Secrets
ABAP
Apex
AzureResourceManager
C
C#
C++
CloudFormation
COBOL
CSS
Dart
Docker
Flex
Go
HTML
Java
JavaScript
JCL
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

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...

Allowing shell scripts execution during package installation is security-sensitive
Security Hotspot

Using host operating system namespaces is security-sensitive
Security Hotspot

Setting loose POSIX file permissions is security-sensitive
Security Hotspot

Reduce the amount of consecutive RUN instructions
Code Smell

Prefer COPY over ADD for copying local resources
Code Smell

WORKDIR instruction should only be used with absolute path
Code Smell

Too long RUN instruction should be split into multiple lines
Code Smell

Prefer Exec form for ENTRYPOINT and CMD instructions
Code Smell

"WORKDIR" instruction should be used instead of "cd" commands
Code Smell

Specific version tag for image should be used
Code Smell

Package update should not be executed without installing it
Code Smell

Cache should be cleaned after package installation

Access variable which is not available in the current scope

Analyze your code

Intentionality - Logical | Reliability

Bug | Major

The variable is not available in the current scope. It will be evaluated to an empty value.

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

Documentation

- ARG scope - Dockerfile reference

Available In:

sonarlint | sonarcloud | sonarqube