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...

Requesting dangerous Android permissions is security-sensitive
Security Hotspot

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

Requesting dangerous Android permissions is security-sensitive

Analyze your code

Security Hotspot | Major | cwe android privacy owasp

Permissions that can have a large impact on user privacy, marked as dangerous or "not for use by third-party applications" by Android, should be requested only if they are really necessary to implement critical features of an application.

Ask Yourself Whether

- It is not sure that `dangerous` permissions requested by the application are really necessary.
- The users are not clearly informed why and when dangerous permissions are requested by the application.

You are at risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

It is recommended to carefully review all the permissions and to use `dangerous` ones only if they are really necessary.

Sensitive Code Example

In AndroidManifest.xml:

```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" /> <!-- Sensitive -->
<uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION" /> <!-- Sensitive -->
```

Compliant Solution

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" /> <!-- Compliant -->
```

See

- OWASP Top 10 2021 Category A1 - Broken Access Control
- Mobile AppSec Verification Standard - Platform Interaction Requirements
- OWASP Mobile Top 10 2016 Category M1 - Improper Platform Usage
- MITRE, CWE-250 - Execution with Unnecessary Privileges
- developer.android.com - App permissions best practices
- Google Play - Privacy, Security, and Deception - Permissions

Available In:

sonarcloud | sonarqube