sonar RULES

Products

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...

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

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

`str_replace` should be preferred to `preg_replace`

Code Smell

"default" clauses should be first or last

Code Smell

A conditionally executed single line should be denoted by indentation

Code Smell

Conditionals should start on new lines

Code Smell

A new session should be created during user authentication

Analyze your code

Vulnerability | Critical | cwe owasp

Session fixation attacks occur when an attacker can force a legitimate user to use a session ID that he knows. To avoid fixation attacks, it’s a good practice to generate a new session each time a user authenticates and delete/invalidate the existing session (the one possibly known by the attacker).

Noncompliant Code Example

In a Symfony Security's context, session fixation protection can be disabled with the value `none` for the `session_fixation_strategy` attribute:

```
namespace Symfony\Component\DependencyInjection\Loader\

return static function (ContainerConfigurator $containe
    $container->extension('security', [
        'session_fixation_strategy' => 'none', // Nonco
    ]);
};
```

Compliant Solution

In a Symfony Security's context, session fixation protection is enabled by default. It can be explicitly enabled with the values `migrate` and `invalidate` for the `session_fixation_strategy` attribute:

```
namespace Symfony\Component\DependencyInjection\Loader\

return static function (ContainerConfigurator $containe
    $container->extension('security', [
        'session_fixation_strategy' => 'migrate', // Co
    ]);
};
```

See

- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
- OWASP Top 10 2017 Category A2 - Broken Authentication
- OWASP Sesssion Fixation
- MITRE, CWE-384 - Session Fixation

Available In:

sonarlint | sonarcloud | sonarqube

Cognitive Complexity of functions should not be too high

Code Smell

Parentheses should not be used for calls to "echo"

Code Smell

Functions should not be nested too deeply

Code Smell

References should not be passed to function calls

Code Smell

"switch" statements should have "default" clauses