -v
Docker version 27.2.0, build 3ab4256
```

Step 3: Install sonarqube image Command: docker pull sonarqube

```
C:\Users\Student>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
762bedf4b1b7: Pull complete
95f9bd9906fa: Pull complete
a32d681e6b99: Pull complete
aabdd0a18314: Pull complete
5161e45ecd8d: Pull complete
aeb0020dfa06: Pull complete
01548d361aea: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:bb444c58c1e04d8a147a3bb12af941c57e0100a5b21d10e599384d59b
Status: Downloaded newer image for sonarqube:latest
docker.io/library/sonarqube:latest

What's next:
  View a summary of image vulnerabilities and recommendations → docker
```

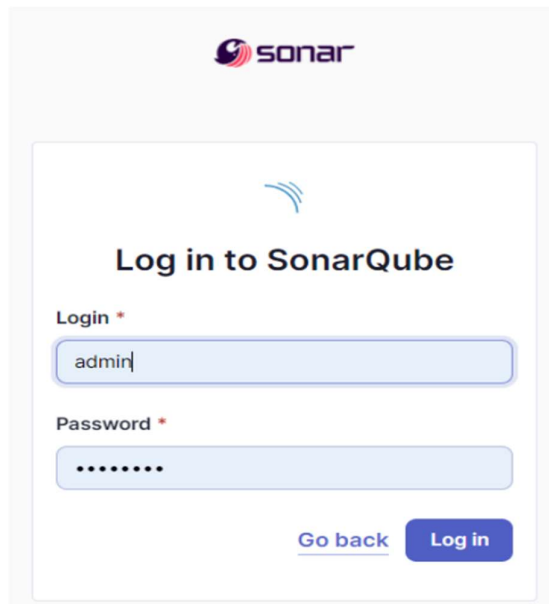
Step 4: Keep Jenkins installed on your system.

EXPERIMENT STEPS:

Step1: Run SonarQube image `docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest`. This command will run the SonarQube image that was just installed using docker.

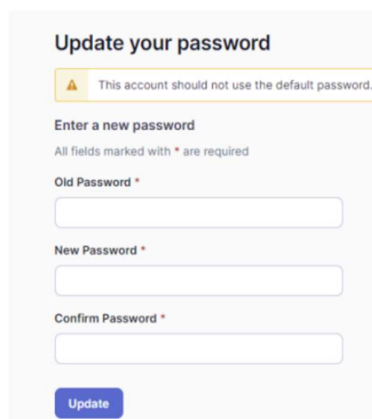
```
C:\Users\Student>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
83330c33cd961d8d659f362c5f62c6cd1ff87f31ec99da134350b9b419370561
```

Step 2: Once the SonarQube image is started, you can go to <http://localhost:9000> to find the SonarQube that has started



The image shows the SonarQube login interface. At the top, there is the Sonar logo. Below it, the text "Log in to SonarQube" is displayed. There are two input fields: "Login *" with the text "admin" entered, and "Password *" with masked characters ".....". At the bottom right, there are two buttons: "Go back" (a link) and "Log in" (a blue button).

Step 3: On this interface, login with username = 'admin' and password = 'admin'. Once logged in successfully, SonarQube will ask you to reset this password. Reset it and remember this password.



The image shows the "Update your password" form. At the top, there is a warning message: "This account should not use the default password." Below this, the text "Enter a new password" is displayed, followed by the note "All fields marked with * are required". There are three input fields: "Old Password *" (empty), "New Password *" (empty), and "Confirm Password *" (empty). At the bottom left, there is a blue "Update" button.

Step 4: After changing the password, you will be directed to this screen. Click on Create a Local Project. Give the project a display name and project key

Click on Create Project

1 of 2

Create a local project

Project display name *



Project key *



Main branch name *

The name of your project's default branch [Learn More](#)CancelNext

Set up the project as required and click on create.

In the Step 2 while creating the project, Sonarqube ask you regarding which code should be considered as the new code for examining it .

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMoreQ

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 attention on the most recent changes to your project, enabling you to follow the Clean as 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.

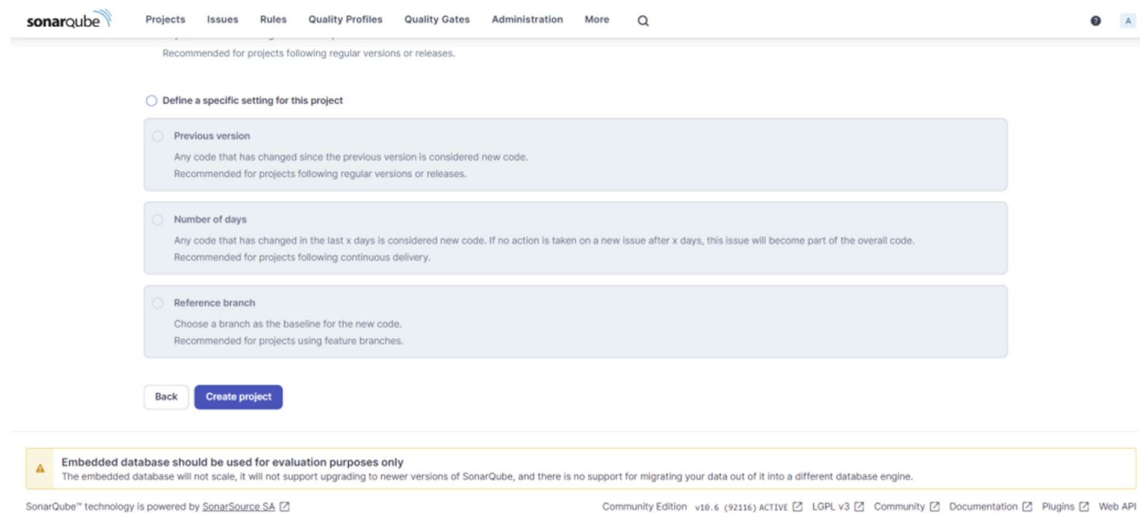
Recommended for projects following regular versions or releases.

☐ Number of days

Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.

Recommended for projects following continuous delivery.

☐ Reference branch



SonarQube

Projects Issues Rules Quality Profiles Quality Gates Administration More Q

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.
Recommended for projects following regular versions or releases.

☐ Number of days
Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.
Recommended for projects following continuous delivery.

☐ Reference branch
Choose a branch as the baseline for the new code.
Recommended for projects using feature branches.

[Back](#) [Create 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.

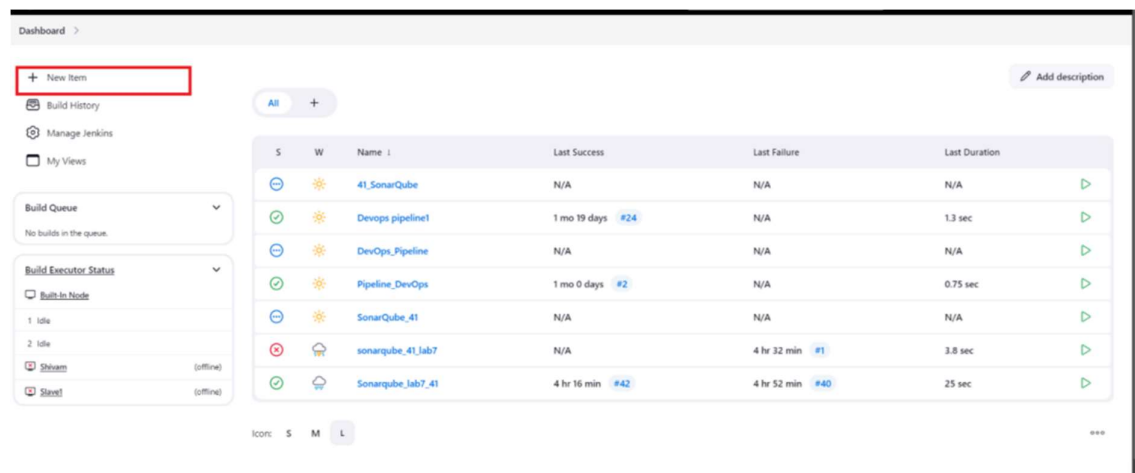
SonarQube™ technology is powered by [SonarSource SA](#)

Community Edition v10.6 (92116) ACTIVE [LGPL v3](#) [Community](#) [Documentation](#) [Plugins](#) [Web API](#)

Click on Create

Project is created

Step 5: Open Jenkins on whichever port it is installed. (<http://localhost:>). Go to the new item



Dashboard >

[+ New Item](#)

[Build History](#)

[Manage Jenkins](#)

[My Views](#)

Build Queue
No builds in the queue.

Build Executor Status

Builds in Node

1. **Idle**

2. **Idle**

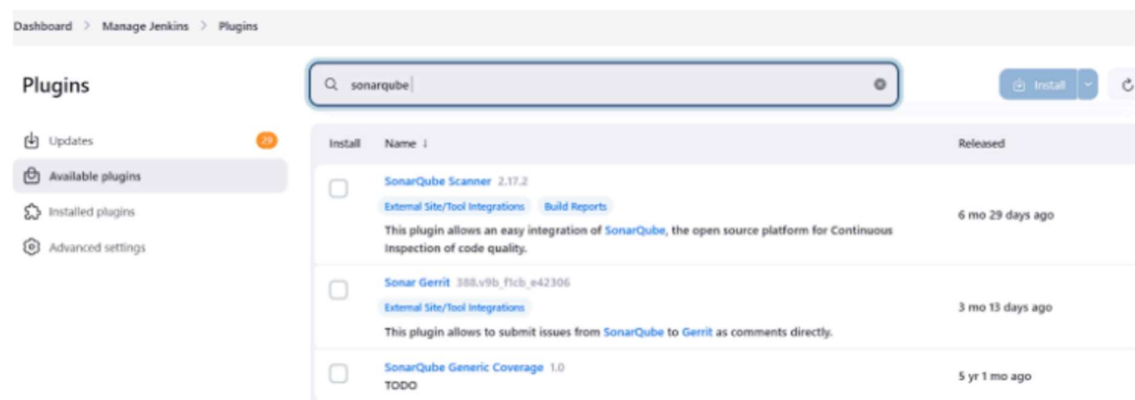
Shyam (offline)

Sham (offline)

S	W	Name	Last Success	Last Failure	Last Duration
🔄	☀️	41_SonarQube	N/A	N/A	N/A
✅	☀️	Devops pipeline1	1 mo 19 days #24	N/A	1.3 sec
🔄	☀️	DevOps_Pipeline	N/A	N/A	N/A
✅	☀️	Pipeline_DevOps	1 mo 0 days #2	N/A	0.75 sec
🔄	☀️	SonarQube_41	N/A	N/A	N/A
❌	🏠	sonarqube_41_lab7	N/A	4 hr 32 min #1	3.8 sec
✅	🏠	Sonarqube_lab7_41	4 hr 16 min #42	4 hr 52 min #40	25 sec

Icons: S M L

Step 6: Go to manage jenkins →available plugins then Search for Sonarqube Scanner for Jenkins and install it



Dashboard > Manage Jenkins > Plugins

Plugins

[Updates](#) 29

[Available plugins](#)

[Installed plugins](#)

[Advanced settings](#)

Search:

[Install](#) [Refresh](#)

Install	Name	Released
<input type="checkbox"/>	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
<input type="checkbox"/>	Sonar Gerrit 388.v9b_fcib_e42306 External Site/Tool Integrations This plugin allows to submit issues from SonarQube to Gerrit as comments directly.	3 mo 13 days ago
<input type="checkbox"/>	SonarQube Generic Coverage 1.0 TODO	5 yr 1 mo ago

Step 7: Now, go to Manage Jenkins → System. Under Sonarqube servers, add a server. Add server authentication token if needed.

Dashboard > Manage Jenkins > System >

SonarQube servers

If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.

☐ Environment variables

SonarQube installations

List of SonarQube installations

Name

This property is mandatory.

Server URL

Default is http://localhost:9000

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

+ Add +

Advanced ▾

Add SonarQube

Save Apply

Step 8: Go to Manage Jenkins → Tools. Go to SonarQube scanner, choose the latest configuration and choose to install automatically.

Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations

Edited

Add SonarQube Scanner

SonarQube Scanner

Name

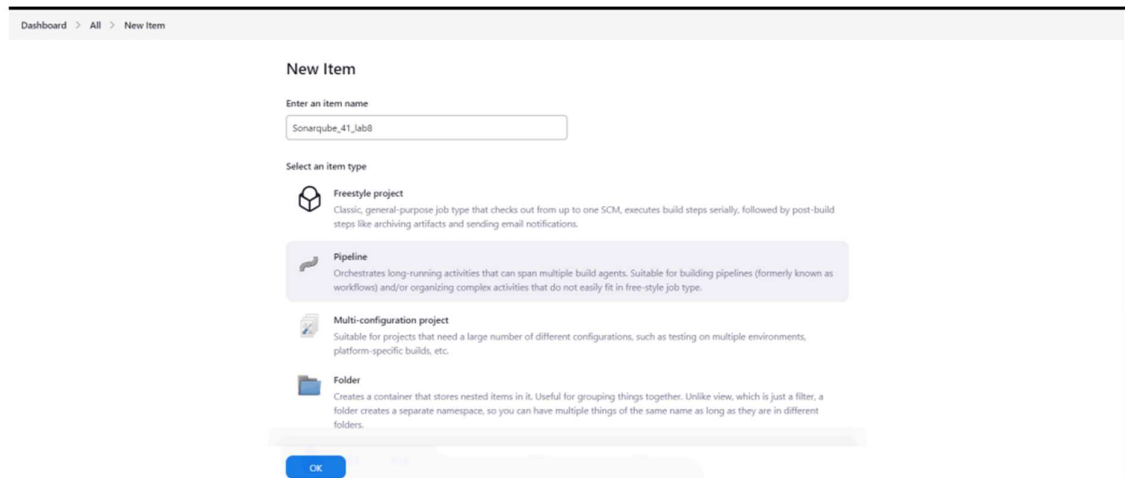
☒ Install automatically ?

Install from Maven Central

Version

Add Installer ▾

Save Apply



Step 10: Under Pipeline script, enter the following:

```
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
bat ""
```

```
C:\\Users\\Sandesh\\Downloads\\SonarqubeCLI\\sonar-scanner-6.1.0.4477-windows-x64\\bin\\sonar-scanner.bat ^
-D sonar.login=admin ^
-D sonar.password=Sandesh2@ ^
-D sonar.projectKey=SonarQube_Lab8 ^
-D sonar.exclusions=vendor/**,resources/**,**/*.java ^
-D sonar.host.url=http://localhost:9000/
""
}
}
}
```

```
1 = node {
2   stage('Cloning the GitHub Repo') {
3     git 'https://github.com/shaoforset/SQL.git'
4   }
5
6   stage('SonarQube analysis') {
7     withSonarQubeEnv('sonarqube') {
8       bat '
9         C:\\Users\\Gurajal\\OneDrive\\Desktop\\SonarqubeCLI\\sonar-scanner-6.1.0.4477-x864\\bin\\sonar-scanner.bat
10        -D sonar.login=admin "
11        -D sonar.password=Shivan@ "
12        -D sonar.projectKey=SonarQube_Lab1 "
13        -D sonar.exclusions=vendor\\**\\resources\\**\\*.java "
14        -D sonar.host.url=http://localhost:9000/
15      '
16    }
17  }
18 }
```

Click on save.

Build History trend

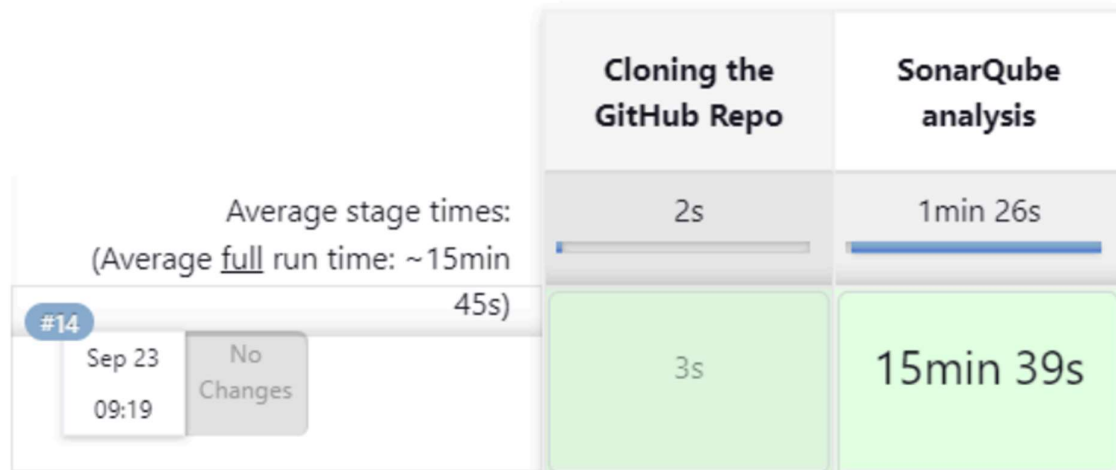
No builds

Atom feed for all Atom feed for failures

This is a Java sample project with many repetitive sections and coding issues that SonarQube will be able to detect during analysis.

Step 11: Go back to Jenkins. Go to the job you had just built and click on Build Now.

Stage View



The problem was C:\windows\system32 was not there so we need to add in our environment variable .

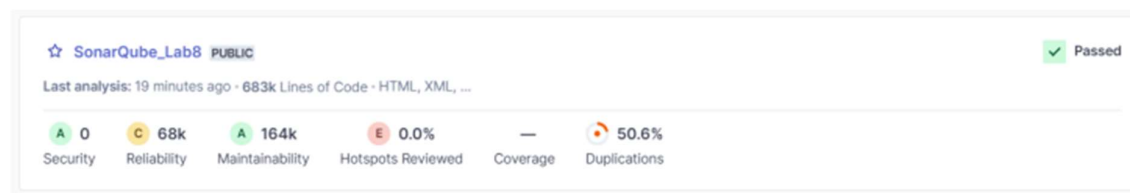
Now Check the console output once

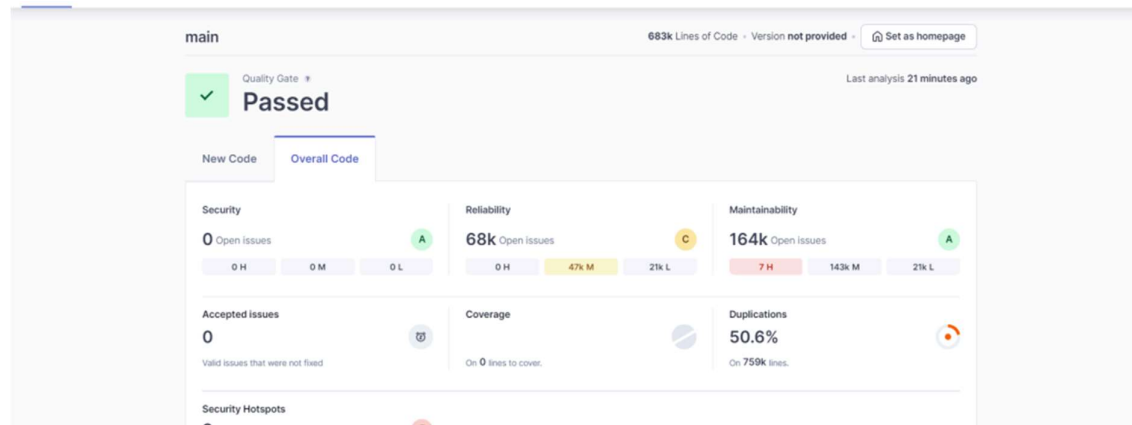
```
Keep only the first 100 references.
09:31:43.178 WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/assertions/gui/package-summary.html for block at line 40. Keep only the first 100 references.
09:31:43.194 WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/mail/sampler/package-summary.html for block at line 39. Keep only the first 100 references.
09:31:43.194 WARN: Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/mail/sampler/package-summary.html for block at line 40. Keep only the first 100 references.
09:31:43.213 INFO: CPD Executor CPD calculation finished (done) | time=170824ms
09:31:43.213 INFO: SCM revision ID 'ba799ba7e1b576f04a612322b0412c5ede1e54'
09:34:16.341 INFO: Analysis report generated in 4552ms, dir size=127.2 MB
09:34:33.584 INFO: Analysis report compressed in 17210ms, zip size=29.6 MB
09:34:34.392 INFO: Analysis report uploaded in 807ms
09:34:34.395 INFO: ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=SonarQube_Lab8
09:34:34.395 INFO: Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
09:34:45.805 INFO: More about the report processing at http://localhost:9000/api/ci/task?id=7dfe78a1-793d-47f9-bf86-4630b755c09
09:34:45.870 INFO: SonarScanner Engine completed successfully
09:34:45.929 INFO: EXECUTION SUCCESS
09:34:45.932 INFO: Total time: 15:36.252s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

REST API Jenkins 2.462.1

Successfully BUILD

Step 12: After the build is finished, return to SonarQube and review the linked project in detail.

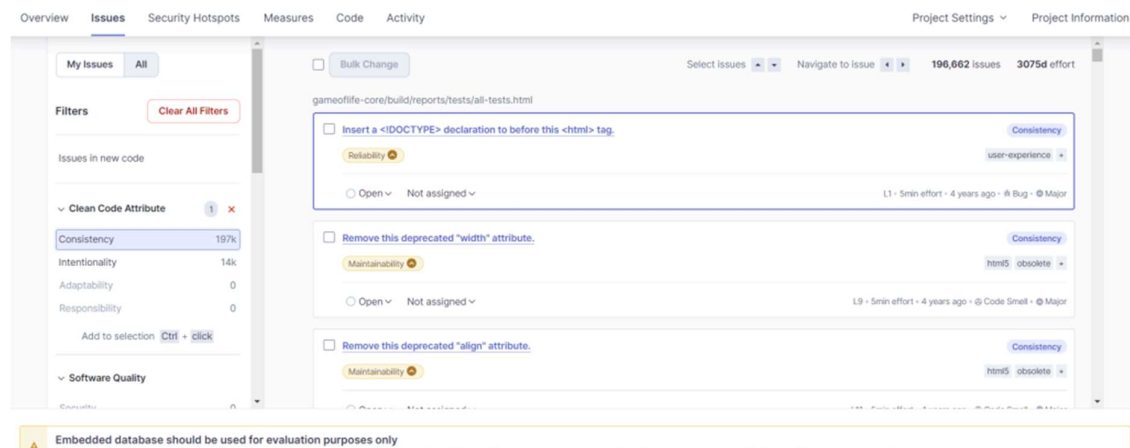




Under different options on the navbar , we can check all the issues with the code.

UNDER ISSUES:

1) Consistency



2) Reliability

The screenshot shows the SonarQube 'Issues' page for a project. The left sidebar displays a hierarchy of quality categories: Adaptability (0), Responsibility (0), Software Quality (1), Security (0), Reliability (14k), and Maintainability (15). The main panel shows a list of issues under the 'Accessibility' category. The first issue is 'Add "lang" and/or "xml:lang" attributes to this "<html>" element' with a severity of 'Intentionality' and a reliability of 'wcag2-a'. The second issue is 'Add "<th>" headers to this "<table>:"' with a severity of 'Intentionality' and a reliability of 'wcag2-a'. Both issues are marked as 'Open' and 'Not assigned'. A warning banner at the bottom states 'Embedded database should be used for evaluation purposes only'.

3) Maintainability

The screenshot shows the SonarQube 'Issues' page for a project. The left sidebar displays a hierarchy of quality categories: Adaptability (0), Responsibility (0), Software Quality (1), Security (0), Reliability (14k), and Maintainability (15). The main panel shows a list of issues under the 'Maintainability' category. The first issue is 'Use a specific version tag for the image.' with a severity of 'Intentionality' and a reliability of 'No tags'. The second issue is 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' with a severity of 'Intentionality' and a reliability of 'No tags'. Both issues are marked as 'Open' and 'Not assigned'. A warning banner at the bottom states 'Embedded database should be used for evaluation purposes only'.

4) Severity

The screenshot shows the SonarQube 'Issues' page for a project. The left sidebar displays a hierarchy of quality categories: Adaptability (0), Responsibility (0), Software Quality (1), Security (0), Reliability (14k), and Maintainability (15). The main panel shows a list of issues under the 'Severity' category. The first issue is 'Add the "let", "const" or "var" keyword to this declaration of "prop" to make it explicit.' with a severity of 'Intentionality' and a reliability of 'pitfall'. The second issue is 'Add the "let", "const" or "var" keyword to this declaration of "prop" to make it explicit.' with a severity of 'Intentionality' and a reliability of 'pitfall'. Both issues are marked as 'Open' and 'Not assigned'. A warning banner at the bottom states 'Embedded database should be used for evaluation purposes only'.

UNDER SECURITY HOTSPOT:

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

0.0% Security Hotspots Reviewed

To reviewAcknowledgedFixedSafe

3 Security Hotspots

Review priority: Medium

Permission1

The tomcat image runs with root as the default user. Make sure it is safe here.

Review priority: Low

Encryption of Sensitive Data1

Others1

The tomcat image runs with root as the default user. Make sure it is safe here.

Running containers as a privileged user is security-sensitive [docker:56471](#)

Status: To review

This security hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk?What's the risk?Assess the riskHow can I fix it?Activity

gameoflife-web/Dockerfile

Open in IDE

```
1FROM tomcat:8-jre8
2
3
4RUN rm -rf /usr/local/tomcat/webapps/*
5COPY target/gameOfLife.war /usr/local/tomcat/webapps/ROOT.war
6
7EXPOSE 8080
8CMD ["catalina.sh", "run"]
9
```

UNDER MEASURES:

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Project Overview

Security>

Reliability>

Maintainability>

Security Review>

Duplications>

Size>

Complexity>

SonarQube_Lab8

Risk

(Only showing data for the first 500 files)

See the data presented on this chart as a list

Color: Worse of Reliability Rating and Security Rating Size: Lines of Code

Zoom: 100%

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Duplications

Overview

Overall Code

Density50.6%

Duplicated Lines384,007

Duplicated Blocks42,819

Duplicated Files979

Size>

Complexity>

Issues>

Duplications Overview

(Only showing data for the first 500 files)

See the data presented on this chart as a list

Size: Duplicated Blocks

Zoom: 100%

CONCLUSION: