

































-  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 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... 🔍

Sections of code should not be commented out	Code Smell
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	

## Sections of code should not be commented out

Analyze your code

- Code Smell
- Major ?
- unused

Programmers should not comment out code as it bloats programs and reduces readability.

Unused code should be deleted and can be retrieved from source control history if required.

Available In:

sonarlint | sonarcloud | sonarqube