sonar RULES

Products

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...

Cryptographic keys should be robust
Vulnerability

Weak SSL/TLS protocols should not be used
Vulnerability

Regular expressions should not be vulnerable to Denial of Service attacks
Vulnerability

Hashes should include an unpredictable salt
Vulnerability

Regular expressions should have valid delimiters
Bug

Regex lookahead assertions should not be contradictory
Bug

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

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

Regex patterns following a possessive quantifier should not always fail
Bug

Assertion failure exceptions should not be ignored
Bug

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

"$this" should not be used in a static context

Analyze your code

Bug Blocker

`$this` refers to the current class instance. But static methods can be accessed without instantiating the class, and `$this` is not available to them. Using `$this` in a static context will result in a fatal error at runtime.

Noncompliant Code Example

```
class Clazz {
  $name=NULL;  // instance variable

  public static function foo(){
    if ($this->name != NULL) {
      // ...
    }
  }
}
```

Compliant Solution

```
class Clazz {
  $name=NULL;  // instance variable

  public static function foo($nameParam){
    if ($nameParam != NULL) {
      // ...
    }
  }
}
```

Available In:

sonarlint | sonarcloud | sonarqube

Using clear-text protocols is security-sensitive

Security Hotspot

Expanding archive files without controlling resource consumption is security-sensitive

Security Hotspot

Signalling processes is security-sensitive

Security Hotspot

Configuring loggers is security-sensitive

Security Hotspot