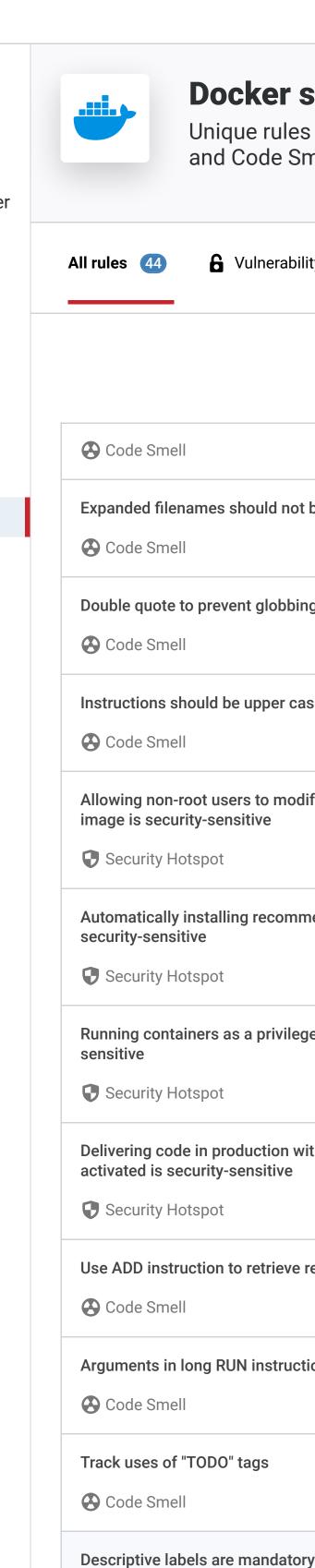
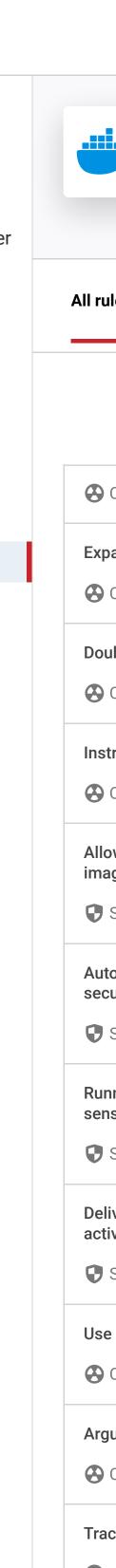
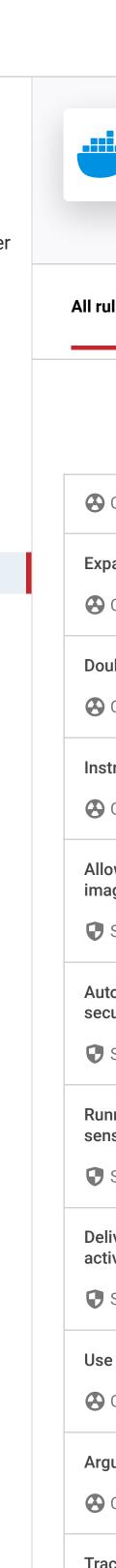
Q

Sonar RULES Secrets Apex AzureResourceManager CloudFormation COBOL CSS Docker Flex **=GO** Go HTML JavaScript Kubernetes Objective C PL/SQL RPG Terraform **Text** TypeScript T-SQL



Code Smell





Docker static code analysis

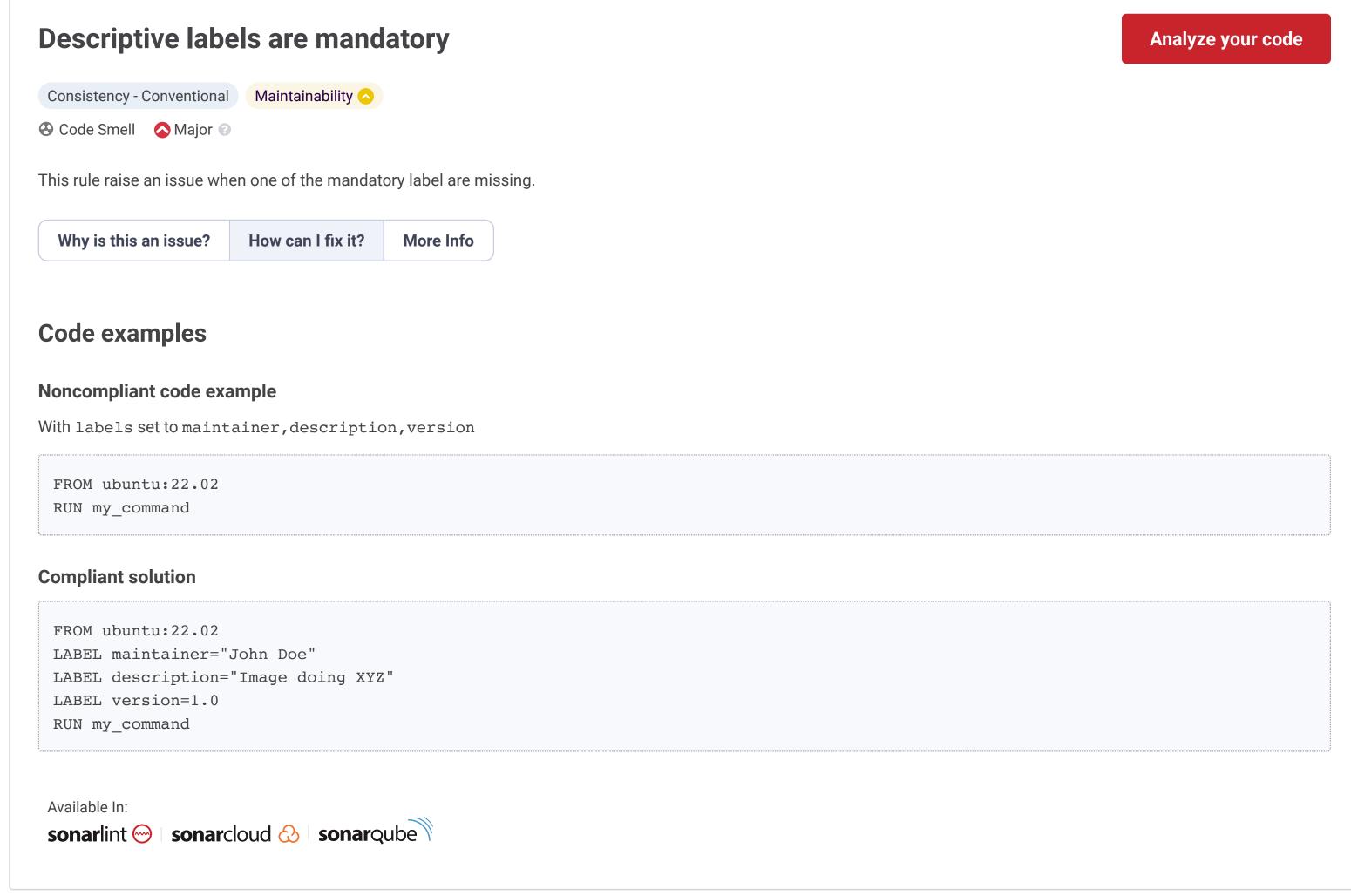
Unique rules to find Vulnerabilities, Security Hotspots, and Code Smells in your DOCKER code

rules 44	6 Vulnerability 4	🕏 Bug 4	Security Hotspot 15	Code Smell 21

Tags

Impact

Code Smell	
Expanded filenames should not become option	าร
Code Smell	
Double quote to prevent globbing and word sp	litting
Code Smell	
Instructions should be upper case	
Code Smell	
Allowing non-root users to modify resources c image is security-sensitive	opied to an
Security Hotspot	
Automatically installing recommended packag security-sensitive	es is
Security Hotspot	
Running containers as a privileged user is secu sensitive	ırity-
Security Hotspot	
Delivering code in production with debug featu activated is security-sensitive	ires
Security Hotspot	
Use ADD instruction to retrieve remote resourc	ees
Code Smell	
Arguments in long RUN instructions should be	sorted
Code Smell	
Track uses of "TODO" tags	
Code Smell	



Search by name...

Clean code attribute

© 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

