Docker static code analysis

Unique rules to find Vulnerabilities, Security Hotspots, and Code Smells in your DOCKER code

All rules 44 | Vulnerability 4 | Bug 4 | Security Hotspot 15 | Code Smell 21

Tags | Impact | Clean code attribute | Search by name...

Double quote to prevent globbing and word splitting
Code Smell

Instructions should be upper case
Code Smell

Allowing non-root users to modify resources copied to an image is security-sensitive
Security Hotspot

Automatically installing recommended packages is security-sensitive
Security Hotspot

Running containers as a privileged user is security-sensitive
Security Hotspot

Delivering code in production with debug features activated is security-sensitive
Security Hotspot

Use ADD instruction to retrieve remote resources
Code Smell

Arguments in long RUN instructions should be sorted
Code Smell

Track uses of "TODO" tags
Code Smell

Descriptive labels are mandatory
Code Smell

Use digest to pin versions of base images
Code Smell

Dockerfile parsing failure
Code Smell

Descriptive labels are mandatory

Analyze your code

Consistency - Conventional | Maintainability

Code Smell | Major

This rule raise an issue when one of the mandatory label are missing.

Why is this an issue? | How can I fix it? | More Info

Adding labels to your image help to organize images by project, record licensing information, aid in automation and for other reasons. The rule provide the possibility to configure the list of mandatory label that must be present in every Dockerfile.

Available In:
sonarlint | sonarcloud | sonarqube