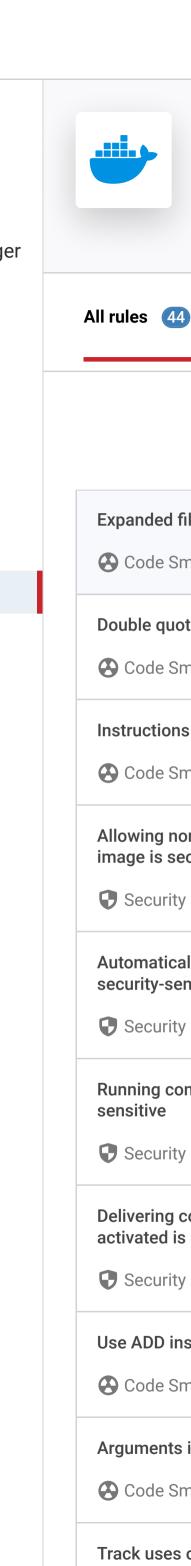
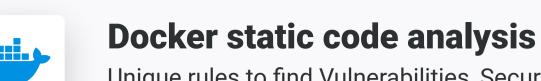
Search by name...

Q



Sonar RULES		
Ø	Secrets	
SAP	ABAP	
APEX	Apex	
	AzureResourceManage	
С	С	
C#	C#	
G	C++	
Ф	CloudFormation	
COBOL	COBOL	
₹	CSS	
	Dart	
<u></u>	Docker	
\bowtie	Flex	
=GO	Go	
5	HTML	
	Java	
JS	JavaScript	
JCL	JCL	
	Kotlin	
*	Kubernetes	
É	Objective C	
Php	PHP	
PL/I	PL/I	
PL/SQL	PL/SQL	
	Python	
RPG	RPG	
2	Ruby	
	Scala	
<u> </u>	Swift	
	Terraform	
	Text	
TS	TypeScript	
	T-SQL	
VB	VB.NET	
VB6	VB6	
XML	XML	





6 Vulnerability 4

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

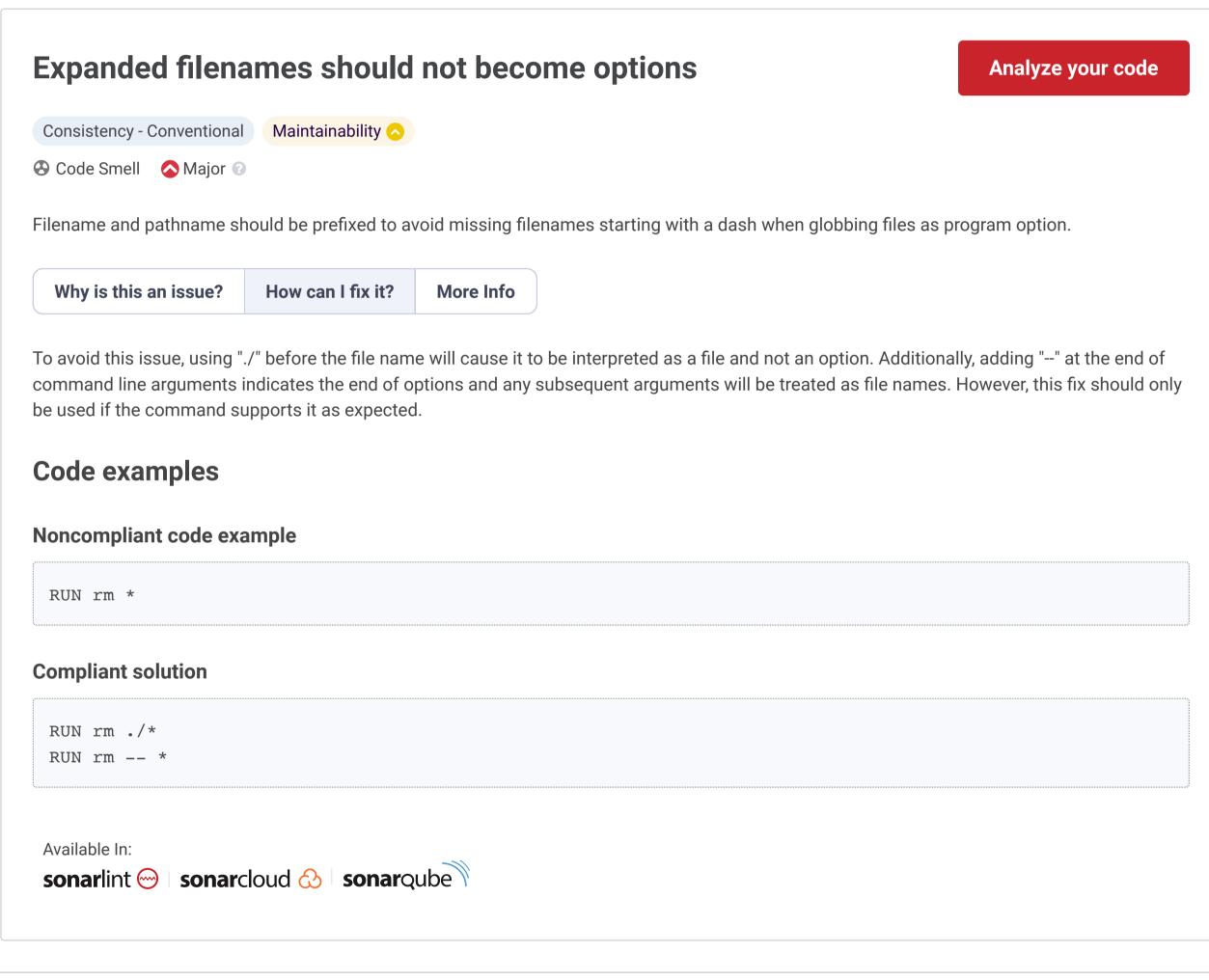
Rug 4

Security Hotspot 15

Code Smell 21

Impact

	Tags
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	
Arguments in long RUN instructions should be sorted Code Smell	
Track uses of "TODO" tags Code Smell	
Descriptive labels are mandatory Code Smell	



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

