

Secrets

SAP ABAP

Apex Apex

C

C++

CloudFormation

COBOL COBOL

C# C#

CSS

Flex

=GO Go

HTML

Java

JavaScript

Kotlin

Kubernetes

Objective C

Php PHF

PL/I

PL/SQL

Python

Swift

Ruby

Terraform

E Text

Ts TypeScript

T-SQL

VB VB.NET

• \/D.c

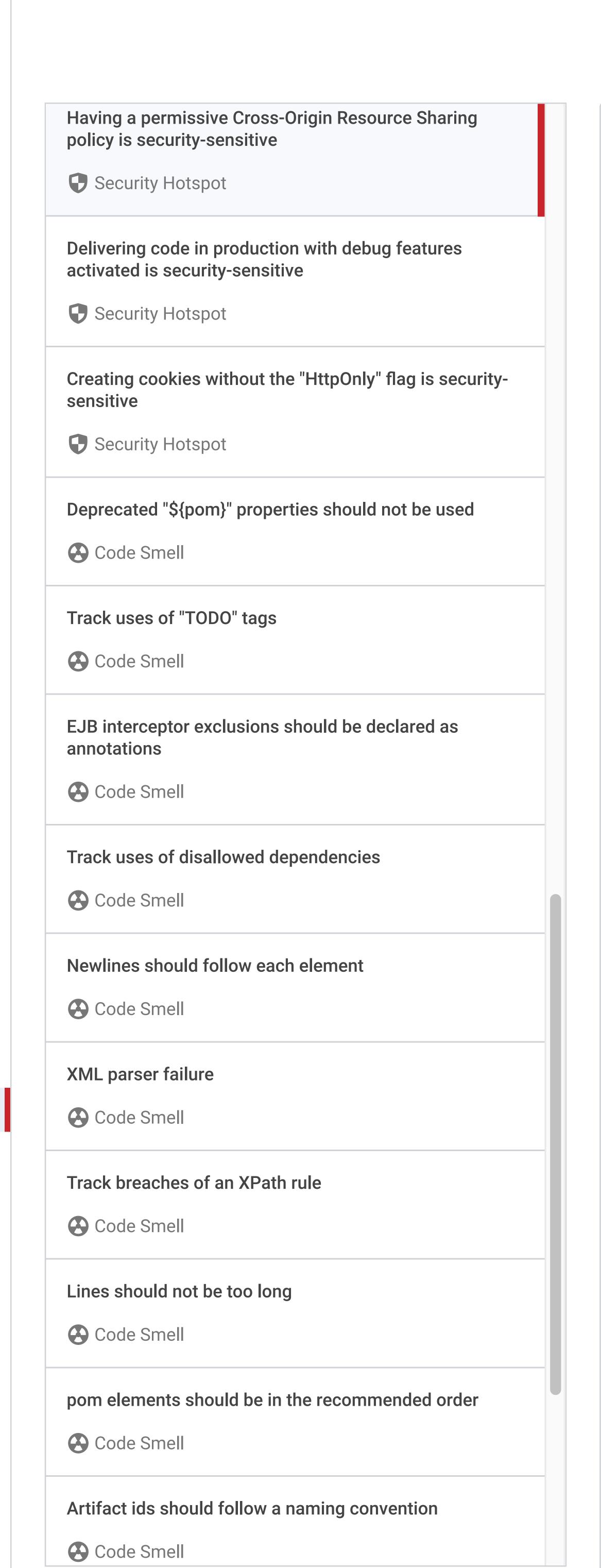
VB6 VB6

XML XML



Unique rules to find Bugs and Code Smells in your XML code







Analyze your code

Search by name...

Having a permissive Cross-Origin Resource Sharing policy is security-sensitive. It has led in the past to the following vulnerabilities:

Tags

• CVE-2018-0269

• CVE-2017-14460

Same origin policy in browsers prevents, by default and for security-reasons, a javascript frontend to perform a cross-origin HTTP request to a resource that has a different origin (domain, protocol, or port) from its own. The requested target can append additional HTTP headers in response, called <u>CORS</u>, that act like directives for the browser and change the access control policy / relax the same origin policy.

Ask Yourself Whether

- You don't trust the origin specified, example: Access-Control-Allow-Origin: untrustedwebsite.com.
- Access control policy is entirely disabled: Access-Control-Allow-Origin: *
- Your access control policy is dynamically defined by a user-controlled input like origin header.

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

Recommended Secure Coding Practices

- The Access-Control-Allow-Origin header should be set only for a trusted origin and for specific resources.
- 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

Compliant Solution

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