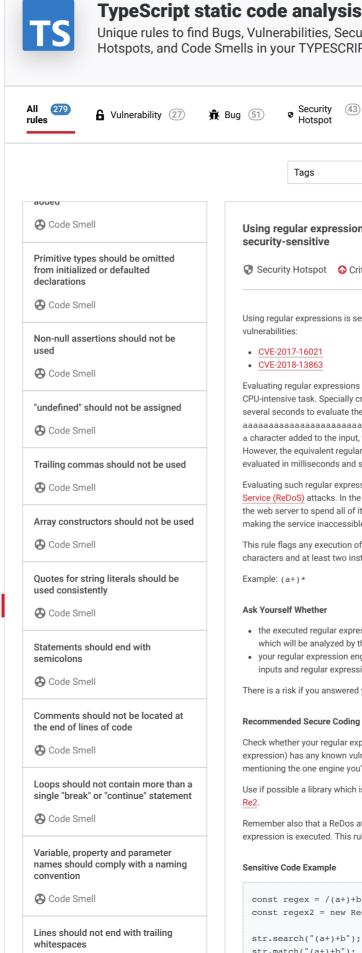
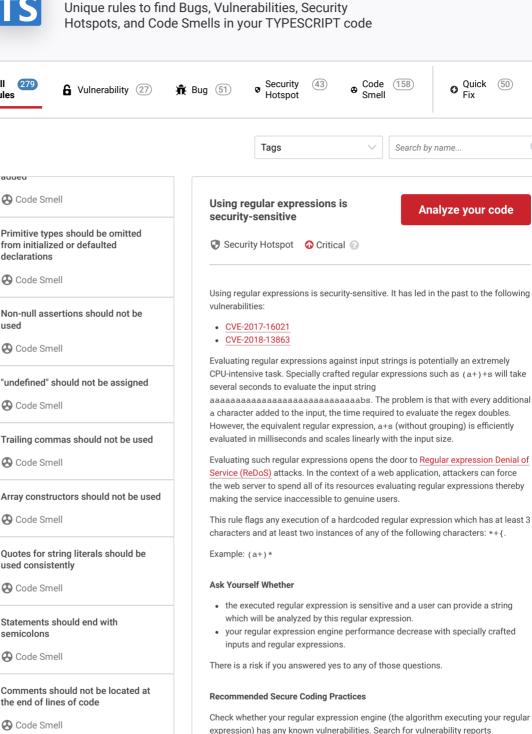


Products ✓







Use if possible a library which is not vulnerable to Redos Attacks such as Google

Remember also that a ReDos attack is possible if a user-provided regular expression is executed. This rule won't detect this kind of injection.

mentioning the one engine you're are using.

Sensitive Code Example

Code Smell

Files should contain an empty newline at the end

Code Smell

An open curly brace should be located at the end of a line

A Code Smell

Tabulation characters should not be used

Code Smell

Function and method names should comply with a naming convention

Code Smell

Note: String.matchAll does not raise any issue as it is not supported by NodeJS.

## Exceptions

Some corner-case regular expressions will not raise an issue even though they might be vulnerable. For example: (a  $|aa\rangle$ +, (a  $|a?\rangle$ +.

It is a good idea to test your regular expression if it has the same pattern on both side of a "  $\mid$  ".

## See

- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-624 Executable Regular Expression Error
- OWASP Regular expression Denial of Service ReDoS

## Deprecated

This rule is deprecated; use {rule:javascript:S5852} instead.

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