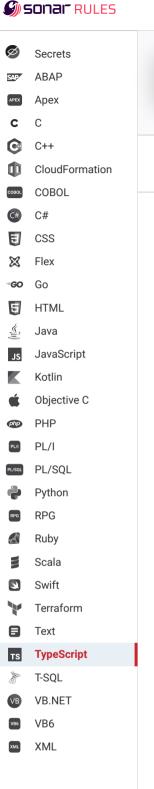
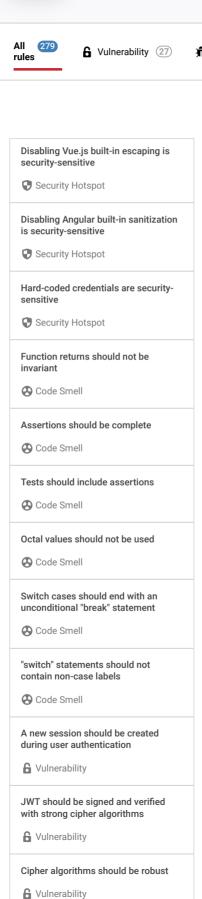
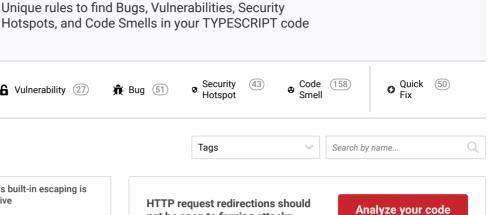
TypeScript static code analysis



Products >







```
injection cwe sans-top25 owasp
User-provided data, such as URL parameters, POST data payloads, or cookies,
should always be considered untrusted and tainted. Applications performing HTTP
redirects based on tainted data could enable an attacker to redirect users to a
malicious site to, for example, steal login credentials.
This problem could be mitigated in any of the following ways:
 · Validate the user-provided data based on an allowlist and reject input not
```

• Redesign the application to not perform redirects based on user-provided data.

Noncompliant Code Example

not be open to forging attacks

```
function redirect(reg, res) {
 const url = req.query.url; // user-controlled input
  res.redirect(url); // Noncompliant
function setLocationHeader(req, res) {
 const url = req.query.url; // user-controlled input
 res.location(url); // Noncompliant
  res.sendStatus(302);
```

Compliant Solution

Validate the URL with an allowlist:

```
function isValidUrl(url) {
 if(url.startsWith("https://www.safe.com/")) {
    return true;
 return false;
function redirect(req, res) {
 const url = req.query.url; // user-controlled input
 if(isValidUrl(url)) {
    res.redirect(url); // Compliant
}
```

• OWASP Top 10 2021 Category A1 - Broken Access Control

TypeScript static code analysis: HTTP request redirections should not be open to forging attacks

TypeScript static code analysis
Encryption algorithms should be used with secure mode and padding scheme

Vulnerability

Server hostnames should be verified during SSL/TLS connections

Vulnerability

Server certificates should be verified during SSL/TLS connections

Vulnerability

Cryptographic keys should be robust

Vulnerability

OWASP Top 10 2017 Category A5 - Broken Access Control

MITRE, CWE-20 - Improper Input Validation

MITRE, CWE-601 - URL Redirection to Untrusted Site ('Open Redirect')

SANS Top 25 - Risky Resource Management

Available In:

sonarcloud & sonarqube Developer Edition

© 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