

JavaScript

Objective C

Kotlin

PHP

PL/I

PL/SQL

Python

RPG

Ruby

Scala

Swift

Text

T-SQL

VB.NET

VB6

XML

Terraform

TypeScript

D

月 тѕ

JS



All rules (268)

PHP static code analysis

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

6	Vulnerability	40
6	Vulnerability	(40)

♣ Bug (51)

Tags

Security Hotspot 33

Code Smell (144)

Search by name...

Identical expressions should not be used on both sides of a binary operator

🖟 Bug

All code should be reachable

Loops with at most one iteration should be refactored

🛊 Bug

Short-circuit logic should be used to prevent null pointer dereferences in conditionals

👬 Bug

Variables should not be self-assigned

📆 Bug

Useless "if(true) {...}" and "if(false){...}" blocks should be removed

All "catch" blocks should be able to catch exceptions

📆 Bug

Constructing arguments of system commands from user input is security-sensitive

Security Hotspot

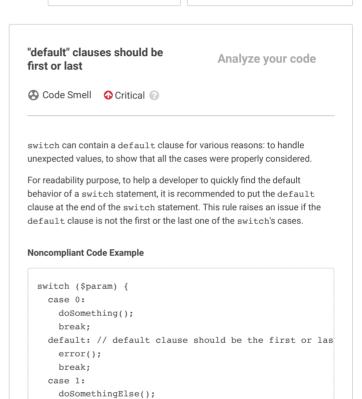
Allowing unfiltered HTML content in WordPress is security-sensitive

Security Hotspot

Allowing unauthenticated database repair in WordPress is securitysensitive

Security Hotspot

Allowing all external requests from a WordPress server is security-sensitive



Compliant Solution

break;

```
switch ($param) {
 case 0:
    doSomething();
   break:
 case 1:
   doSomethingElse();
   break;
 default:
    error();
    break;
```

Available In:

sonarlint ⊕ | sonarcloud ↔ | sonarqube

© 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

Disabling automatic updates is security-sensitive

Security Hotspot

WordPress theme and plugin editors are security-sensitive

Security Hotspot

Allowing requests with excessive content length is security-sensitive

Security Hotspot

Manual generation of session ID is security-sensitive