

Secrets ABAP

Apex

C++

CloudFormation

**COBOL** 

C#

CSS

**=GO** 

HTML

Flex

Go

Java

JavaScript

Kubernetes

Objective C

PL/SQL

Python

Ruby

Swift

Terraform

Text

**TypeScript** 

T-SQL

**VB.NET** 

**XML** 



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

All rules 36

**6** Vulnerability 6







See

Available In:

sonarcloud & sonarqube

developer.android.com - Implementing content provider permissions

OWASP Mobile Top 10 2016 Category M1 - Improper platform usage

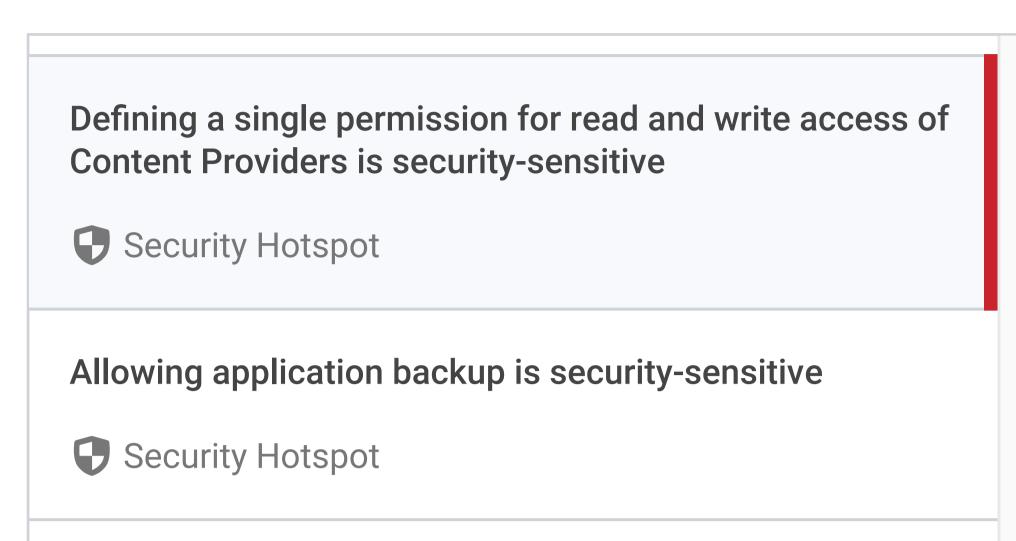
OWASP Mobile Top 10 2016 Category M6 - Insecure Authorization

MITRE, CWE-1220 - Insufficient Granularity of Access Control

Mobile AppSec Verification Standard - Platform Interaction Requirements



Code Smell (16)



Requesting dangerous Android permissions is securitysensitive

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

**6** 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 securitysensitive

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

