

- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- 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... 🔍

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	Code Smell
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 empty string	Bug
Function and method parameters' initial values should not be ignored	Bug
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

A "for" loop update clause should move the counter in the right direction

Analyze your code

Bug Major ?

A `for` loop with a counter that moves in the wrong direction is not an infinite loop. Because of wraparound, the loop will eventually reach its stop condition, but in doing so, it will run many, many more times than anticipated, potentially causing unexpected behavior.

Noncompliant Code Example

```
for ($i = 0; $i < $length; $i--) { // Noncompliant
    //...
}
```

Compliant Solution


```
for ($i = 0; $i < $length; $i++) {
    //...
}
```

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](#)


Creating cookies without the "HttpOnly" flag is security-sensitive

 Security Hotspot


Creating cookies without the "secure" flag is security-sensitive

 Security Hotspot

Using hardcoded IP addresses is security-sensitive

 Security Hotspot

Regular expression quantifiers and character classes should be used concisely

 Code Smell

Character classes should be preferred