Code Smell (144)







PHP static code analysis

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

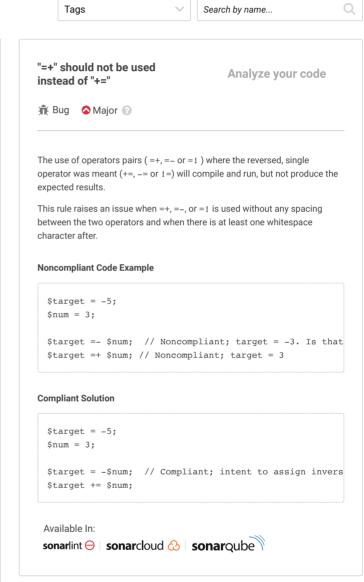
♣ Bug (51)

All rules 268 Vulnerability 40
3 3343 3
Generic exceptions ErrorException, RuntimeException and Exception should not be thrown Code Smell
Local variables should not have the same name as class fields
Code Smell
Redundant pairs of parentheses should be removed
☼ Code Smell
Inheritance tree of classes should not be too deep
☼ Code Smell
Nested blocks of code should not be left empty Code Smell
Functions should not have too many parameters
Code Smell
Unused "private" fields should be removed
Collapsible "if" statements should be merged
☼ Code Smell
OS commands should not be vulnerable to argument injection attacks
■ Vulnerability
Logging should not be vulnerable to

injection attacks

• Vulnerability

Repeated patterns in regular expressions should not match the



Security Hotspot 33

© 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

empty string

Rug

Function and method parameters' initial values should not be ignored

Rug

Having a permissive Cross-Origin Resource Sharing policy is security-sensitive

Security Hotspot

Delivering code in production with debug features activated is security-sensitive

Security Hotspot

Creating cookies without the