Security

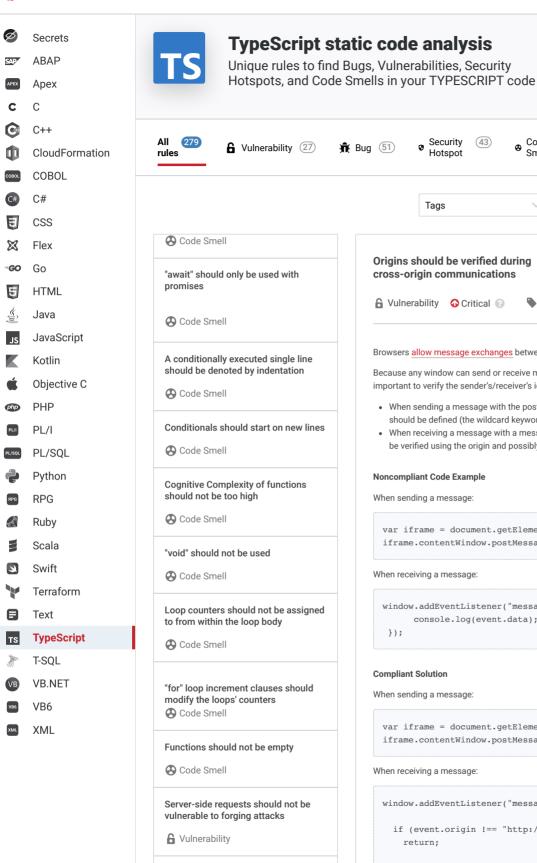
Hotspot

Tags



Products ✓

O Quick 50 Fix



```
6 Vulnerability (27)
                                         # Bug (51)
"await" should only be used with
A conditionally executed single line
should be denoted by indentation
Conditionals should start on new lines
Cognitive Complexity of functions
"void" should not be used
Loop counters should not be assigned
to from within the loop body
"for" loop increment clauses should
modify the loops' counters
Functions should not be empty
Server-side requests should not be
vulnerable to forging attacks
Non-empty statements should change
control flow or have at least one side-
effect
👬 Bug
Regular expressions with the global
flag should be used with caution
R Bug
```

```
Origins should be verified during
                                             Analyze your code
cross-origin communications
cwe html5 owasp
Browsers allow message exchanges between Window objects of different origins.
Because any window can send or receive messages from another window, it is
important to verify the sender's/receiver's identity:
 • When sending a message with the postMessage method, the identity's receiver
   should be defined (the wildcard keyword (*) should not be used)
 . When receiving a message with a message event, the sender's identity should
   be verified using the origin and possibly source properties.
Noncompliant Code Example
When sending a message:
 var iframe = document.getElementById("testiframe");
 iframe.contentWindow.postMessage("secret", "*"); // Noncompl
When receiving a message:
 window.addEventListener("message", function(event) { // Nonc
        console.log(event.data);
Compliant Solution
When sending a message:
  var iframe = document.getElementById("testsecureiframe");
 iframe.contentWindow.postMessage("hello", "https://secure.ex
When receiving a message:
 window.addEventListener("message", function(event) {
    if (event.origin !== "http://example.org") // Compliant
    console.log(event.data)
 });
See
  OWASP Top 10 2021 Category A1 - Broken Access Control
```

OWASP Top 10 2017 Category A3 - Broken Authentication and Session

MITRE, CWE-345 - Insufficient Verification of Data Authenticity

developer.mozilla.org - postMessage API

⊗ Code

Smell

(158)

Search by name.

TypeScript static code analysis керпасетель strings snould reference existing regular expression groups

Вид

Regular expressions should not contain control characters

Вид

Alternation in regular expressions should not contain empty alternatives

Вид

Мосhа timeout should be disabled by setting it to "0".



© 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