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...

Credentials should not be hard-coded
Vulnerability

Using ENV or ARG to handle secrets is security-sensitive
Security Hotspot

Permissions of sensitive mount points should be restrictive
Vulnerability

Server certificates should be verified during SSL/TLS connections
Vulnerability

Weak SSL/TLS protocols should not be used
Vulnerability

Disabling builder sandboxes is security-sensitive
Security Hotspot

Exposing administration services is security-sensitive
Security Hotspot

Recursively copying context directories is security-sensitive
Security Hotspot

Using clear-text protocols is security-sensitive
Security Hotspot

Using weak hashing algorithms is security-sensitive
Security Hotspot

Malformed JSON in Exec form leads to unexpected behavior
Bug

Dockerfile should only have one ENTRYPOINT and CMD instruction

Weak SSL/TLS protocols should not be used

Analyze your code

Responsibility - Trustworthy | Security

Vulnerability | Critical | cwe privacy

This vulnerability exposes encrypted data to a number of attacks whose goal is to recover the plaintext.

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

Articles & blog posts

- Wikipedia, Padding Oracle Attack
- Wikipedia, Chosen-Ciphertext Attack
- Wikipedia, Chosen-Plaintext Attack
- Wikipedia, Semantically Secure Cryptosystems
- Wikipedia, OAEP
- Wikipedia, Galois/Counter Mode

Standards

- CWE - CWE-327 - Use of a Broken or Risky Cryptographic Algorithm

Available In:

sonarlint | sonarcloud | sonarqube