

Php PHP PL/I

PL/SQL PL/SQL

Python

RPG RPG

Ruby

Scala

Swift

Terraform

Text

TS TypeScript

T-SQL

VB VB.NET

VB6 VB6

XML XML



PHP static code analysis

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

 ∰ Bug 51

Tags

A new session should be

Security Hotspot 33

Code Smell 144

Search by name...

Expanding archive files without controlling resource consumption is security-sensitive

Security Hotspot

Signalling processes is securitysensitive

Security Hotspot

Configuring loggers is securitysensitive

Security Hotspot

Using weak hashing algorithms is security-sensitive

Security Hotspot

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

`str_replace` should be preferred to `preg_replace`

Code Smell

"default" clauses should be first or last

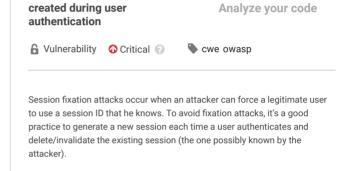
Code Smell

A conditionally executed single line should be denoted by indentation

Code Smell

Conditionals should start on new lines

Code Smell



Noncompliant Code Example

In a Symfony Security's context, session fixation protection can be disabled with the value none for the $session_fixation_strategy$ attribute:

Compliant Solution

In a Symfony Security's context, session fixation protection is enabled by default. It can be explicitly enabled with the values migrate and invalidate for the session_fixation_strategy attribute:

See

- OWASP Top 10 2021 Category A7 Identification and Authentication
 Failures
- OWASP Top 10 2017 Category A2 Broken Authentication
- OWASP Sesssion Fixation
- MITRE, CWE-384 Session Fixation

Available In:

sonarlint ⊕ | sonarcloud 🔂 | sonarqube

Cognitive Complexity of functions should not be too high

Code Smell

Parentheses should not be used for calls to "echo"

Code Smell

Functions should not be nested too deeply

Code Smell

References should not be passed to function calls

Code Smell

"switch" statements should have "default" clauses

© 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