Security

Hotspot

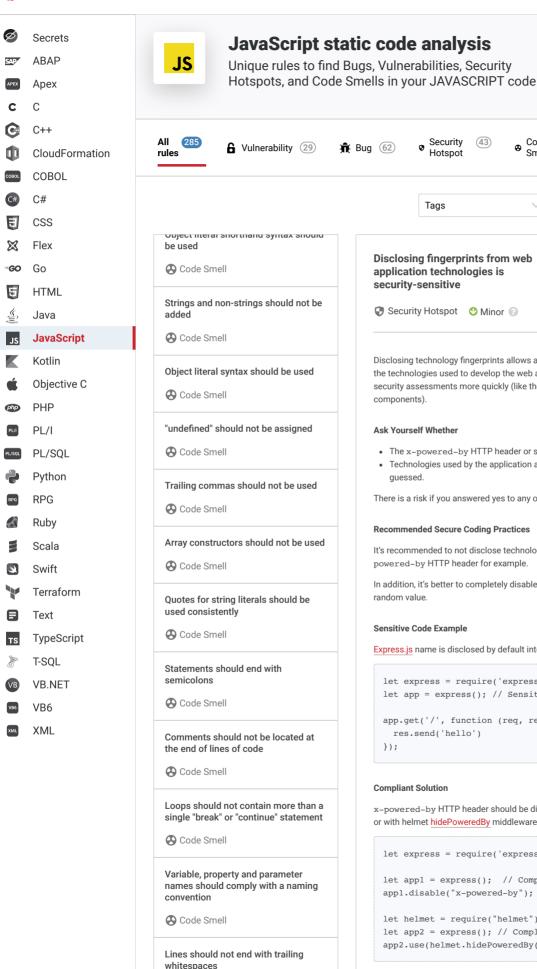
Tags

(43)



Products >

O Quick 41 Fix





Disclosing technology fingerprints allows an attacker to gather information about the technologies used to develop the web application and to perform relevant security assessments more quickly (like the identification of known vulnerable components).

#### Ask Yourself Whether

- The x-powered-by HTTP header or similar is used by the application.
- Technologies used by the application are confidential and should not be easily quessed

There is a risk if you answered yes to any of these questions.

# **Recommended Secure Coding Practices**

It's recommended to not disclose technologies used on a website, with xpowered-by HTTP header for example.

In addition, it's better to completely disable this HTTP header rather than setting it a random value

### Sensitive Code Example

Express.js name is disclosed by default into the x-powered-by HTTP header:

```
let express = require('express');
let app = express(); // Sensitive
app.get('/', function (req, res) {
  res.send('hello')
});
```

## Compliant Solution

x-powered-by HTTP header should be disabled in Express.js with app.disable or with helmet hidePoweredBy middleware:

```
let express = require('express');
let app1 = express(); // Compliant
appl.disable("x-powered-by");
let helmet = require("helmet");
let app2 = express(); // Compliant
app2.use(helmet.hidePoweredBy());
```

### See

• OWASP Top 10 2021 Category A5 - Security Misconfiguration

Code Smell

JavaScript static code analysis: Disclosing fingerprints from web application technologies is security-sensitive

JavaScript static code analysis: Disclor 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

OWASP Testing Guide - OTG-INFO-008 - Fingerprint Web Application Framework
 OWASP Top 10 2017 Category A6 - Security Misconfiguration
 MITRE, CWE-200 - Information Exposure

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