ANDROID STATIC ANALYSIS REPORT

QKSMS (3.9.2)

File Name:	QKSMS_v3.9.2.com.apk
Package Name:	com.moez.QKSMS
Scan Date:	March 3, 2022, 5:55 a.m.
App Security Score:	**50/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	3/421

FINDINGS SEVERITY

HIGH	WARNING	INFO	✓ SECURE
0	17	2	0

FILE INFORMATION

File Name: QKSMS_v3.9.2.com.apk
Size: 11.26MB
MD5: 6b7211027746d278e0118a5e98ac1de2
SHA1: 20cc815890140bd20d60e128d9251c61b3d08986
SHA256: 9461a8db41ec9a63840ddb74e69a7a6a8b3a7858e543421fe0f3eba8ae4e1fb3

APP INFORMATION

App Name: QKSMS
Package Name: com.moez.QKSMS
Main Activity: com.moez.QKSMS.feature.main.MainActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 3.9.2

Android Version Code: 2216

APP COMPONENTS

Activities: 13
Services: 9
Receivers: 21
Providers: 4
Exported Activities: 1
Exported Services: 2
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=CA, ST=Ontario, L=Oakville, O=Moez, OU=Moez, CN=Moez Bhatti
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-03-12 05:14:46+00:00
Valid To: 2038-03-06 05:14:46+00:00
Issuer: C=CA, ST=Ontario, L=Oakville, O=Moez, OU=Moez, CN=Moez Bhatti
Serial Number: 0x4daeeccd
Hash Algorithm: sha256
md5: 865209fe6a89916637a6019e94722775
sha1: 0bc2fa43fb167d3515026b35b3cdeef4df0ece86
sha256: 7c6aa309f970cd867729e5e09b323890403f356fd70b0a5d9d8dcad87efb16a0
sha512: affc780cab0d01ce1d9f68797ccd180839d2703c0bb6034ff90f348b136904269e67d94591e51e656aaf1e66bd3b332567e5570e914360af69e8899283a47186
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8b4c9e579cd3616c4409704bee1504b15568b34bef717a0dd4bc964909f49737
```

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.

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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.
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
SIM operator check
network operator name check
device ID check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.moez.QKSMS.feature.compose.ComposeActivity	Schemes: sms://, smsto://, mms://, mmsto://, sms_body://, Mime Types: text/plain, image/*, text/x-vcard,

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	Activity (com.moez.QKSMS.feature.compose.ComposeActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.moez.QKSMS.receiver.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.
4	Broadcast Receiver (com.moez.QKSMS.receiver.DefaultSmsChangedReceiver) 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.
5	Broadcast Receiver (com.moez.QKSMS.receiver.SmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_SMS [android:exported=true]	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. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (com.moez.QKSMS.receiver.MmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_WAP_PUSH [android:exported=true]	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. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (com.moez.QKSMS.receiver.SmsProviderChangedReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Broadcast Receiver (com.moez.QKSMS.feature.widget.WidgetProvider) 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.
9	Service (com.moez.QKSMS.service.HeadlessSmsSendService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Service (com.moez.QKSMS.common.util.QkChooserTargetService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CHOOSER_TARGET_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/load/data/medias

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tore/ThumbFetcher.java com/bumptech/glide/load/resource/bitmap/Downsampler.java io/realm/internal/OsRealmConfig.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java me/leolin/shortcutbadger/ShortcutBadger.java com/amplitude/api/AmplitudeClient.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/moez/QKSMS/common/util/FileLoggingTree.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/model/ByteBufferFileLoader.java io/realm/RealmObject.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java io/realm/internal/FinalizerRunnable.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/model/ResourceLoader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/load/data/AssetPathFetcher.java io/realm/internal/Util.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/DecodePath.java com/amplitude/api/AmplitudeLog.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/Glide.java com/amplitude/api/DatabaseHelper.java io/realm/RealmCache.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/resource/bit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				map/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java timber/log/Timber.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java io/realm/RealmResults.java io/realm/BaseRealm.java io/realm/Realm.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/data/LocalUriFetcher.java
2	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/bumptech/glide/load/engine/ResourceCacheKey.java com/moez/QKSMS/interactor/SetDefaultPhoneNumber.java com/moez/QKSMS/feature/main/DrawerBadgesExperiment.java com/moez/QKSMS/mapper/CursorToContactGroupMember.java com/moez/QKSMS/experiment/Variant.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/moez/QKSMS/feature/plus/experiment/UpgradeButtonExperiment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/moez/QKSMS/common/util/FileLoggingTree.java com/moez/QKSMS/repository/MessageRepositoryImpl.java com/moez/QKSMS/repository/BackupRepositoryImpl.java
4	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/klinker/android/send_message/Transaction.java com/moez/QKSMS/experiment/Experiment.java
5	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/moez/QKSMS/common/util/ClipboardUtils.java
6	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/amplitude/api/DatabaseHelper.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/librealm-jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/librealm-jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/mips/librealm-jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/librealm-jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/x86_64/librealm-jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

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.
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 ['address book'].
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 does not encrypt files 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.
14	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
qklabs.com	ok	**IP:** 151.101.1.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firestore.googleapis.com	ok	**IP:** 142.250.67.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bit.ly	ok	**IP:** 67.199.248.11 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **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
qksms-app.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.67.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.199.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
realm.io	ok	**IP:** 13.249.224.123 **Country:** India **Region:** Telangana **City:** Hyderabad **Latitude:** 17.375280 **Longitude:** 78.474442 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.amplitude.com	ok	**IP:** 44.238.97.181 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
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
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://qksms-app.firebaseio.com	info App talks to a Firebase Database.

✉ EMAILS

EMAIL	FILE
moez@qklabs.com	com/moez/QKSMS/common/Navigator.java
moez@qklabs.com	Android String Resource
help@realm.io	lib/arm64-v8a/librealm-jni.so
help@realm.io	lib/armeabi-v7a/librealm-jni.so
help@realm.io	lib/mips/librealm-jni.so
help@realm.io	lib/x86/librealm-jni.so
help@realm.io	lib/x86_64/librealm-jni.so

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://qksms-app.firebaseio.com"
"google_api_key" : "AIzaSyAGGhC6E6736ALcHgBm16q5LpXEH8ccbBQ"
"google_crash_reporting_api_key" : "AIzaSyAGGhC6E6736ALcHgBm16q5LpXEH8ccbBQ"

PLAYSTORE INFORMATION

Title: QKSMS

Score: 3.9626865 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Communication **Play Store URL:** com.moez.QKSMS

Developer Details: Moez Bhatti, 7472856873836800989, 624 Adelaide St W Toronto, ON M6J 1A9 Canada, https://github.com/moezbhatti/qksms, moez@qklabs.com,

Release Date: Nov 6, 2014 **Privacy Policy:** Privacy link

Description:

We're making texting magical again. QKSMS is the most beautiful messaging experience you've ever used. Replace your stock messaging app and fall in love with texting all over again. QKSMS is also completely ad-free and open source, the way your messaging app should be. New: Dual-SIM and Multi-SIM phones are now fully supported by QKSMS! Clean A beautiful, intuitive, and clutter-free design that allows you to focus on what matters. Customizable Use any of the millions of colors to theme the entire app, or any particular conversation. Per-contact notifications allow you to easily prioritize and distinguish your messages. Manual and automatic night mode are great too. Powerful Use MMS to share photos, stickers, or join your friends in a group chat. Conversation search allows you to find things easier than ever. Safe Easily Back up and Restore your messages, all without having to install another app. Private Easily block conversations and manage your blacklist, or automatically filter out spam with Should I Answer? integration. Convenient Reply to your messages from anywhere using the QK Reply popup, your Wear OS (Android Wear) watch, or directly from your notification shade (Android 7.0+) Accessibility High contrast black theme, and full support for TalkBack and Samsung Voice Assistant. We love hearing what you have to say, so always feel free to let us know whenever you have any feedback or suggestions! If you'd like to view the QKSMS source code, it's available on Github: https://github.com/moezbhatti/qksms/

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.