


































-  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... 

Allowing application backup is security-sensitive	 Security Hotspot
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

Allowing application backup is security-sensitive

Analyze your code

 Security Hotspot

 Major 

 cwe owasp android

Android has a built-in backup mechanism that can save and restore application data. When application backup is enabled, local data from your application can be exported to Google Cloud or to an external device via `adb backup`. Enabling Android backup exposes your application to disclosure of sensitive data. It can also lead to corruption of local data when restore is performed from an untrusted source.

By default application backup is enabled and it includes:

- Shared preferences files
- Files saved in one of the paths returned by
 - `getDatabasePath(String)`
 - `getFilesDir()`
 - `getDir(String, int)`
 - `getExternalFilesDir(String)`

Ask Yourself Whether

- Application backup is enabled and sensitive data is stored in local files, local databases or shared preferences.
- Your application never validates data from files that are included in backups

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

Recommended Secure Coding Practices

- Disable application backup unless it's required for your application to work properly.
- Narrow the scope of backed-up files by using either
 - backup rules (see `android:fullBackupContent` attribute)
 - a custom `BackupAgent`
 - or the dedicated "no_backup" folder (see `android.content.Context#getNoBackupFilesDir()`).
- Don't backup local data containing sensitive information unless they are properly encrypted.
- Make sure that the keys used to encrypt backup data are not included in the backup.
- Validate data from backed-up files. They should be considered untrusted as they could have been restored from an untrusted source.

Noncompliant Code Example

```
<application
    android:allowBackup="true"> <!-- Sensitive -->
</application>
```

Compliant Solution

Disable application backup.

```
<application
    android:allowBackup="false">
</application>
```

If targeting Android 6.0 or above (API level 23), define files to include/exclude from the application backup. `<application android:allowBackup="true" android:fullBackupContent="@xml/backup.xml"> </application>`

See

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [Back up user data with Auto Backup](#)
- [Mobile AppSec Verification Standard](#) - Data Storage and Privacy Requirements
- [OWASP Mobile Top 10 2016 Category M1](#) - Improper platform usage
- [OWASP Mobile Top 10 2016 Category M2](#) - Insecure Data Storage
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [MITRE, CWE-922](#) - Insecure Storage of Sensitive Information

Available In:

