Code Smell (144)







All rules (268)

PHP static code analysis

6 Vulnerability (40)

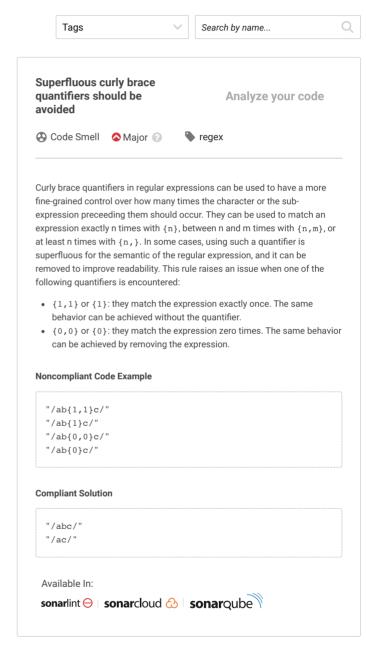
Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your PHP code

₩ Bug (51)

0	NTOL VOLLION CHALLING WAT TO LLOOK
	ctal values should not be used
6	Code Smell
	witch cases should end with an
_	
6	Code Smell
	ession-management cookies should
	ot be persistent
	Vulnerability
Cr	ryptographic RSA algorithms should
	ways incorporate OAEP (Optimal symmetric Encryption Padding)
6	Vulnerability
Sŀ	HA-1 and Message-Digest hash
	gorithms should not be used in
_	Vulnerability
	Vullerability
	ssertions should not be made at the
<u>}</u> []	(Bug
	egular expressions should be
	ntactically valid
}ſĪ	Eug
	nly one method invocation is
_	spected when testing exceptions
<u>}[ī</u>	(Bug
	eading the Standard Input is
	curity-sensitive
V	Security Hotspot
	sing command line arguments is
	curity-sensitive
6	Security Hotspot

Using Sockets is security-sensitive

Security Hotspot



© 2008-2022 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. Privacy Policy

Security Hotspot 33

Encrypting data is security-sensitive

Security Hotspot

Using regular expressions is security-sensitive

Security Hotspot

Deserializing objects from an untrusted source is security-sensitive

Security Hotspot

Literal boolean values and nulls should not be used in equality assertions

Code Smell

"global" should not be used