




































-  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... 🔍

"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
 Code Smell
Deprecated instructions should not be used
 Code Smell
Consent flag should be set to avoid manual input
 Code Smell
Environment variables should not be unset on a different layer than they were set
 Code Smell
Expanded filenames should not become options
 Code Smell
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

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

Analyze your code

Intentionality - Clear

Maintainability ⬆️

 Code Smell

 Major ?

Why is this an issue?

How can I fix it?

More Info

Where possible, ensure that all usages of `cd` commands are replaced by a `WORKDIR` instruction. The `cd` commands at the beginning or end of a chain of commands are a reliable sign that they can be replaced. Also, using absolute paths can be considered for commands that accept them.

Code examples

Noncompliant code example

```
RUN cd /app/bin && ./start.sh
```

Compliant solution

```
WORKDIR /app/bin
RUN ./start.sh

# Or:
RUN /app/bin/start.sh
```

Available In:

sonarlint  | **sonarcloud**  | **sonarqube** 

