- 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...

be used to end lines

Code Smell

More than one property should not be declared per statement

Code Smell

The "var" keyword should not be used

Code Smell

"<?php" and "<?=" tags should be used

Code Smell

File names should comply with a naming convention

Code Smell

Comments should not be located at the end of lines of code

Code Smell

Local variable and function parameter names should comply with a naming convention

Code Smell

Field names should comply with a

naming convention

Code Smell

Lines should not end with trailing whitespaces

Code Smell

Files should contain an empty newline at the end

Code Smell

Modifiers should be declared in the correct order

Code Smell

An open curly brace should be located at the beginning of a line

"file_uploads" should be disabled

Analyze your code

Vulnerability   Blocker

`file_uploads` is an on-by-default PHP configuration that allows files to be uploaded to your site. Since accepting candy files from strangers is inherently dangerous, this feature should be disabled unless it is absolutely necessary for your site.

This rule raises an issue when `file_uploads` is not explicitly disabled.

Noncompliant Code Example

```
; php.ini
file_uploads=1  ; Noncompliant
```

Compliant Solution

```
; php.ini
file_uploads=0
```

See

- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- MITRE, CWE-434 - Unrestricted Upload of File with Dangerous Type
- SANS Top 25 - Insecure Interaction Between Components

Deprecated

This rule is deprecated, and will eventually be removed.

Available In:

sonarlint | sonarcloud | sonarqube

Code Smell

An open curly brace should be located at the end of a line

Code Smell

Tabulation characters should not be used

Code Smell

Method and function names should comply with a naming convention

Code Smell

Creating cookies with broadly defined "domain" flags is security-sensitive

Security Hotspot