Search by name...

Sonar RULES		
Ø	Secrets	
SAP	ABAP	
APEX	Apex	
	AzureResourceManager	
C	С	
C#	C#	
<b>©</b>	C++	
Ф	CloudFormation	
COBOL	COBOL	
<b>3</b>	CSS	
	Dart	
<b>—</b>	Docker	
$\bowtie$	Flex	
<b>=GO</b>	Go	
5	HTML	
	Java	
JS	JavaScript	
JCL	JCL	
	Kotlin	
*	Kubernetes	
É	Objective C	
php	PHP	
PL/I	PL/I	
PL/SQL	PL/SQL	
Ş	Python	
RPG	RPG	
	Ruby	
	Scala	
<u> </u>	Swift	
	Terraform	
	Text	
TS	TypeScript	
	T-SQL	
VB	VB.NET	
VB6	VB6	
XML	XML	



## **Docker static code analysis**

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

All rules 44	Security Hotspot 15
	Tags
Environment variables should not be unset on a different layer than they were set  Code Smell	Environme than they
Expanded filenames should not become options  Code Smell	Consistency - Con  Code Smell
Double quote to prevent globbing and word splitting  Code Smell	Setting an environ subsequent build particular layer, bu
Instructions should be upper case  Code Smell	Why is this an i
Allowing non-root users to modify resources copied to an image is security-sensitive  Security Hotspot	dumped anytime.  Available In:
Automatically installing recommended packages is security-sensitive  Security Hotspot	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

## Environment variables should not be unset on a different layer than they were set

Clean code attribute

**Analyze your code** 

Q

Setting an environment variable using the ENV instruction creates a new layer in the Docker image. The variable is then persisted for all subsequent build stages and is also present in the resulting image. Calling RUN unset <env-variable> unsets the variable only for this particular layer, but it is still possible to dump the environment variable from the previous layer.

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

Code Smell 21

Impact

Consistency - Conventional Maintainability 🛆

The environment variables often contain secrets, tokens, and other sensitive information. They are present in the containers and could be dumped anytime. Calling unset doesn't prevent this information from being hidden for other commands.

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

