TypeScript static code analysis

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

Empty collections should not be accessed or iterated
Bug

"delete" should be used only with object properties
Bug

Function parameters, caught exceptions and foreach variables' 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 monitoring is security-sensitive
Security Hotspot

Disabling Strict-Transport-Security policy is security-sensitive
Security Hotspot

Disabling strict HTTP no-referrer policy is security-sensitive
Security Hotspot

Allowing browsers to sniff MIME types is security-sensitive
Security Hotspot

Disabling content security policy frame-ancestors directive is security-sensitive
Security Hotspot

A "for" loop update clause should move the counter in the right direction

Analyze your code

Bug Major

A `for` loop with a stop condition that can never be reached, such as one with a counter that moves in the wrong direction, will run infinitely. While there are occasions when an infinite loop is intended, the convention is to construct such loops as `while` loops. More typically, an infinite `for` loop is a bug.

Noncompliant Code Example

```
for (var i = 0; i < strings.length; i--) { // Noncompliant;
  //...
}
```

Compliant Solution

```
for (var i = 0; i < strings.length; i++) {
  //...
}
```

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

Allowing mixed-content is security-sensitive

Security Hotspot

Disabling content security policy fetch directives is security-sensitive

Security Hotspot

Disabling resource integrity features is security-sensitive

Security Hotspot

Disclosing fingerprints from web application technologies is security-sensitive

Security Hotspot