Code Smell 144





XML



PHP static code analysis

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

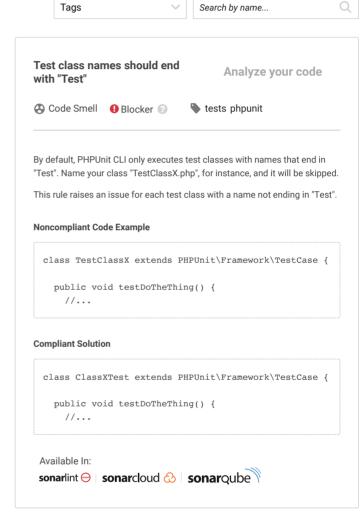
R Bug (51)

| All rules (268) | Vulnerability (40) |
|---|--|
| | |
| Regex lookahe | ead assertions should dictory |
| 👚 Bug | |
| | hould only refer to ups that are matched |
| 👬 Bug | |
| • | ries should not be used can never be matched |
| Rug | |
| | s following a possessive uld not always fail |
| 👚 Bug | |
| Assertion failu | ure exceptions should |
| <table-of-contents> Bug</table-of-contents> | |
| References us should be "uns | sed in "foreach" loops set" |
| 📆 Bug | |
| Using clear-te sensitive | xt protocols is security- |
| Security H | otspot |
| | chive files without source consumption is tive |
| Security He | otspot |
| Signalling pro- | cesses is security- |
| Security H | otspot |
| Configuring lo | ggers is security- |

Security Hotspot

security-sensitive

Using weak hashing algorithms is



Security Hotspot 33

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are rademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. Privacy Policy

Disabling CSRF protections is security-sensitive

Security Hotspot

Using pseudorandom number generators (PRNGs) is security-sensitive

Security Hotspot

Dynamically executing code is security-sensitive

Security Hotspot

Security Hotspot

Security Hotspot

Security Hotspot

Security Hotspot

M Ondo Omeall