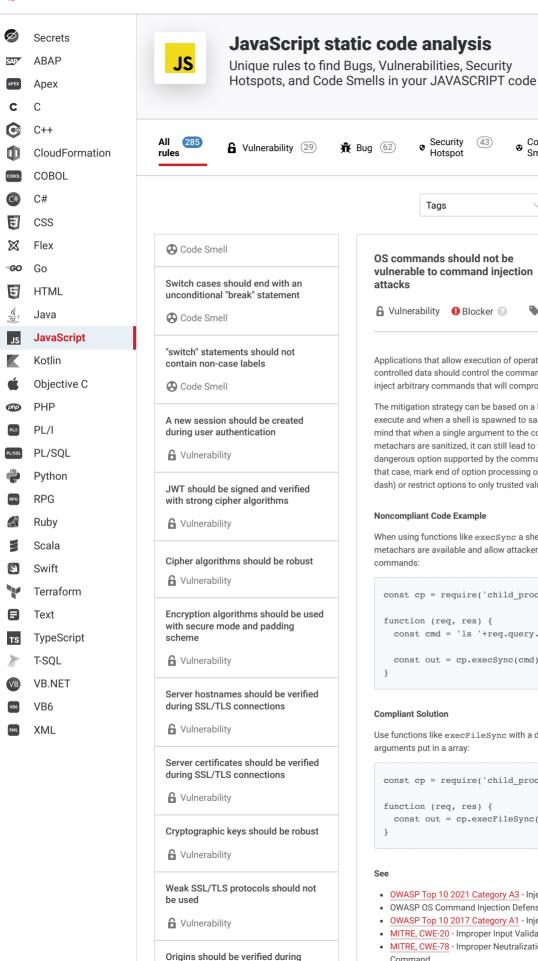
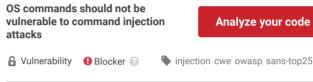


Products ✓





Security

Hotspot

Tags

(43)

Analyze your code

O Quick 41 Fix

Applications that allow execution of operating system commands from usercontrolled data should control the command to execute, otherwise an attacker can inject arbitrary commands that will compromise the underlying operating system.

(151)

Search by name.

The mitigation strategy can be based on a list of authorized and safe commands to execute and when a shell is spawned to sanitize shell meta-characters. Keep in mind that when a single argument to the command is user-controlled and shellmetachars are sanitized, it can still lead to vulnerabilities if the attacker can inject a dangerous option supported by the command, such as -exec available with find, in that case, mark end of option processing on the command line using -- (doubledash) or restrict options to only trusted values.

Noncompliant Code Example

When using functions like execSync a shell is spawn and therefore shell metachars are available and allow attackers to execute additional arbitrary

```
const cp = require('child_process');
function (req, res) {
 const cmd = 'ls '+req.query.arg;
  const out = cp.execSync(cmd); // Noncompliant: example of
```

Compliant Solution

Use functions like execFileSync with a defined command and user-controlled arguments put in a array:

```
const cp = require('child process');
function (req, res) {
  const out = cp.execFileSync("ls", [req.query.arg]); // Com
```

See

- OWASP Top 10 2021 Category A3 Injection
- OWASP OS Command Injection Defense Cheat Sheet
- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-78 Improper Neutralization of Special Elements used in an OS
- SANS Top 25 Insecure Interaction Between Components

Available In:

cross-origin communications

Vulnerability

JavaScript static code analysis: O
Regular expressions should not be vulnerable to Denial of Service attacks
6 Vulnerability
File uploads should be restricted
6 Vulnerability
Function calls should not pass extra arguments
∰ Bug
Regular expressions should be syntactically valid
j n t Bug
Getters and setters should access the

sonarcloud 🐼 | sonarqube | 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