# 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...

- 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
- 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

## Deprecated instructions should not be used

Analyze your code

Consistency - Conventional | Maintainability

Code Smell | Major

Deprecated instructions should be replaced by other suggested instructions.

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

Languages and technologies evolve, which leads to deprecation of some features. At some day they may be removed. It is important to use up-to-date constructs to avoid issues by migration to newer version of technology.

Available In:

sonarlint | sonarcloud | sonarqube