



## ANDROID STATIC ANALYSIS REPORT



 RetroMusicPlayer-6.1.0.zip

File Name: RetroMusicPlayer-6.1.0.zip

Package Name:






Scan Date: Oct. 6, 2023, 3:12 p.m.

App Security Score: **61/100 (LOW RISK)**

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	5	3	2	1

## FILE INFORMATION

**File Name:** RetroMusicPlayer-6.1.0.zip

**Size:** 15.74MB

**MD5:** 6ef56fd9d1b8d44c96ee0eeceb9b7abe

**SHA1:** eb378d064cc05ca9552f8acae7344fbce0f21e0b

**SHA256:** a01d6e64075d4a7f2ebd0372e4d68dcd3199f3bf982361e3059a9a7e2ef0dd23

## APP INFORMATION

**App Name:**

**Package Name:**

**Main Activity:**

**Target SDK:**

**Min SDK:**

**Max SDK:**

**Android Version Name:**

**Android Version Code:**

## APP COMPONENTS

Activities: 14

Services: 2

Receivers: 9

Providers: 1

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

## CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

## APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
	unknown	Unknown permission	Unknown permission from android reference

## NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
-------	----------	-------------

## MANIFEST ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

## CODE ANALYSIS

HIGH: 1 | WARNING: 4 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	code/name/monkey/retromusic/network/DeezerService.kt code/name/monkey/retromusic/network/RetrofitClient.kt

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	code/name/monkey/retromusic/activities/tageditor/AbsTagEditorActivity.kt code/name/monkey/retromusic/activities/tageditor/TagWriter.kt code/name/monkey/retromusic/dialogs/SongDetailDialog.kt code/name/monkey/retromusic/misc/CustomFragmentStatePagerAdapter.java code/name/monkey/retromusic/service/MediaButtonIntentReceiver.kt code/name/monkey/retromusic/service/MultiPlayer.kt code/name/monkey/retromusic/service/MusicService.kt code/name/monkey/retromusic/util/FileUtils.kt code/name/monkey/retromusic/util/LogUtil.kt code/name/monkey/retromusic/util/LyricUtil.kt code/name/monkey/retromusic/util/MusicUtil.kt code/name/monkey/retromusic/util/PackageValidator.kt code/name/monkey/retromusic/util/PlagiarismUtil.kt code/name/monkey/retromusic/util/SAFUtil.java code/name/monkey/retromusic/util/color/NotificationColorUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	code/name/monkey/retromusic/dialogs/BlacklistFolderChooserDialog.kt code/name/monkey/retromusic/fragments/folder/FoldersFragment.kt code/name/monkey/retromusic/helper/BackupHelper.kt code/name/monkey/retromusic/helper/MusicPlayerRemote.kt code/name/monkey/retromusic/providers/BlacklistStore.java code/name/monkey/retromusic/repository/SongRepository.kt code/name/monkey/retromusic/util/FileUtil.java code/name/monkey/retromusic/util/FileUtils.kt
4	Hidden elements in view can be used to hide data from user. But this data can be leaked	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-STORAGE-7	code/name/monkey/retromusic/views/BreadCrumbLayout.java
5	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	code/name/monkey/retromusic/misc/CustomFragmentStatePagerAdapter.java code/name/monkey/retromusic/network/LastFMService.kt
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	code/name/monkey/retromusic/service/PersistentStorage.kt code/name/monkey/retromusic/util/ArtistSignatureUtil.kt code/name/monkey/retromusic/util/CustomArtistImageUtil.kt

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	<a href="#">App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	code/name/monkey/retromusic/providers/BlacklistStore.java code/name/monkey/retromusic/providers/HistoryStore.java code/name/monkey/retromusic/providers/MusicPlaybackQueueStore.java code/name/monkey/retromusic/providers/SongPlayCountStore.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	code/name/monkey/retromusic/util/SAFUtil.java
9	<a href="#">This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.</a>	info	OWASP MASVS: MSTG-STORAGE-10	code/name/monkey/retromusic/activities/bugreport/BugReportActivity.kt

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## EMAILS

EMAIL	FILE
this@absbaseactivity.packagenam	code/name/monkey/retromusic/activities/base/AbsBaseActivity.kt



EMAIL	FILE
this@viewholder.song	code/name/monkey/retromusic/adaptersong/SongAdapter.kt
this@focusandshowkeyboard.showthekey	code/name/monkey/retromusic/extensions/ViewExtensions.kt
eenriquelopez@gmail.com	code/name/monkey/retromusic/helper/StackBlur.java
freedompaladin@gmail.com	code/name/monkey/retromusic/lyrics/Lrc.java

## HARDCODED SECRETS

POSSIBLE SECRETS
c679c8d3efa84613dc7dcb2e8d42da4c

---

### Report Generated by - MobSF v3.7.8 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).