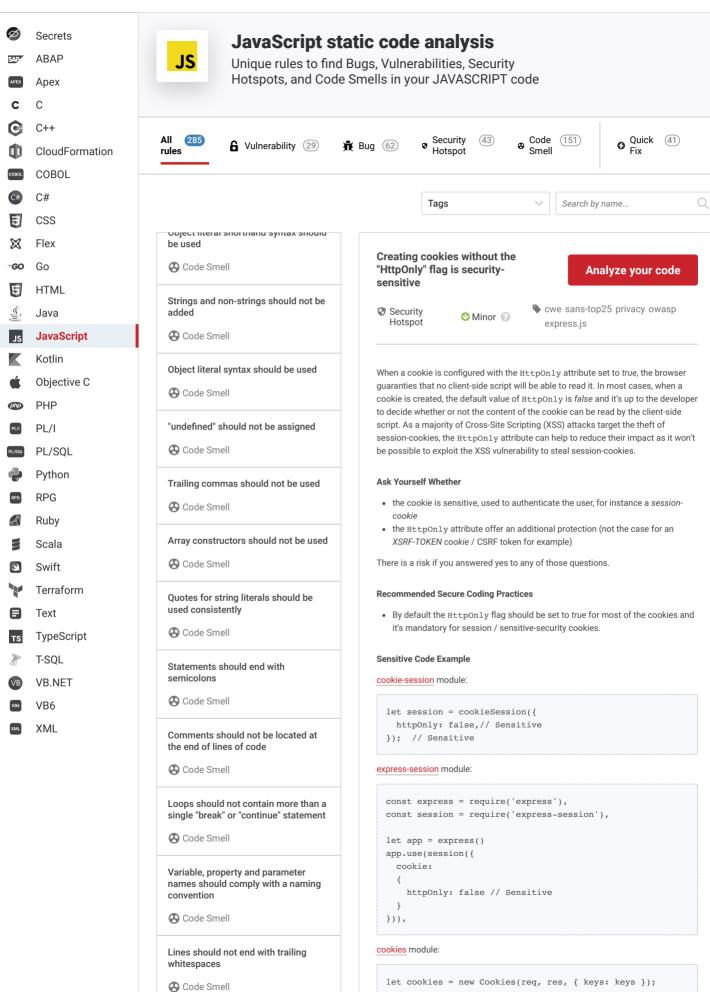


Products ✓



cookies.set('LastVisit', new Date().toISOString(), {

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

```
httpOnly: false // Sensitive
}); // Sensitive
```

csurf module:

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

Compliant Solution

cookie-session module:

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

express-session module:

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

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

cookies module:

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

$\underline{\mathsf{csurf}} \ \mathsf{module} :$

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

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP HttpOnly
- OWASP Top 10 2017 Category A7 Cross-Site Scripting (XSS)
- MITRE, CWE-1004 Sensitive Cookie Without 'HttpOnly' Flag
- SANS Top 25 Insecure Interaction Between Components
- Derived from FindSecBugs rule HTTPONLY_COOKIE

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