





































-  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...

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

 Bug

Access variable which is not available in the current scope

 Bug

A space before the equal sign in key-value pair may lead to unintended behavior

 Bug

## Server certificates should be verified during SSL/TLS connections

Analyze your code

Responsibility - Trustworthy

Security 

 Vulnerability

 Critical



 cwe privacy ssl

This vulnerability makes it possible that an encrypted communication is intercepted.

Why is this an issue?

How can I fix it?

More Info

## Standards

- OWASP - [Top 10 2021 Category A2 - Cryptographic Failures](#)
- OWASP - [Top 10 2021 Category A5 - Security Misconfiguration](#)
- OWASP - [Top 10 2021 Category A7 - Identification and Authentication Failures](#)
- OWASP - [Top 10 2017 Category A3 - Sensitive Data Exposure](#)
- OWASP - [Top 10 2017 Category A6 - Security Misconfiguration](#)
- OWASP - [Mobile Top 10 2016 Category M3 - Insecure Communication](#)
- OWASP - [Mobile AppSec Verification Standard - Network Communication Requirements](#)
- CWE - [CWE-295 - Improper Certificate Validation](#)
- STIG Viewer - [Application Security and Development: V-222550](#) - The application must validate certificates by constructing a certification path to an accepted trust anchor.

Available In:

**sonarlint**



**sonarcloud**



**sonarqube**



© 2008-2024 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE, and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Sonar helps developers write [Clean Code](#).  
[Privacy Policy](#) | [Cookie Policy](#)

