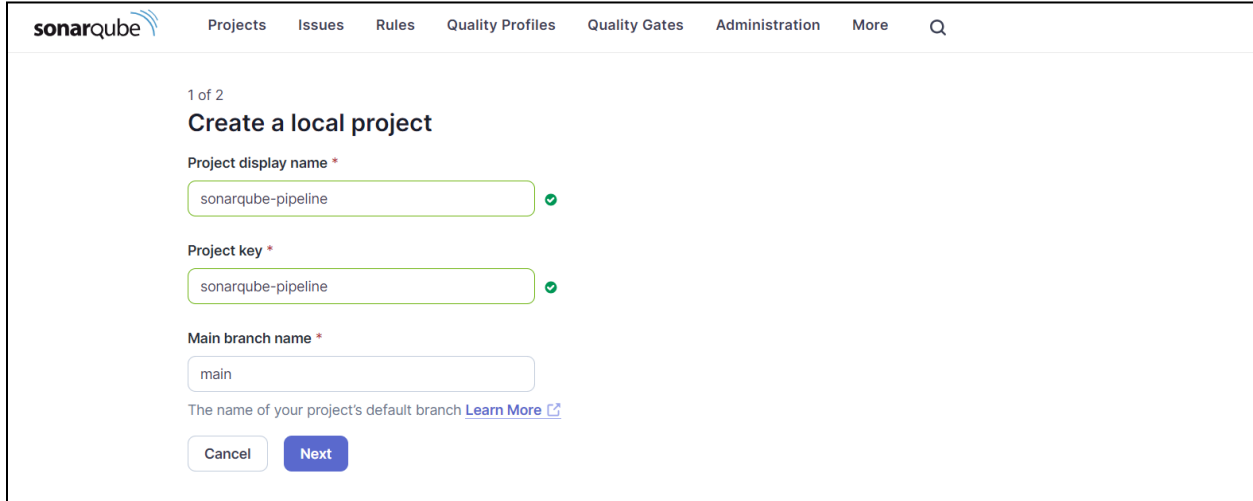


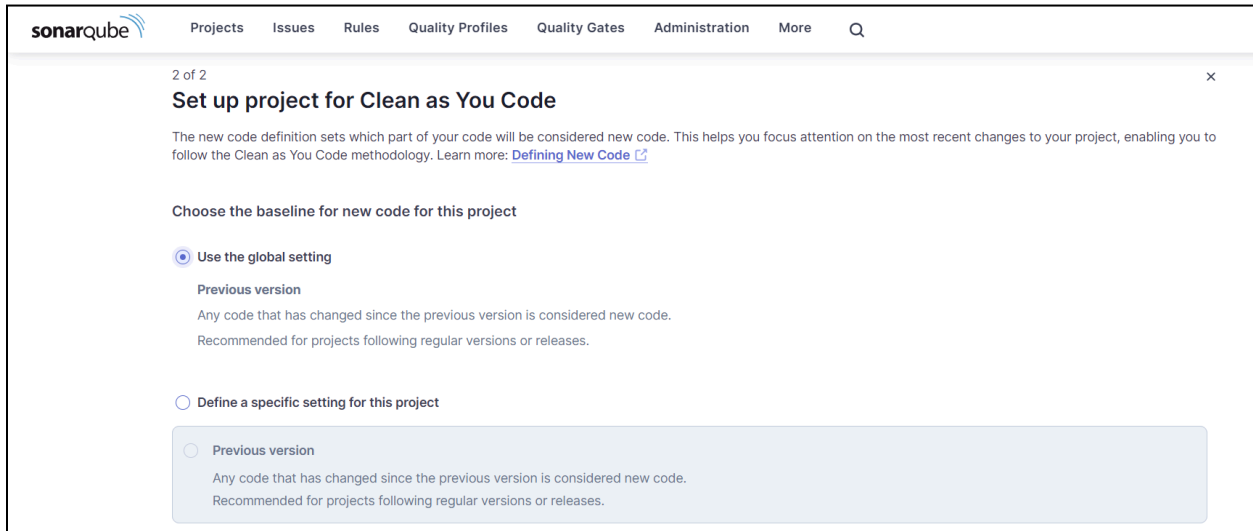
Experiment 8

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: Log in to sonarqube portal and create a local project.



The screenshot shows the 'Create a local project' form in the SonarQube portal. The form is titled '1 of 2 Create a local project'. It contains three input fields: 'Project display name' with the value 'sonarqube-pipeline', 'Project key' with the value 'sonarqube-pipeline', and 'Main branch name' with the value 'main'. Each field has a green checkmark icon to its right. Below the 'Main branch name' field, there is a link 'Learn More' with an external link icon. At the bottom of the form are two buttons: 'Cancel' and 'Next'.



The screenshot shows the 'Set up project for Clean as You Code' form in the SonarQube portal. The form is titled '2 of 2 Set up project for Clean as You Code'. It contains a text block explaining the new code definition and a link 'Defining New Code'. Below this, there is a section 'Choose the baseline for new code for this project' with two radio button options: 'Use the global setting' (selected) and 'Define a specific setting for this project'. The 'Define a specific setting for this project' option is expanded, showing a 'Previous version' option with a description: 'Any code that has changed since the previous version is considered new code. Recommended for projects following regular versions or releases.'

Step 2: Go to [download_sonarscanner](#) to download sonar scanner

sonarqube

Docs 10.6

Search...

Homepage

Try out SonarQube

Server installation and setup

Analyzing source code

Scanners

Analysis parameters

Latest | Analyzing source code | Scanners | SonarScanner CLI

SonarScanner CLI

SonarScanner

Issue Tracker

Show fewer

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

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

6.0

2024-06-04

New bootstrapping mechanism and JRE provisioning with SonarQube 10.6+ and SonarCloud

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

START FREE

On this page

Configuring your project

Running SonarScanner CLI from the zip file

Running SonarScanner CLI from the Docker image

Scanning C, C++, or Objective-C projects

Sample projects

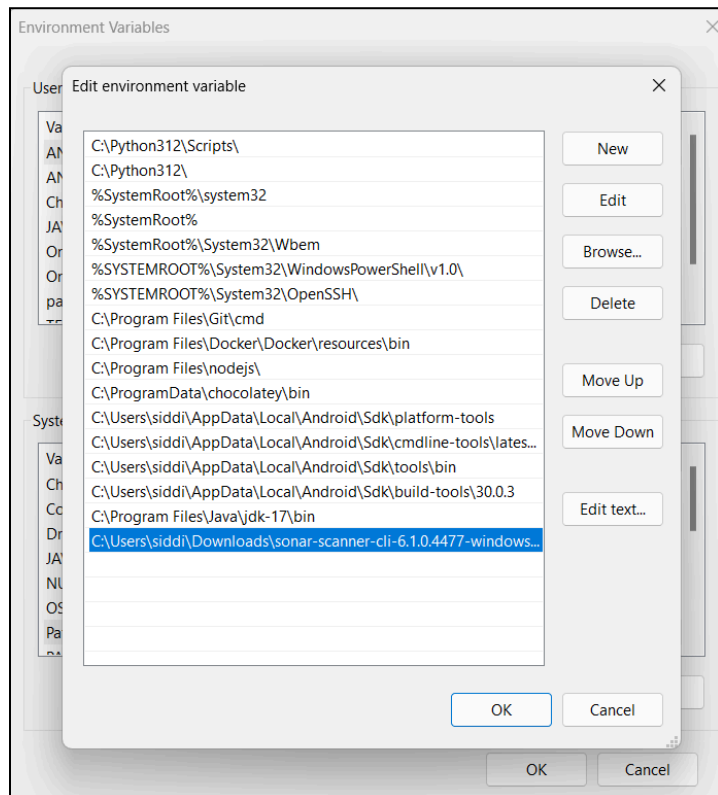
Alternatives to sonar-project.properties

Alternate analysis directory

Advanced configuration

Troubleshooting

After the download is complete, extract the file and copy the path to bin folder
Go to environment variables, system variables and click on path
Add a new path, paste the path copied earlier.




Step 3: Create a New Item in Jenkins, choose Pipeline.

Dashboard > All > New Item


New Item

Enter an item name


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.




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


OK

Dashboard > sonarqube-pipeline > Configuration


Configure



General



Advanced Project Options



Pipeline

Pipeline

Definition

Pipeline script

Script ?

```
1 node {
2   stage('Cloning the Github Repo') {
3     git 'https://github.com/shazforiot/GOL.git'
4   }
5   stage('SonarQube analysis') {
6     withSonarQubeEnv('sonarqube') {
7       bat ---
8       C:\Users\siddi\Downloads\sonar-scanner-cli-6.1.0.4477-windows-x64\sonar-scanner-6.1.0.4477-windows-x64\bin\sonar-scan
9       -Dsonar.login=admin ^
10      -Dsonar.password=Mahvish ^
11      -Dsonar.projectKey=sonarqube-pipeline ^
12      -Dsonar.exclusions=vendor/**,resources/**,*/*.java ^
13      -Dsonar.host.url=http://localhost:9000/
14      ""
15     }
16   }
17 }
```


☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

Save Apply

Step 4: Save the pipeline and build it.

Dashboard > sonarqube-pipeline >

Status  sonarqube-pipeline

</> Changes

▶ Build Now

⚙️ Configure

🗑️ Delete Pipeline

🔍 Full Stage View

🌊 SonarQube

📁 Stages

✎ Rename

🔍 Pipeline Syntax

Stage View

	Cloning the GitHub Repo	SonarQube analysis
Average stage times: (Average full run time: ~7min 49s)	9s	3min 53s
#2 Sep 26 20:42 No Changes	2s	7min 46s
#1 Sep 26 20:24 No Changes	15s	1s failed

Build History

trend ▾

Filter...

- #2
Sep 26, 2024, 8:42 PM
- #1
Sep 26, 2024, 8:24 PM

Permalinks

- Last build (#2), 9 min 1 sec ago
- Last stable build (#2), 9 min 1 sec ago
- Last successful build (#2), 9 min 1 sec ago
- Last failed build (#1), 26 min ago
- Last unsuccessful build (#1), 26 min ago
- Last completed build (#2), 9 min 1 sec ago

Console output:

Dashboard > sonarqube-pipeline > #2

Status  Console Output  Download  Copy View as plain text

</> Changes

📄 Console Output

✎ Edit Build Information

🗑️ Delete build '#2'

🕒 Timings

🔗 Git Build Data

🌊 Pipeline Overview

📄 Pipeline Console

🔄 Replay

📁 Pipeline Steps

📁 Workspaces

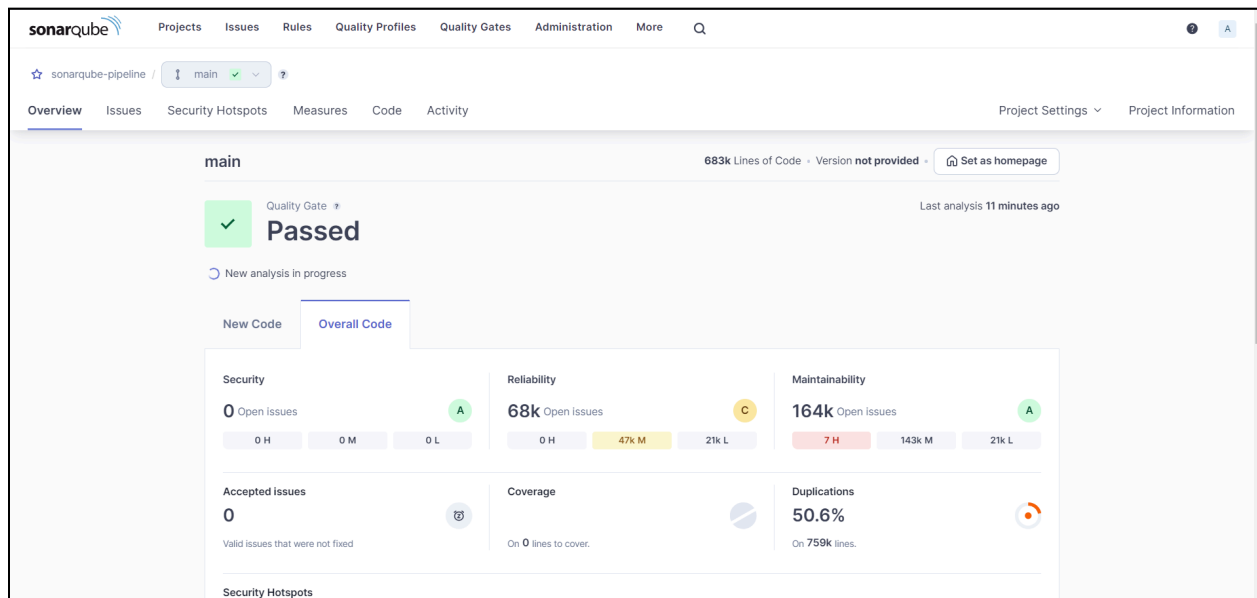
← Previous Build

Skipping 4,248 KB. [Full Log](#)

```
20:49:35.711 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 40. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 65. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 41. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 17. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 1487. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 226. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 229. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 225. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 226. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 424. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 17. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at
```

```
20:50:01.832 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-pipeline
20:50:01.832 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
20:50:01.832 INFO More about the report processing at http://localhost:9000/api/ce/task?id=159a9d05-1f5f-4e17-bd27-3643a32a836a
20:50:12.108 INFO Analysis total time: 7:37.235 s
20:50:12.110 INFO SonarScanner Engine completed successfully
20:50:12.849 INFO EXECUTION SUCCESS
20:50:12.851 INFO Total time: 7:44.878s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Step 5: After that, check the project in SonarQube



Under different tabs, check all different issues with the code.

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-pipeline / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Reliability Maintainability Security Review Duplications Size Complexity Issues

Overall Code

Open Issues 210,549

Confirmed Issues 0

Accepted Issues 0

False Positive Issues 0

sonarqube-pipeline View as Tree Select files Navigate 6 files

Open Issues 210,549 See history

gameoflife-acceptance-tests	4
gameoflife-build	0
gameoflife-core	603
gameoflife-deploy	0
gameoflife-web	209,940
pom.xml	2

6 of 6 shown

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-pipeline / main

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 x

Consistency	107k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

Security	0
Reliability	54k
Maintainability	164k

Bulk Change

Select issues Navigate to issue 196,662 issues 3075d effort

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

Insert a <DOCTYPE> declaration to before this <html> tag. Consistency user-experience L1 - 5min effort - 4 years ago - @ Bug - @ Major

Remove this deprecated "width" attribute. Consistency html5 obsolete L9 - 5min effort - 4 years ago - @ Code Smell - @ Major

Remove this deprecated "align" attribute. Consistency html5 obsolete L11 - 5min effort - 4 years ago - @ Code Smell - @ Major

Remove this deprecated "align" attribute. Consistency html5 obsolete

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-pipeline / main

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 x

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection [Ctrl + click](#)

Software Quality 1 x

Security	0
Reliability	14k
Maintainability	15

Add to selection [Ctrl + click](#)

☐ Bulk Change Select issues [x](#) Navigate to issue [x](#) **13,887 issues** **59d effort**

gameoflife-acceptance-tests/Dockerfile

☐ Use a specific version tag for the image. **Intentionality**

Maintainability

☐ Open ☐ Not assigned

☐ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. **Intentionality**

Maintainability

☐ Open ☐ Not assigned

☐ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. **Intentionality**

Maintainability

☐ Open ☐ Not assigned

Introducing Clean Code Attributes

Clean Code attributes are the characteristics that your code must have to be considered Clean Code.

You can now filter by these attributes to evaluate why your code is breaking away from being clean.

1 of 5 [Next](#)

L12 • 5min effort • 4 years ago • @ Code Smell • @ Major

No tags

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More Q

sonarqube-pipeline / main

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 x

Consistency	54k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection [Ctrl + click](#)

Software Quality 1 x

Security	0
Reliability	14k
Maintainability	15

Add to selection [Ctrl + click](#)

☐ Bulk Change Select issues [x](#) Navigate to issue [x](#) **13,872 issues** **59d effort**

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

☐ Add "lang" and/or "xml:lang" attributes to this "chtmlb" element **Intentionality**

Reliability

☐ Open ☐ Not assigned

L1 • 2min effort • 4 years ago • @ Bug • @ Major

accessibility wcag2-a

☐ Add "<th>" headers to this "table". **Intentionality**

Reliability

☐ Open ☐ Not assigned

L9 • 2min effort • 4 years ago • @ Bug • @ Major

gameoflife-core/build/reports/tests/allclasses-frame.html

☐ Add "lang" and/or "xml:lang" attributes to this "chtmlb" element **Intentionality**

Reliability

☐ Open ☐ Not assigned

L1 • 2min effort • 4 years ago • @ Bug • @ Major

accessibility wcag2-a

☐ Add "<th>" headers to this "table". **Intentionality**

Reliability

☐ Open ☐ Not assigned

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project Settings

My IssuesAll

Filters

Clear All Filters

Issues in new code

Clean Code Attribute1

Consistency164k

Intentionality15

Adaptability0

Responsibility0

Add to selectionCtrl + click

Software Quality1

Security0

Reliability14k

Maintainability15

Add to selectionCtrl + click

Bulk Change

Select issues

Navigate to issue

15 issues44min 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

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

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project Settings

Security0

Reliability253

Maintainability15

Add to selectionCtrl + click

Severity

Type1

Bug0

Vulnerability0

Code Smell15

Scope

Status

Security Category

Creation Date

Bulk Change

Select issues

Navigate to issue

15 issues44min 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

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

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

0.0% Security Hotspots Reviewed

3 Security Hotspots

Review priority: Medium

Permission

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

Review priority: Low

Encryption of Sensitive Data

Others

3 of 3 shown

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 risk

How can I fix it?

Activity

gameoflife-web/Dockerfile

Open in IDE

1FROM tomcat:8-jre8

2

3RUN rm -rf /usr/local/tomcat/webapps/*

4

5COPY target/gameoflife.war /usr/local/tomcat/webapps/ROOT.war

6

7EXPOSE 8080

8CMD ["catalina.sh", "run"]

9

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

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Reliability

Maintainability

Security Review

Duplications

Overview

Overall Code

Density50.6%

Duplicated Lines384,007

Duplicated Blocks42,808

Duplicated Files979

Size

sonarqube-pipeline

View asTree

Select files

Navigate

6 files

Duplicated Lines (%)50.6%See history

	Duplicated Lines (%)	Duplicated Lines
gameoflife-acceptance-tests	0.0%	0
gameoflife-build	0.0%	0
gameoflife-core	9.6%	374
gameoflife-deploy	0.0%	0
gameoflife-web	50.9%	383,633
pom.xml	0.0%	0

