Secrets
ABAP
Apex
C
C++
CloudFormation
COBOL
C#
CSS
Flex
Go
HTML
Java
JavaScript
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

<XML/>

XML static code analysis

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

All rules 36 | Vulnerability 6 | Bug 5 | Security Hotspot 9 | Code Smell 16

Tags

Search by name...

Track uses of "FIXME" tags
Code Smell

Custom permissions should not be defined in the 'android.permission' namespace
Vulnerability

Having a permissive Cross-Origin Resource Sharing policy is security-sensitive
Security Hotspot

Delivering code in production with debug features activated is security-sensitive
Security Hotspot

Creating cookies without the "HttpOnly" flag is security-sensitive
Security Hotspot

Deprecated "${pom}" properties should not be used
Code Smell

Track uses of "TODO" tags
Code Smell

EJB interceptor exclusions should be declared as annotations
Code Smell

Track uses of disallowed dependencies
Code Smell

Newlines should follow each element
Code Smell

XML parser failure
Code Smell

Track breaches of an XPath rule
Code Smell

Track uses of "FIXME" tags

Analyze your code

Code Smell | Major | cwe

`FIXME` tags are commonly used to mark places where a bug is suspected, but which the developer wants to deal with later.

Sometimes the developer will not have the time or will simply forget to get back to that tag.

This rule is meant to track those tags and to ensure that they do not go unnoticed.

Noncompliant Code Example

```
<!-- FIXME we should update version to 3.8.1 -->
<dependency>
  <groupId>org.apache.commons</groupId>
  <artifactId>commons-lang3</artifactId>
  <version>3.6</version>
</dependency>
```

See

- MITRE, CWE-546 - Suspicious Comment

Available In:

sonarlint | sonarcloud | sonarqube