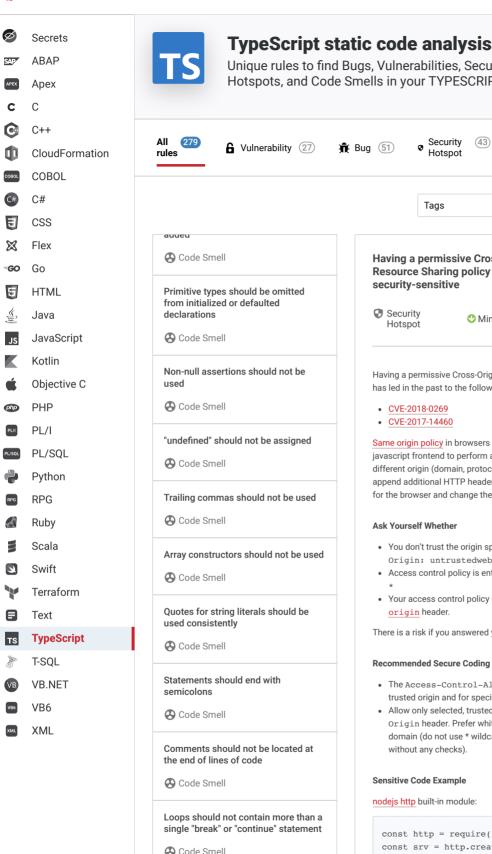
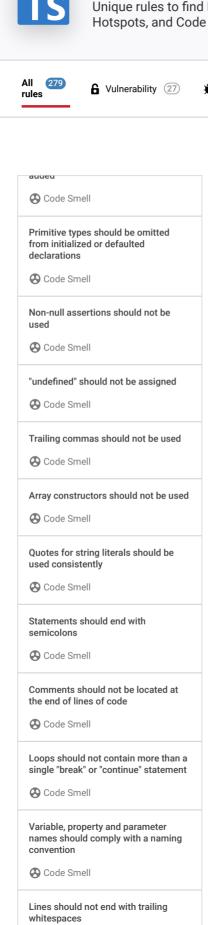
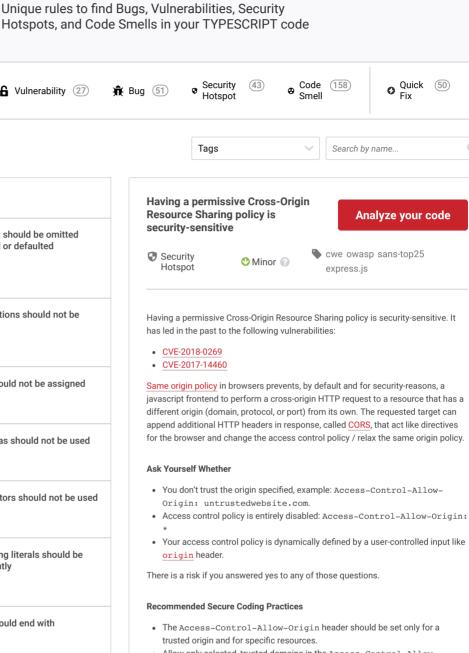


Products >

Q







- · Allow only selected, trusted domains in the Access-Control-Allow-Origin header. Prefer whitelisting domains over blacklisting or allowing any domain (do not use \* wildcard nor blindly return the Origin header content without any checks).

## Sensitive Code Example

nodejs http built-in module:

```
const http = require('http');
const srv = http.createServer((req, res) => {
  res.writeHead(200, { 'Access-Control-Allow-Origin': '*' })
  res.end('ok');
});
srv.listen(3000);
```

Express.js framework with cors middleware:

```
const cors = require('cors');
let app1 = express();
appl.use(cors()); // Sensitive: by default origin is set to
```

Code Smell

Files should contain an empty newline at the end

Code Smell

An open curly brace should be located at the end of a line

Code Smell

Tabulation characters should not be used

Code Smell

Function and method names should comply with a naming convention

Code Smell

```
let corsOptions = {
  origin: '*' // Sensitive
};
let app2 = express();
app2.use(cors(corsOptions));
```

User-controlled origin:

```
function (req, res) {
  const origin = req.header('Origin');
  res.setHeader('Access-Control-Allow-Origin', origin); // S
};
```

## **Compliant Solution**

nodejs http built-in module:

```
const http = require('http');
const srv = http.createServer((req, res) => {
  res.writeHead(200, { 'Access-Control-Allow-Origin': 'trust
  res.end('ok');
});
srv.listen(3000);
```

Express.js framework with cors middleware:

```
const cors = require('cors');
let corsOptions = {
  origin: 'trustedwebsite.com' // Compliant
};
let app = express();
app.use(cors(corsOptions));
```

User-controlled origin validated with an allow-list:

```
function (req, res) {
  const origin = req.header('Origin');

if (trustedOrigins.indexOf(origin) >= 0) {
   res.setHeader('Access-Control-Allow-Origin', origin);
  }
};
```

## See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2021 Category A7 Identification and Authentication Failures
- developer.mozilla.org CORS
- developer.mozilla.org Same origin policy
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- OWASP HTML5 Security Cheat Sheet Cross Origin Resource Sharing
- MITRE, CWE-346 Origin Validation Error
- MITRE, CWE-942 Overly Permissive Cross-domain Whitelist
- SANS Top 25 Porous Defenses

Available In:

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