

- 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...

Functions and variables should not be defined outside of classes	Code Smell
Track lack of copyright and license headers	Code Smell
Octal values should not be used	Code Smell
Switch cases should end with an unconditional "break" statement	Code Smell
Session-management cookies should not be persistent	Vulnerability
Cryptographic RSA algorithms should always incorporate OAEP (Optimal Asymmetric Encryption Padding)	Vulnerability
SHA-1 and Message-Digest hash algorithms should not be used in secure contexts	Vulnerability
Assertions should not be made at the end of blocks expecting an exception	Bug
Regular expressions should be syntactically valid	Bug
Only one method invocation is expected when testing exceptions	Bug
Reading the Standard Input is security-sensitive	Security Hotspot

"goto" statement should not be used

Analyze your code

Code Smell

Major ?

brain-overload

goto is an unstructured control flow statement. It makes code less readable and maintainable. Structured control flow statements such as if, for, while, continue or break should be used instead.

Noncompliant Code Example

```
$i = 0;
loop:
echo("i = $i");
$i++;
if ($i < 10){
    goto loop;
}
```

Compliant Solution

```
for ($i = 0; $i < 10; $i++){
    echo("i = $i");
}
```


Available In:

sonarlint

sonarcloud

sonarqube


Using command line arguments is security-sensitive

 Security Hotspot


Using Sockets is security-sensitive

 Security Hotspot

Encrypting data is security-sensitive

 Security Hotspot

Using regular expressions is security-sensitive

 Security Hotspot

Deserializing objects from an untrusted source is security-sensitive

 Security Hotspot