ANDROID STATIC ANALYSIS REPORT

Phonograph (1.3.7)

File Name:	Phonograph Music Player_v1.3.7_apkpure.com.apk
Package Name:	com.kabouzeid.gramophone
Scan Date:	March 3, 2022, 5:16 a.m.
App Security Score:	**52/100 (MEDIUM RISK)**
Grade:	B

⊞ FINDINGS SEVERITY

🐞 HIGH	⚠ WARNING	ℹ INFO	✔ SECURE
2	12	2	2

📦 FILE INFORMATION

File Name: Phonograph Music Player_v1.3.7_apkpure.com.apk
Size: 5.9MB
MD5: c811d5c2eddb7f3e21150758604127cb
SHA1: 5add56628d24ce5760918cf3edc5248930c55e81
SHA256: 67c5b1a9ad3782aa027c44edc3b59600466f501b69d945b4a87cdc7e0771643c

ℹ APP INFORMATION

App Name: Phonograph
Package Name: com.kabouzeid.gramophone
Main Activity: com.kabouzeid.gramophone.ui.activities.MainActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 1.3.7
Android Version Code: 182

🔳 APP COMPONENTS

Activities: 18
Services: 1
Receivers: 6
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

✺ CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=DE, ST=NRW, L=Aachen, CN=Karim Abou Zeid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-03-18 13:36:47+00:00
Valid To: 2040-03-11 13:36:47+00:00
Issuer: C=DE, ST=NRW, L=Aachen, CN=Karim Abou Zeid
Serial Number: 0x55097f6f
Hash Algorithm: sha1
md5: 14bc63557f260c388e26be9fac539cfa
sha1: 367e9afcbf6e93dcc52c201cb70394b9c0f4612a
sha256: 26f2df37331fe1c1a6f8700dc8a1c302786346a919f7445b547f384ad48875ce
sha512: 067e89c4f4d16ed6a50ed6b11a0994eb349117de4354379eae4bf35294ad17f95eafd6990088d15aad07844b1353744f85d0a386637e60fc01f54805c8aa5603
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 784c354f84be2ba348d2e0e83d207dec9152ce36e13227d9ef877c46916ae525

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

≔ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

🔍 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

📑 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kabouzeid.gramophone.ui.activities.MainActivity	Schemes: content://, file://, http://, Mime Types: audio/*, application/ogg, application/x-ogg, application/itunes, vnd.android.cursor.dir/playlist, vnd.android.cursor.dir/albums, vnd.android.cursor.dir/artists, vnd.android.cursor.dir/audio,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

🔍 MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag 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.
2	Launch Mode of Activity (com.kabouzeid.gramophone.appshortcuts.AppShortcutLauncherActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.kabouzeid.gramophone.service.MediaButtonIntentReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (com.kabouzeid.gramophone.appwidgets.BootReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[App can read/write to External Storage. Any App can read data written to External Storage.](#)	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/kabouzeid/gramophone/util/PlaylistsUtil.java com/kabouzeid/gramophone/util/MusicUtil.java com/afollestad/materialdialogs/folderselector/FileChooserDialog.java com/kabouzeid/gramophone/dialogs/ScanMediaFolderChooserDialog.java com/kabouzeid/gramophone/provider/BlacklistStore.java com/kabouzeid/gramophone/ui/fragments/mainactivity/folders/FoldersFragment.java com/kabouzeid/gramophone/helper/MusicPlayerRemote.java com/kabouzeid/gramophone/dialogs/BlacklistFolderChooserDialog.java com/afollestad/materialdialogs/folderselector/FolderChooserDialog.java
				com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/Glide.java com/revenuecat/purchases/common/LogUtilsKt.java com/bumptech/glide/load/data/MediaStoreThumbFetcher.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemAddAnimationManager.java butterknife/ButterKnife.java com/bumptech/glide/request/GenericRequest.java com/bumptech/glide/gifdecoder/GifDecoder.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/resource/bitmap/D

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ownsampler.java
				com/h6ah4i/android/widget/advrecyclerview/draggable/DraggableItemWrapperAdapter.java
				com/bumptech/glide/gifdecoder/GifHeaderParser.java
				com/bumptech/glide/load/data/AssetPathFetcher.java
				com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemChangeAnimationManager.java
				com/kabouzeid/gramophone/dialogs/SongDetailDialog.java
				com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java
				com/bumptech/glide/load/resource/bitmap/RecyclableBufferedInputStream.java
				com/bumptech/glide/load/engine/CacheLoader.java
				org/jaudiotagger/audio/mp4/atom/Mp4StcoBox.java
				com/bumptech/glide/load/engine/EngineRunnable.java
				me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java
				com/bumptech/glide/load/resource/bitmap/ImageHeaderParser.java
				com/bumptech/glide/util/ByteArrayPool.java
				com/revenuecat/purchases/Purchases.java
				com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java
				com/afollestad/materialdialogs/internal/MDTintHelper.java
				com/bumptech/glide/load/model/ResourceLoader.java
				com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemMoveAnimationManager.java
				com/bumptech/glide/manager/RequestManagerRetriever.java
				com/bumptech/glide/request/target/ViewTarg
	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	information should never be logged.	Info	Information Into Log File OWASP MASVS: MSTG-STORAGE-3	et.java com/afollestad/materialdialogs/MaterialDialog.java com/bumptech/glide/load/model/ImageVideoModelLoader.java com/bumptech/glide/load/engine/executor/FifoPriorityThreadPoolExecutor.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/util/ContentLengthInputStream.java com/kabouzeid/gramophone/ui/activities/MainActivity.java com/kabouzeid/gramophone/helper/MusicPlayerRemote.java com/bumptech/glide/load/engine/Engine.java com/h6ah4i/android/widget/advrecyclerview/animator/GeneralItemAnimator.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/kabouzeid/gramophone/ui/activities/tageditor/AbsTagEditorActivity.java com/bumptech/glide/load/data/LocalUriFetcher.java com/kabouzeid/gramophone/service/MultiPlayer.java com/bumptech/glide/load/engine/DecodeJob.java com/kabouzeid/gramophone/misc/CustomFragmentStatePagerAdapter.java com/h6ah4i/android/widget/advrecyclerview/draggable/RecyclerViewDragDropManager.java com/triggertrap/seekarc/SeekArc.java com/kabouzeid/gramophone/glide/artistimage

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/ArtistImageFetcher.java com/bumptech/glide/load/resource/bitmap/ImageVideoBitmapDecoder.java
				com/bumptech/glide/load/resource/gif/GifResourceEncoder.java com/revenuecat/purchases/Purchases$fetchAndCachePurchaserInfo$2.java com/bumptech/glide/load/resource/gif/GifResourceDecoder.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java com/revenuecat/purchases/util/AdvertisingIdClient$getAdvertisingIdInfo$1.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemRemoveAnimationManager.java com/bumptech/glide/gifencoder/AnimatedGifEncoder.java com/bumptech/glide/load/model/StreamEncoder.java
3	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	org/jaudiotagger/audio/generic/AudioFileWriter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/revenuecat/purchases/subscriberattributes/AttributionKeys.java com/kabouzeid/appthemehelper/common/prefs/supportv7/dialogs/ATEPreferenceDialogFragment.java org/jaudiotagger/tag/id3/ID3v24Frames.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/kabouzeid/appthemehelper/ThemeStorePrefKeys.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/common/BackendKt.java org/jaudiotagger/tag/id3/ID3v23Frames.java org/eclipse/egit/github/core/service/DownloadService.java com/revenuecat/purchases/common/caching/DeviceCache.java org/jaudiotagger/tag/id3/ID3v22Frames.java
5	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.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/kabouzeid/gramophone/provider/HistoryStore.java com/kabouzeid/gramophone/provider/BlacklistStore.java com/kabouzeid/gramophone/provider/SongPlayCountStore.java com/kabouzeid/gramophone/provider/MusicPlaybackQueueStore.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/kabouzeid/gramophone/lastfm/rest/LastFMRestClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/kabouzeid/gramophone/service/MusicService.java com/kabouzeid/gramophone/helper/MusicPlayerRemote.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/revenuecat/purchases/common/UtilsKt.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/afollestad/materialdialogs/BuildConfig.java com/afollestad/materialdialogs/commons/BuildConfig.java
10	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/kabouzeid/gramophone/ui/activities/bugreport/BugReportActivity.java

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
13	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
creativecommons.org	ok	**IP:** 104.20.151.16 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 104.18.210.56 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
opensource.org	ok	**IP:** 159.65.34.8 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
api.revenuecat.com	ok	**IP:** 34.206.248.15 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
musicbrainz.org	ok	**IP:** 138.201.227.205 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mozilla.org	ok	**IP:** 44.236.48.31 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
phonograph.oneskyapp.com	ok	**IP:** 54.163.46.208 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.id3.org	ok	**IP:** 167.99.106.11 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map
play.google.com	ok	**IP:** 142.250.199.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.github.com	ok	**IP:** 20.205.243.168 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** [Google Map](#)
kabouzeid.com	ok	**IP:** 104.198.14.52 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** [Google Map](#)
psdev.de	ok	**IP:** 5.9.31.240 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** [Google Map](#)
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
cookicons.co	ok	**IP:** 69.163.196.156 **Country:** United States of America **Region:** California **City:** Brea **Latitude:** 33.930222 **Longitude:** -117.888420 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
echeung.me	ok	**IP:** 104.21.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
maartencorpel.com	ok	**IP:** 104.21.20.10 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.eclipse.org	ok	**IP:** 198.41.30.198 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.345139 **Longitude:** -75.765076 **View:** [Google Map](#)

✉ EMAILS

EMAIL	FILE
contact@kabouzeid.com	com/kabouzeid/gramophone/ui/activities/AboutActivity.java

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"username" : "Username"
"password" : "Passwort"
"username" : "Benutzername"

POSSIBLE SECRETS

"password" : "Password"
"username" : "Username"
"bug_report_failed_wrong_credentials" : "   "
"bug_report_no_password" : "   GitHub   "
"bug_report_no_username" : "   GitHub   "
"password" : "   "
"username" : "   "
"your_account_data_is_only_used_for_authentication" : "   "
"password" : "סיסמא"
"password" : "Парола"
"username" : "Юзернейм"
"password" : "Salasana"
"username" : "Käyttäjänimi"
"password" : "Пароль"
"password" : "Wachtwoord"

POSSIBLE SECRETS

"username" : "Gebruikersnaam"

"password" : "Hasło"

"password" : "   "

"password" : "Parolă"

"password" : "Lozinka"

"password" : "Şifre"

"password" : "Heslo"

"password" : "Jelszó"

"username" : "Felhasználónév"

"password" : "Пароль"

"password" : "סיסמא"

"password" : "Password"

"username" : "Username"

"password" : "Password"

"username" : "Username"

POSSIBLE SECRETS

"bug_report_failed_wrong_credentials" : "   "
"password" : "   "
"username" : "   "
"your_account_data_is_only_used_for_authentication" : "   "
"password" : "Senha"
"password" : "Contraseña"
"password" : "Contraseña"
"password" : "Senha"
"bug_report_failed_wrong_credentials" : "   "
"password" : "   "
"username" : "   "
"your_account_data_is_only_used_for_authentication" : "   "

▶ PLAYSTORE INFORMATION

Title: Phonograph Music Player

Score: 3.8227513 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Music & Audio **Play Store URL:** com.kabouzeid.gramophone

Developer Details: Karim Abou Zeid, 5958475666241621742, Eilendorfer Str. 92 52078 Aachen Germany, https://kabouzeid.com, contact@kabouzeid.com,

Release Date: Apr 11, 2015 **Privacy Policy:** [Privacy link](#)

Description:

Probably the best looking music player out there. Material Design The user interface matches every single detail of the material design guidelines to ensure Phonograph is an eye candy for you. Easy to Use No complicated or overblown menus but a familiar and clean interface. Last.fm Integration Phonograph automatically downloads additional information about your artists such as their images or biographies. When you install the official Last.fm app, scrobbling will work right out of the box too. Dynamic Colors The UI colors change dynamically to match the main contents base color. Customizability There is an inbuilt theme engine with many different colors to choose from. Tag Editor The tag editor allows you to easily edit the tags of your music files such as title, artist, album name (...) for single songs or whole albums. You can even either let Phonograph automatically download missing album covers for you (powered by Last.fm) or choose one from your internal storage. And OF COURSE - Phonograph has all standard features such as: - Create and edit playlists - Homescreen widget - Lockscreen playback controls - "Go-To Actions" such as jump from a song or an album right to its artist - ... Licenses for the album covers used in the screenshots: Credits: https://www.flickr.com/photos/room122/ Link: https://www.flickr.com/photos/room122/3248118087 License: https://creativecommons.org/licenses/by/2.0/ Credits: https://www.flickr.com/photos/40985721@N00/ Link: https://www.flickr.com/photos/40985721@N00/7918133232 License: https://creativecommons.org/licenses/by/2.0/ Credits: https://www.flickr.com/photos/wheatfields/ Link: https://www.flickr.com/photos/wheatfields/3328507930 License: https://creativecommons.org/licenses/by/2.0/

Report Generated by - MobSF v3.5.1 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.