ANDROID STATIC ANALYSIS REPORT

YUP (1.0)

File Name:	YUP_v1.0_apkpure.com.apk
Package Name:	com.yup.app
Average CVSS Score:	5.8
App Security Score:	20/100 (HIGH RISK)
Trackers Detection:	4/285

FILE INFORMATION

File Name: YUP_v1.0_apkpure.com.apk
Size: 23.24MB
MD5: 0c7fc3328d993ce257174736c1f178f4
SHA1: 0744b6cf2a0b4308c8067ea91b0c1fd72a39b894
SHA256: 471ff049bda8ef379d284882a0f605c5024dfa79fff0e0f1eb556adaa8a062b1

APP INFORMATION

App Name: YUP
Package Name: com.yup.app
Main Activity: com.yup.app.SplashActivity
Target SDK: 27
Min SDK: 19
Max SDK:
Android Version Name: 1.0
Android Version Code: 2

APP COMPONENTS

Activities: 46
Services: 12
Receivers: 3
Providers: 6
Exported Activities: 2
Exported Services: 5
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-01-17 08:43:19+00:00
Valid To: 2049-01-17 08:43:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x8faa21da70d209a34479501e43814de0f8af7240
Hash Algorithm: sha256
md5: 3cdebe45580b44a8a380c003b3b25a20
sha1: 3236ed1ff489a615d0ecc2518fc0151bde3ffb28
sha256: 23dfef14441a3f448d305a7d0b41384a3bd10253fe4575f0c5c1eb27546f521f
sha512:
eb491dc5efdd68d1ee7ce1f2d0d91df27ad2073fbb936adc2076c58df16a085d20b42715ce1998207954a470491fab8b5842e5b6b4d335dea5a929128ba4e08e

PublicKey Algorithm: rsa

Bit Size: 4096
Fingerprint: 7455eb707748e0a300d84fa68ad3c4950444650467f728cad3bedb477b238bd2

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
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.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine

			where you are and may consume additional battery power.
android.permission.CHANGE_NETWORK_STATE	dangerous	change network connectivity	Allows an application to change the state of network connectivity.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	dangerous	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

FILE	DETAILS

<table>
<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table></td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Activity (com.yup.app.MainActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Service (com.yup.helper.MyFirebaseInstanceIDService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Service (com.yup.helper.MyFirebaseMessagingService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Activity (com.facebook.accountkit.ui.AccountKitEmailRedirectActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Launch Mode of Activity (org.acra.dialog.CrashReportDialog) 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.

Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	high	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.
Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	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.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	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.
Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			jp/wasabeef/glide/transformations/MaskTransformation.java jp/wasabeef/glide/transformations/Gra

				yscaleTransformation.java jp/wasabeef/glide/transformations/CropSquareTransformation.java jp/wasabeef/glide/transformations/CropTransformation.java jp/wasabeef/glide/transformations/RoundedCornersTransformation.java jp/wasabeef/glide/transformations/BlurTransformation.java jp/wasabeef/glide/transformations/ColorFilterTransformation.java jp/wasabeef/glide/transformations/SupportRSBlurTransformation.java jp/wasabeef/glide/transformations/CropCircleTransformation.java jp/wasabeef/glide/transformations/gpu/GPUFilterTransformation.java jp/wasabeef/glide/transformations/gpu/InvertFilterTransformation.java jp/wasabeef/glide/transformations/gpu/PixelationFilterTransformation.java jp/wasabeef/glide/transformations/gpu/ContrastFilterTransformation.java jp/wasabeef/glide/transformations/gpu/SepiaFilterTransformation.java jp/wasabeef/glide/transformations/gpu/SwirlFilterTransformation.java jp/wasabeef/glide/transformations/gpu/ToonFilterTransformation.java jp/wasabeef/glide/transformations/gpu/SketchFilterTransformation.java jp/wasabeef/glide/transformations/gpu/KuwaharaFilterTransformation.java jp/wasabeef/glide/transformations/gpu/BrightnessFilterTransformation.java jp/wasabeef/glide/transformations/gpu/VignetteFilterTransformation.java retrofit2/Utils.java org/acra/collector/StacktraceCollector.java org/webrtc/MediaConstraints.java org/webrtc/HardwareVideoEncoder.java org/webrtc/CameraEnumerationAndroid.java com/bumptech/glide/signature/ObjectKey.java com/bumptech/glide/signature/MediaStoreSignature.java com/bumptech/glide/load/MultiTransformation.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/Options.java com/bumptech/glide/load/resource/gif/GifDrawableTransformation.java com/bumptech/glide/load/resource/bitmap/RoundedCorners.java com/bumptech/glide/load/resource/bitmap/DrawableTransformation.java com/bumptech/glide/load/resource/bitmap/CenterCrop.java com/bumptech/glide/load/resource/bitmap/FitCenter.java com/bumptech/glide/load/resource/bitmap/BitmapDrawableTransformation.j

This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	ava com/bumptech/glide/load/resource/bitmap/CircleCrop.java com/bumptech/glide/load/resource/bitmap/CenterInside.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineKey.java com/bumptech/glide/load/engine/prefill/PreFillType.java com/bumptech/glide/load/engine/bitmap_recycle/SizeConfigStrategy.java com/bumptech/glide/load/engine/bitmap_recycle/AttributeStrategy.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/model/ModelCache.java com/bumptech/glide/load/model/GlideUrl.java com/bumptech/glide/load/model/LazyHeaders.java com/bumptech/glide/util/Util.java com/bumptech/glide/util/MultiClassKey.java com/bumptech/glide/util/CachedHashCodeArrayMap.java com/bumptech/glide/request/SingleRequest.java com/airbnb/lottie/LottieDrawable.java com/airbnb/lottie/model/MutablePair.java com/airbnb/lottie/model/DocumentData.java com/airbnb/lottie/model/FontCharacter.java com/airbnb/lottie/parser/RectangleShapeParser.java com/airbnb/lottie/parser/PolystarShapeParser.java com/airbnb/lottie/parser/MergePathsParser.java com/airbnb/lottie/parser/AnimatableTextPropertiesParser.java com/airbnb/lottie/parser/DocumentDataParser.java com/airbnb/lottie/parser/AnimatableTransformParser.java com/airbnb/lottie/parser/RepeaterParser.java com/airbnb/lottie/parser/GradientFillParser.java com/airbnb/lottie/parser/KeyframeParser.java com/airbnb/lottie/parser/KeyframesParser.java com/airbnb/lottie/parser/FontCharacterParser.java com/airbnb/lottie/parser/CircleShapeParser.java com/airbnb/lottie/parser/ShapeGroupParser.java

			com/airbnb/lottie/parser/LayerParser.java com/airbnb/lottie/parser/FontParser.java com/airbnb/lottie/parser/GradientStrokeParser.java com/airbnb/lottie/parser/LottieCompositionParser.java com/airbnb/lottie/parser/ShapePathParser.java com/airbnb/lottie/parser/ShapeStrokeParser.java com/airbnb/lottie/parser/JsonUtils.java com/airbnb/lottie/parser/ContentModelParser.java com/airbnb/lottie/parser/MaskParser.java com/airbnb/lottie/parser/ShapeDataParser.java com/airbnb/lottie/parser/ShapeFillParser.java com/airbnb/lottie/parser/AnimatablePathValueParser.java com/airbnb/lottie/parser/ShapeTrimPathParser.java com/yup/helper/AutoStartPermissionHelper.java com/yup/helper/MyFirebaseMessagingService.java com/yup/helper/SocketConnection.java com/yup/helper/ForegroundService.java com/yup/external/ImagePicker.java com/yup/app/ChatActivity.java com/yup/app/GroupChatActivity.java com/yup/app/CallActivity.java com/yup/app/ChannelChatActivity.java com/yup/app/CallFragment.java com/yup/app/ForwardActivity.java com/yup/app/ChatFragment.java com/yup/app/GroupFragment.java com/yup/appRTC/PeerConnectionClient.java droidninja/filepicker/models/PhotoDirectory.java droidninja/filepicker/models/FileType.java
			org/acra/ACRA.java org/acra/ErrorReporter.java org/acra/file/BulkReportDeleter.java org/acra/legacy/ReportMigrator.java org/acra/util/IOUtils.java org/acra/util/PackageManagerWrapper.java org/acra/util/ProcessFinisher.java org/acra/util/JsonUtils.java org/acra/util/Installation.java org/acra/util/InstanceCreator.java org/acra/collector/LogFileCollector.java org/acra/collector/SimpleValuesCollector.java org/acra/collector/DeviceIdCollector.java org/acra/collector/ConfigurationCollect

				or.java org/acra/dialog/BaseCrashReportDialog.java org/acra/sender/DefaultReportSenderFactory.java org/acra/sender/NullSender.java org/acra/sender/ReportDistributor.java org/acra/http/BaseHttpRequest.java org/acra/security/AssetKeyStoreFactory.java org/acra/security/FileKeyStoreFactory.java org/acra/log/AndroidLogDelegate.java org/acra/attachment/DefaultAttachmentProvider.java org/acra/attachment/AcraContentProvider.java org/acra/builder/LastActivityManager.java org/acra/builder/ReportExecutor.java de/tavendo/autobahn/WebSocketConnection.java de/tavendo/autobahn/WebSocketWriter.java de/tavendo/autobahn/WebSocketReader.java com/bumptech/glide/Glide.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java

The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/module/ManifestParser.java com/wang/avi/AVLoadingIndicatorView.java com/makeramen/roundedimageview/RoundedImageView.java com/makeramen/roundedimageview/RoundedDrawable.java com/airbnb/lottie/LottieDrawable.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/LottieComposition.java com/airbnb/lottie/L.java com/airbnb/lottie/manager/ImageAsset

				Manager.java com/airbnb/lottie/manager/FontAsset Manager.java com/airbnb/lottie/model/layer/BaseLay er.java com/airbnb/lottie/model/content/Merg ePaths.java com/airbnb/lottie/parser/AnimatableTr ansformParser.java com/airbnb/lottie/parser/ContentMode lParser.java com/airbnb/lottie/parser/MaskParser.ja va com/yup/helper/ImageDownloader.jav a com/yup/helper/StorageManager.java com/yup/helper/DownloadFiles.java com/yup/helper/CallNotificationService .java com/yup/helper/DatabaseHandler.java com/yup/helper/NetworkUtil.java com/yup/helper/MyFirebaseMessaging Service.java com/yup/helper/SocketConnection.java com/yup/helper/FileUploadService.java com/yup/helper/Utils.java com/yup/helper/NetworkReceiver.java com/yup/helper/MyFirebaseInstanceID Service.java com/yup/helper/ForegroundService.jav a com/yup/external/ImageRotator.java com/yup/external/EndlessRecyclerOnSc rollListener.java com/yup/external/ImageUtils.java com/yup/external/ImagePicker.java com/yup/app/CallContactActivity.java com/yup/app/CreateGroupActivity.java com/yup/app/SubscribersActivity.java com/yup/app/ChatActivity.java com/yup/app/ChannelRequestActivity.j ava com/yup/app/WelcomeActivity.java com/yup/app/ProfileActivity.java com/yup/app/GroupChatActivity.java com/yup/app/BaseActivity.java com/yup/app/CallActivity.java com/yup/app/AllChannelsActivity.java com/yup/app/MainActivity.java com/yup/app/ProfileInfo.java com/yup/app/ChannelChatActivity.java com/yup/app/HelpViewActivity.java com/yup/app/CreateChannelActivity.jav a com/yup/app/CallFragment.java com/yup/app/ReportActivity.java com/yup/app/NewGroupActivity.java com/yup/app/ForwardActivity.java com/yup/app/LocationActivity.java com/yup/app/ChannelInfoActivity.java com/yup/app/EditGroupActivity.java com/yup/app/SplashActivity.java com/yup/app/GroupInfoActivity.java com/yup/app/SelectContact.java com/yup/app/HelpActivity.java

			com/yup/app/ChatFragment.java com/yup/app/ApplicationClass.java com/yup/app/GroupFragment.java com/yup/app/DeleteAccountActivity.java com/yup/appRTC/CustomSdpObserver.java com/yup/appRTC/AppRTCAudioManager.java com/yup/appRTC/CustomPeerConnectionObserver.java com/yup/appRTC/PeerConnectionClient.java com/yup/appRTC/UnhandledExceptionHandler.java com/yup/appRTC/AppRTCProximitySensor.java com/yup/appRTC/AppRTCBluetoothManager.java droidninja/filepicker/MediaDetailsActivity.java droidninja/filepicker/FilePickerActivity.java droidninja/filepicker/fragments/MediaFolderPickerFragment.java droidninja/filepicker/utils/ImageCaptureManager.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/acra/file/Directory.java com/yup/helper/StorageManager.java com/yup/helper/DownloadFiles.java com/yup/helper/ImageCompression.java com/yup/helper/Utils.java com/yup/app/ChatActivity.java com/yup/app/GroupChatActivity.java com/yup/app/ChannelChatActivity.java com/yup/appRTC/PeerConnectionClient.java droidninja/filepicker/utils/ImageCaptureManager.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	de/tavendo/autobahn/WebSocketWriter.java com/yup/helper/MyFirebaseMessagingService.java com/yup/external/RandomString.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 - Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/manager/RequestManagerRetriever.java com/yup/utils/Constants.java droidninja/filepicker/utils/ImageCaptureManager.java
App uses SQLite Database and execute raw SQL query.		CVSS V2: 5.9 (medium)	

Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	**CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	com/yup/helper/DatabaseHandler.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-10	com/yup/app/ChatActivity.java com/yup/app/GroupChatActivity.java com/yup/app/ChannelChatActivity.java
IP Address disclosure	warning	**CVSS V2:** 4.3 (medium) **CWE:** CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor **OWASP MASVS:** MSTG-CODE-2	com/yup/utils/Constants.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.google.com	good	**IP:** 216.58.210.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
maps.google.com	good	**IP:** 172.217.169.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	good	**IP:** 140.82.118.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
yup.im	good	**IP:** 103.224.182.246 **Country:** Australia **Region:** Victoria **City:** Beaumaris **Latitude:** -37.982201 **Longitude:** 145.03894 **View:** Google Map
yupim-c3ea6.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514

		View: Google Map
play.google.com	good	IP: 216.58.204.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

URLS

URL	FILE
http://localhost/	retrofit2/Response.java
https://www.google.com	de/tavendo/autobahn/WebSocketWriter.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
http://maps.google.com/maps/api/staticmap?center= https://yup.im:3000/media/chats/	com/yup/app/ChatActivity.java
https://yup.im:3000/media/chats/	com/yup/app/ChannelRequestActivity.java
https://yup.im:3000/media/chats/	com/yup/app/MyChannelsActivity.java
https://yup.im:3000/media/chats/	com/yup/app/ChannelFragment.java
https://yup.im:3000/media/chats/ http://maps.google.com/maps/api/staticmap?center=	com/yup/app/GroupChatActivity.java
https://yup.im:3000/media/chats/	com/yup/app/AllChannelsActivity.java
https://play.google.com/store/apps/details?id=	com/yup/app/MainActivity.java
https://yup.im:3000/media/chats/ http://maps.google.com/maps/api/staticmap?center=	com/yup/app/ChannelChatActivity.java
https://yup.im:3000/media/chats/	com/yup/app/CreateChannelActivity.java
https://yup.im:3000/media/chats/	com/yup/app/DialogActivity.java
https://yup.im:3000/media/chats/	com/yup/app/ChannelCreatedActivity.java
https://yup.im:3000/media/chats/	com/yup/app/ForwardActivity.java
http://maps.google.com/maps/api/geocode/json	com/yup/app/LocationActivity.java
https://yup.im:3000/media/chats/	com/yup/app/ChannelInfoActivity.java

https://yup.im:3000/media/chats/	com/yup/app/EditGroupActivity.java
https://yup.im:3000/media/chats/	com/yup/app/GroupInfoActivity.java
https://yup.im:3000/media/chats/	com/yup/app/SearchActivity.java
https://yup.im:3000/media/chats/	com/yup/app/GroupFragment.java
https://yup.im:3000/ https://yup.im:3000/media/chats/ http://yup.im:8081 https://yup.im:3000/media/users/	com/yup/utils/Constants.java
https://yupim-c3ea6.firebaseio.com https://github.com/vinc3m1 https://github.com/vinc3m1/RoundedImageView https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://yupim-c3ea6.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
your.account@domain.com	org/acra/sender/DefaultReportSenderFactory.java
crashlog@hitasoft.com	com/yup/app/ApplicationClass.java

TRACKERS

TRACKER	URL
AccountKit	https://reports.exodus-privacy.eu.org/trackers/91
Google Ads	https://reports.exodus-privacy.eu.org/trackers/71
Google DoubleClick	https://reports.exodus-privacy.eu.org/trackers/5
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.9 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.