Code analysis and dependency check tools

Wojtek

Table of Contents

SonarQube

For...

- the most popular tool
- huge community, many thematic forums
- supports Java and Scala
- good integration with CI/CD tools (GitLab, Jenkins)
- extensive code analysis, possible errors, complexity reduction, etc.
- standard in many IT companies
- contains a lot of plugins, including dependency analysis

…and against

- not an open-source tool (paid license)
- bad integration with IntelliJ IDE - poorly rated plugin
- lots of features that we may never use (disadvantage?)
- report isn't created as a static website
- need to put the Sonarqube (server) on some machine (port)

JetBrains Qodana

For...

- extensive code analysis, possible errors, etc.
- support for Java
- very good integration with CI/CD tools (GitLab, Jenkins) and with IntelliJ IDE
- completely new tool, may become very popular in the long term
- report as static website (GitLab artifact and gitlab.io page)

…and against

- currently no support for Scala (work in progress)
- paid license (from March 2023)
- possible bugs (?)
- currently not very popular tool
- bad integration with other plugins

GitLab (Code Climate plugin)

For...

- extensive code analysis, possible errors, complexity reduction, etc.
- support for Java and Scala
- very good integration with CI/CD tool (GitLab)

https://docs.gitlab.com/ee/ci/testing/code_quality.html

…and against

- merge request diff view only in GitLab Ultimate
- less visually attractive reports than, for example, in JetBrains Qodana
- bad integration with IntelliJ IDE

OWASP Dependency Check

For...

- security standard
- easy to use
- good integration with CI/CD tools (GitLab, Jenkins) / with Sonar / with Gradle

…and against

- not a pretty report :)

GitLab – Dependency Scanning

For...

- very good integration with CI/CD tools (GitLab)
- report available directly on GitLab

…and against

- only available in GitLab Ultimate

Questions?