

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...



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

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

Encryption algorithms should be used with secure mode and padding scheme

Analyze your code

Vulnerability Critical cwe privacy owasp sans-top25

Encryption operation mode and the padding scheme should be chosen appropriately to guarantee data confidentiality, integrity and authenticity:

- For block cipher encryption algorithms (like AES):
 - The GCM (Galois Counter Mode) mode which **works internally** with zero/no padding scheme, is recommended, as it is designed to provide both data authenticity (integrity) and confidentiality. Other similar modes are CCM, CWC, EAX, IAPM and OCB.
 - The CBC (Cipher Block Chaining) mode by itself provides only data confidentiality, it's recommended to use it along with Message Authentication Code or similar to achieve data authenticity (integrity) too and thus to **prevent padding oracle attacks**.
 - The ECB (Electronic Codebook) mode doesn't provide serious message confidentiality: under a given key any given plaintext block always gets encrypted to the same ciphertext block. This mode should not be used.
- For RSA encryption algorithm, the recommended padding scheme is OAEP.

Noncompliant Code Example

```
$c01 = mcrypt_encrypt(MCRYPT_DES, $key, $plaintext, "ecb");
$c02 = mcrypt_encrypt(MCRYPT_DES_COMPAT, $key, $plaintext, "ecb");
$c03 = mcrypt_encrypt(MCRYPT_TRIPLEDDES, $key, $plaintext, "ecb");
$c04 = mcrypt_encrypt(MCRYPT_3DES, $key, $plaintext, "ecb");
$c05 = mcrypt_encrypt(MCRYPT_BLOWFISH, $key, $plaintext, "ecb");
$c06 = mcrypt_encrypt(MCRYPT_RC2, $key, $plaintext, "ecb");
$c07 = mcrypt_encrypt(MCRYPT_RC4, $key, $plaintext, "ecb");

function encrypt1($data, $key) {
    $scripted='';
    openssl_public_encrypt($data, $scripted, $key, OPENSSL_NO_PADDING);
    return $scripted;
}
```

```
$c1 = openssl_encrypt($plaintext, "BF-ECB", $key, $options=0);
$c2 = openssl_encrypt($plaintext, "RC2-ECB", $key, $options=0);
$c3 = openssl_encrypt($plaintext, "bf-ecb", $key, $options=0);
$c4 = openssl_encrypt($plaintext, "des-ecb", $key, $options=0);
$c5 = openssl_encrypt($plaintext, "rc2-ecb", $key, $options=0);
```

Compliant Solution


```
$c6 = openssl_encrypt($plaintext, "aes-256-gcm", $key, $options=0);

function encrypt2($data, $key) {
    $scripted='';
    openssl_public_encrypt($data, $scripted, $key, OPENSSL_PKCS1_PADDING);
    return $scripted;
}
```


References should not be passed to function calls

 Code Smell

"switch" statements should have "default" clauses

 Code Smell

Control structures should use curly braces

 Code Smell

String literals should not be duplicated

 Code Smell

See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [MITRE, CWE-327](#) - Use of a Broken or Risky Cryptographic Algorithm
- [SANS Top 25](#) - Porous Defenses

Available In:

sonarlint  | **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](#)