Security

Hotspot

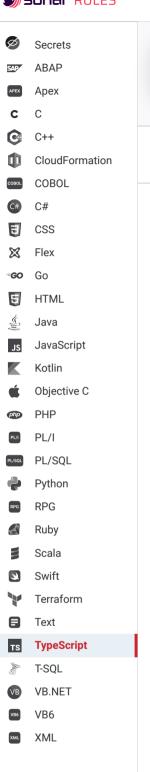
Tags

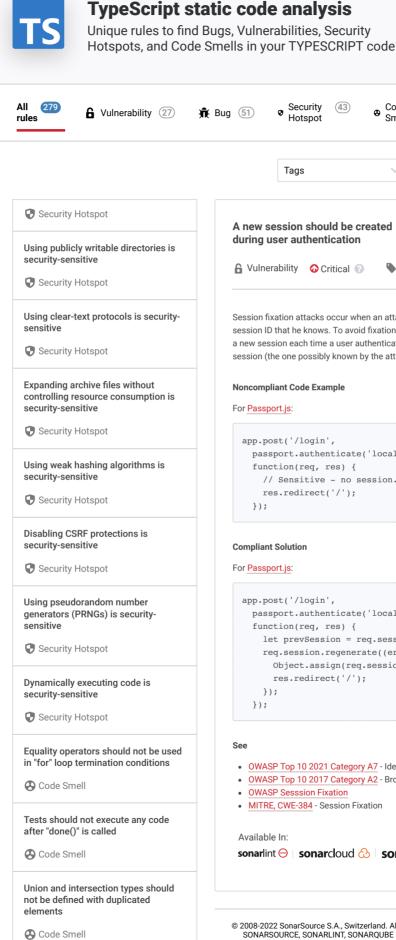
(43)



Products >

O Quick 50 Fix





"default" clauses should be last

```
A new session should be created
                                             Analyze your code
during user authentication
cwe owasp
Session fixation attacks occur when an attacker can force a legitimate user to use a
session ID that he knows. To avoid fixation attacks, it's a good practice to generate
a new session each time a user authenticates and delete/invalidate the existing
session (the one possibly known by the attacker).
Noncompliant Code Example
For Passport.js:
 app.post('/login',
    passport.authenticate('local', { failureRedirect: '/login'
    function(req, res) {
      // Sensitive - no session.regenerate after login
      res.redirect('/');
    });
Compliant Solution
For Passport.js:
 app.post('/login',
    passport.authenticate('local', { failureRedirect: '/login'
    function(req, res) {
      let prevSession = req.session;
      req.session.regenerate((err) => { // Compliant
        Object.assign(req.session, prevSession);
        res.redirect('/'):
      });
    });
See
 • OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
 • OWASP Top 10 2017 Category A2 - Broken Authentication
   OWASP Sesssion Fixation
 • MITRE, CWE-384 - Session Fixation
 Available In:
 sonarlint ⊕ | sonarcloud 🔂 | sonarqube
```

⊗ Code

Smell

(158)

Search by name.

© 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

"await" should only be used with promises
<b>⊘</b> Code Smell
A conditionally executed single line should be denoted by indentation  Code Smell
Conditionals should start on new lines  Code Smell
Cognitive Complexity of functions should not be too high