

- 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... 🔍

| |
|--|
| demimters |
| <div>Bug</div> |
| Regex lookahead assertions should not be contradictory |
| <div>Bug</div> |
| Back references in regular expressions should only refer to capturing groups that are matched before the reference |
| <div>Bug</div> |
| Regex boundaries should not be used in a way that can never be matched |
| <div>Bug</div> |
| Regex patterns following a possessive quantifier should not always fail |
| <div>Bug</div> |
| Assertion failure exceptions should not be ignored |
| <div>Bug</div> |
| References used in "foreach" loops should be "unset" |
| <div>Bug</div> |
| Using clear-text protocols is security-sensitive |
| <div>Security Hotspot</div> |
| Expanding archive files without controlling resource consumption is security-sensitive |
| <div>Security Hotspot</div> |
| Signalling processes is security-sensitive |
| <div>Security Hotspot</div> |
| Configuring loggers is security-sensitive |
| <div>Security Hotspot</div> |

Hard-coded credentials are security-sensitive

Analyze your code

Security Hotspot

Blocker

?

cwe sans-top25 owasp

Because it is easy to extract strings from an application source code or binary, credentials should not be hard-coded. This is particularly true for applications that are distributed or that are open-source.

In the past, it has led to the following vulnerabilities:

- CVE-2019-13466
- CVE-2018-15389

Credentials should be stored outside of the code in a configuration file, a database, or a management service for secrets.

This rule flags instances of hard-coded credentials used in database and LDAP connections. It looks for hard-coded credentials in connection strings, and for variable names that match any of the patterns from the provided list.

It's recommended to customize the configuration of this rule with additional credential words such as "oauthToken", "secret", ...

Ask Yourself Whether

- Credentials allows access to a sensitive component like a database, a file storage, an API or a service.
- Credentials are used in production environments.
- Application re-distribution is required before updating the credentials.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

- Store the credentials in a configuration file that is not pushed to the code repository.
- Store the credentials in a database.
- Use your cloud provider's service for managing secrets.
- If a password has been disclosed through the source code: change it.

Sensitive Code Example


```
$password = "65DBGgwe4uazdWQA"; // Sensitive

$httpUrl = "https://example.domain?user=user&password=65DBGgwe4uazdWQA";
$sshUrl = "ssh://user:65DBGgwe4uazdWQA@example.domain"
```


Compliant Solution

```
$user = getUser();
$password = getPassword(); // Compliant
```


Using weak hashing algorithms is security-sensitive

 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

```
$httpUrl = "https://example.domain?user=$user&password=$password"
$sshUrl = "ssh://$user:$password@example.domain" // Com
```

See

- [OWASP Top 10 2021 Category A7](#) - Identification and Authentication Failures
- [OWASP Top 10 2017 Category A2](#) - Broken Authentication
- [MITRE, CWE-798](#) - Use of Hard-coded Credentials
- [MITRE, CWE-259](#) - Use of Hard-coded Password
- [SANS Top 25](#) - Porous Defenses
- Derived from FindSecBugs rule [Hard Coded Password](#)

Available In:

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](#)