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...

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

Double quote to prevent globbing and word splitting

Analyze your code

Intentionality - Complete | Maintainability

Code Smell | Major

Variable references should be encapsulated with double quotes to avoid globbing and word splitting.

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

Within the command, variable references and command substitutions go through word splitting and pathname expansion (globbing).

This causes issues if the variable contains whitespaces or shell pathname expansion (glob) characters like `*`.

What is the potential impact?

This issue can lead to bugs if the variable contains sensitive characters, which may be interpreted incorrectly and thus lead to undesired behavior.

Available In:
sonarlint | sonarcloud | sonarqube