

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

**TypeScript**

T-SQL

VB.NET

VB6

XML

TS

TypeScript static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your TYPESCRIPT code

All rules279

Vulnerability27

Bug51

Security Hotspot43

Code Smell158

Quick Fix50

Tags

Search by name...

Code Smell

Function call arguments should not start on new lines

Code Smell

"switch" statements should have at least 3 "case" clauses

Code Smell

A "while" loop should be used instead of a "for" loop

Code Smell

Unnecessary imports should be removed

Code Smell

Boolean literals should not be used in comparisons

Code Smell

Extra semicolons should be removed

Code Smell

Class names should comply with a naming convention

Code Smell

Track uses of "TODO" tags

Code Smell

Web SQL databases should not be used

Vulnerability

Variables declared with "var" should be declared before they are used

Code Smell

Track lack of copyright and license headers

Code Smell

Reading the Standard Input is security-sensitive

Regular expressions should not contain multiple spaces

Analyze your code

Code Smell

Major

regex

Multiple spaces in a regular expression can make it hard to tell how many spaces should be matched. It's more readable to use only one space and then indicate with a quantifier how many spaces are expected.

Noncompliant Code Example

const pattern = /Hello,    world!;/;

Compliant Solution

const pattern = /Hello, {3}world!;/;

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](#)

https://rules.sonarsource.com/typescript/RSPEC-6326

1/2

 Security Hotspot
<b>Using command line arguments is security-sensitive</b>  Security Hotspot
<b>Using Sockets is security-sensitive</b>  Security Hotspot
<b>Executing XPath expressions is security-sensitive</b>  Security Hotspot
<b>Encrypting data is security-sensitive</b>  Security Hotspot