sonar RULES

Products

- 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
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML

JavaScript static code analysis

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

All rules 285 | Vulnerability 29 | Bug 62 | Security Hotspot 43 | Code Smell 151 | Quick Fix 41

Tags | Search by name...

- Assignments should not be made from within sub-expressions — Code Smell
- Labels should not be used — Code Smell
- Variables should not be shadowed — Code Smell
- Redundant pairs of parentheses should be removed — Code Smell
- Nested blocks of code should not be left empty — Code Smell
- Functions should not have too many parameters — Code Smell
- OS commands should not be vulnerable to argument injection attacks — Vulnerability
- Repeated patterns in regular expressions should not match the empty string — Bug
- Empty collections should not be accessed or iterated — Bug
- "delete" should be used only with object properties — Bug
- "with" statements should not be used — Bug
- Function parameters, caught exceptions and foreach variables'

Strict equality operators should not be used with dissimilar types

Analyze your code

Bug | Major | Quick Fix

Comparing dissimilar types using the strict equality operators `===` and `!==` will always return the same value, respectively `false` and `true`, because no type conversion is done before the comparison. Thus, such comparisons can only be bugs.

Noncompliant Code Example

```
var a = 8;
var b = "8";

if (a === b) {  // Noncompliant; always false
  // ...
}
```

Compliant Solution

```
var a = 8;
var b = "8";

if (a == b) {
  // ...
}
```

or

```
var a = 8;
var b = "8";

if (a === Number(b)) {
  // ...
}
```

Available In:

sonarlint | sonarcloud | sonarqube

initial values should not be ignored

Bug

Forwarding client IP address is security-sensitive

Security Hotspot

Allowing confidential information to be logged is security-sensitive

Security Hotspot

Allowing browsers to perform DNS prefetching is security-sensitive

Security Hotspot

Disabling Certificate Transparency