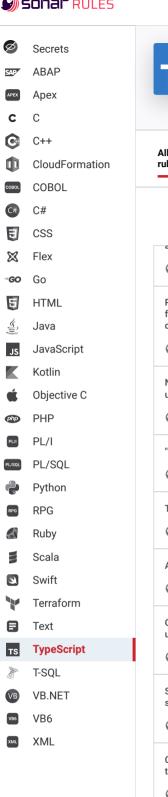
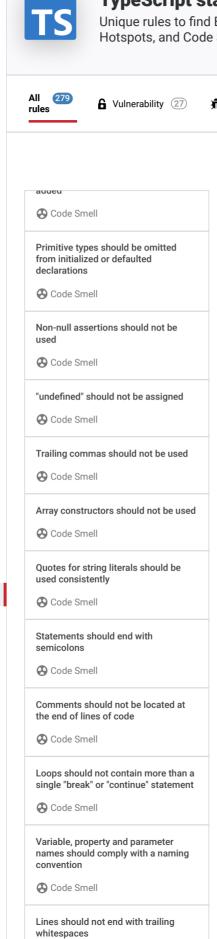
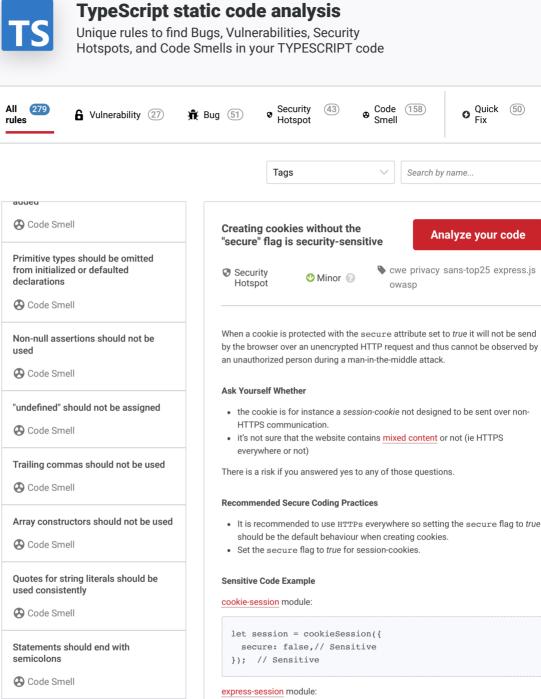


Products >

Q







```
const express = require('express');
const session = require('express-session');
let app = express():
app.use(session({
 cookie:
    secure: false // Sensitive
}));
```

cookies module:

```
let cookies = new Cookies(req, res, { keys: keys });
cookies.set('LastVisit', new Date().toISOString(), {
 secure: false // Sensitive
}); // Sensitive
```

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

csurf module:

```
const cookieParser = require('cookie-parser');
const csrf = require('csurf');
const express = require('express');
let csrfProtection = csrf({ cookie: { secure: false }}); //
```

Compliant Solution

cookie-session module:

```
let session = cookieSession({
  secure: true,// Compliant
}); // Compliant
```

express-session module:

```
const express = require('express');
const session = require('express-session');

let app = express();
app.use(session({
   cookie:
   {
      secure: true // Compliant
   }
}));
```

cookies module:

```
let cookies = new Cookies(req, res, { keys: keys });
cookies.set('LastVisit', new Date().toISOString(), {
   secure: true // Compliant
}); // Compliant
```

csurf module:

```
const cookieParser = require('cookie-parser');
const csrf = require('csurf');
const express = require('express');
let csrfProtection = csrf({ cookie: { secure: true }}); // C
```

See

- OWASP Top 10 2021 Category A4 Insecure Design
- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- MITRE, CWE-311 Missing Encryption of Sensitive Data
- MITRE, CWE-315 Cleartext Storage of Sensitive Information in a Cookie
- $\bullet \quad \underline{\text{MITRE, CWE-614}} \text{ Sensitive Cookie in HTTPS Session Without 'Secure' Attribute} \\$
- 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