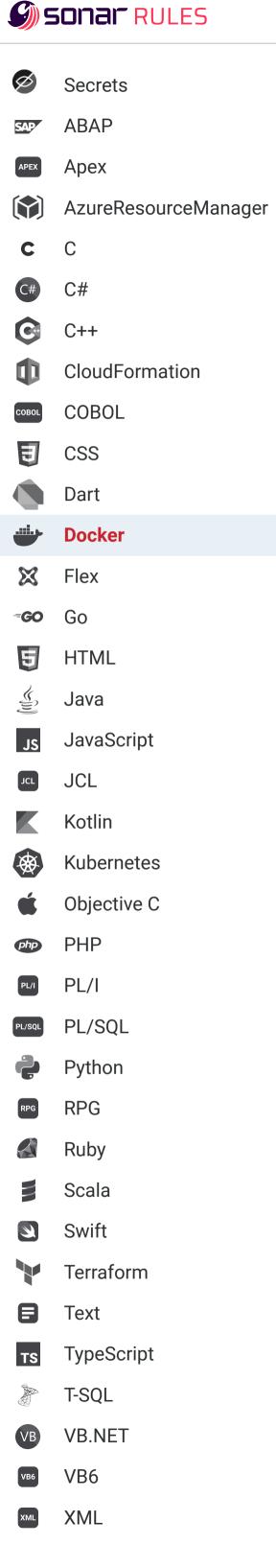
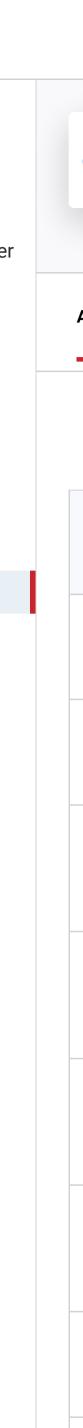
Search by name...

Q







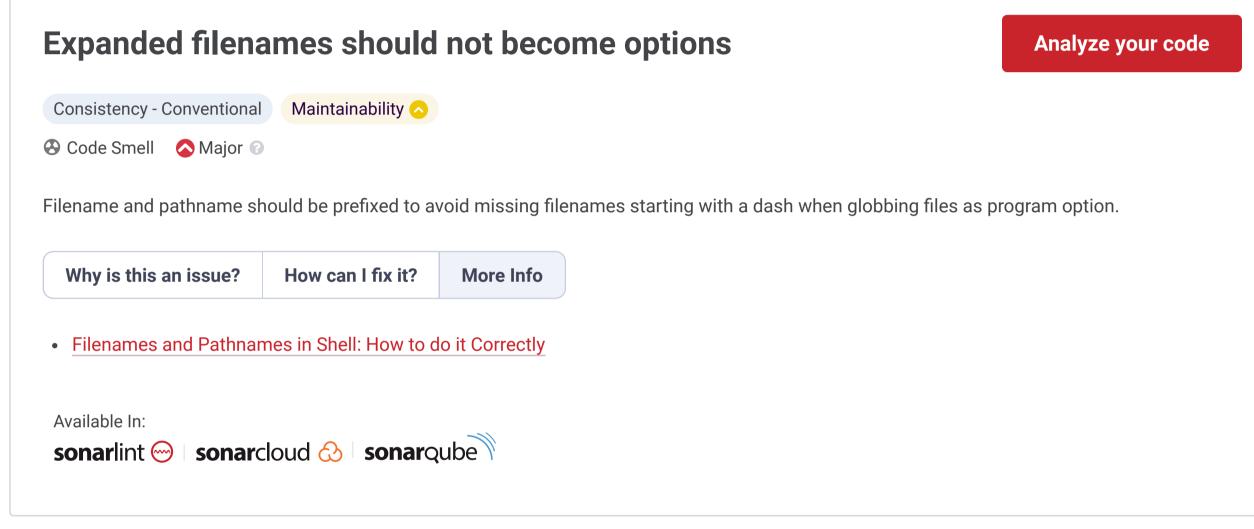
Code Smell



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
	Tags
Expanded filenames should not become options Code Smell	Expanded
Double quote to prevent globbing and word splitting Code Smell	Consistency - Con
Instructions should be upper case Code Smell	Filename and path Why is this an i
Allowing non-root users to modify resources copied to an image is security-sensitive Security Hotspot	• Filenames and
Automatically installing recommended packages is security-sensitive	Available In: sonarlint
Running containers as a privileged user is security- sensitive Security Hotspot	© 2008-2024 SonarSo
Delivering code in production with debug features activated is security-sensitive Security Hotspot	
Use ADD instruction to retrieve remote resources Code Smell	
Arguments in long RUN instructions should be sorted Code Smell	
Track uses of "TODO" tags Code Smell	
Descriptive labels are mandatory	



Clean code attribute

Code Smell (21)

Impact

© 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

