

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- C#
- CSS
- Flex
- Go
- HTML
- Java
- JavaScript
- Kotlin
- Objective C
- PHP**
- PL/I
- PL/SQL
- Python
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML



PHP static code analysis

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

All rules **268**

Vulnerability **40**

Bug **51**

Security Hotspot **33**

Code Smell **144**

Tags

Search by name...



Regex lookahead assertions should not be contradictory



Back references in regular expressions should only refer to capturing groups that are matched before the reference



Regex boundaries should not be used in a way that can never be matched



Regex patterns following a possessive quantifier should not always fail



Assertion failure exceptions should not be ignored



References used in "foreach" loops should be "unset"



Using clear-text protocols is security-sensitive



Expanding archive files without controlling resource consumption is security-sensitive



Signalling processes is security-sensitive



Configuring loggers is security-sensitive



Using weak hashing algorithms is security-sensitive

Test class names should end with "Test"

Analyze your code

Code Smell Blocker tests phpunit

By default, PHPUnit CLI only executes test classes with names that end in "Test". Name your class "TestClassX.php", for instance, and it will be skipped.

This rule raises an issue for each test class with a name not ending in "Test".

Noncompliant Code Example

```
class TestClassX extends PHPUnit\Framework\TestCase {  
  
    public void testDoTheThing() {  
        //...  
    }  
}
```

Compliant Solution

```
class ClassXTest extends PHPUnit\Framework\TestCase {  
  
    public void testDoTheThing() {  
        //...  
    }  
}
```





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](#)

 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
<code>`str_replace`</code> should be preferred to <code>`preg_replace`</code> 