MOBSF

ANDROID STATIC ANALYSIS REPORT

SadaPay (0.1.10762)

File Name:	SadaPay.apk
Package Name:	com.sadapay.app
Scan Date:	Oct. 19, 2024, 11:10 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	23	4	2	2

FILE INFORMATION

File Name: SadaPay.apk
Size: 39.05MB
MD5: 2cfcda8024a44ca1909216557f8875eb
SHA1: a07e36a3261ef962dba56e1823b336a173a6a2b9
SHA256: 48af325e730dfae4b3f4b85e8e91c0a52f10481345fe92b4971b8b0b0a252629

APP INFORMATION

App Name: SadaPay
Package Name: com.sadapay.app
Main Activity: com.sadapay.app.ui.main.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 0.1.10762

Android Version Code: 10762

APP COMPONENTS

Activities: 41
Services: 18
Receivers: 21
Providers: 13
Exported Activities: 5
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-15 04:20:36+00:00
Valid To: 2050-06-15 04:20:36+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x33291106c6f77787c850eb8eeca73dfc18d3c50e
Hash Algorithm: sha256
md5: 3f6c2c63129bf2bf2407bfea7ea105f3
sha1: 6343d2de550af61f38807f9a4f1ca36e93751cf1
sha256: 14322446c72f719a1c42939bac2411b8432a3610bf650d4e70e1609634b581a1
sha512: cc68ab0cea01e8388b2c36c49a16b8cdba695afb1a1cbd8649fc9b45f507a1a01a58a3794db1448096ee9c9ac53d5ea927e416c54f609408bfddbb6a3a59e678
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: cb0149c7d96db918ddeb23c2f985cff4b8946269540b2032facf347f0d779bca
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.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.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.sadapay.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

APKID ANALYSIS

FILE	DETAILS
/home/mobsf/.MobSF/uploads/2cfcda8024a44ca1909216557f8875eb/2cfcda8024a44ca1909216557f8875eb.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>emulator file check possible VM check</td></tr></table>

<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.MANUFACTURER check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<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.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check possible ro.secure check emulator file check possible VM check</td></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.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
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes6.dex	<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 network operator name check</td></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

FILE	DETAILS
classes7.dex	<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.HARDWARE check possible Build.SERIAL check Build.TAGS check network operator name check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes8.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.HARDWARE check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Protector</td><td>InsideSecure Verimatrix</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.sadapay.app.ui.main.MainActivity	Schemes: sadapay.pk/android://, sadapay://, https://, Hosts: open, send-money, money-requests, load-money, order-card, activate-card, my-cards, dashboard, chat, intercom, business-account, sadabiz-proposition, rewards-hub, rewards-sadabiz, invite.sadapay.pk, Paths: /,
com.plaid.internal.LinkRedirectActivity	Schemes: plaid://, Hosts: complete, redirect,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	TaskAffinity is set for activity (com.chuckerteam.chucker.internal.ui.MainActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
3	Activity (com.plaid.internal.LinkRedirectActivity) is not Protected. [android:exported=true]	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.
4	Activity (com.plaid.internal.link.LinkActivity) is not Protected. [android:exported=true]	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.
5	TaskAffinity is set for activity (com.urbanairship.push.NotificationProxyActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	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]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_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.
8	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.
9	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	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.
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **4** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	ab/w.java bd/f.java com/apptimize/aw.java ec0/b.java en/d.java h5/o0.java h5/x.java hb/n0.java i5/x.java in/f.java in/g.java io/sentry/metrics/c.java j$/util/concurrent/ThreadLocalRandom.java jf/k.java jn/c.java jn/i.java jn/n.java ke0/a.java ke0/b.java le0/a.java ll/e.java o5/a1.java pf/a.java pl/f.java qd/c.java rd/a.java ud/a.java uf0/h.java uf0/m.java w/d.java za/s.java za/w.java
				a0/a.java a5/a.java a60/b.java a60/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ab/h.java ab/i.java au/q.java ay/i.java b7/d.java b7/t.java b7/x.java bb/o.java be/d.java bh/t.java bo/c.java bo/d.java cb0/d.java ce/d.java ce/e.java com/apptimize/Apptimize.java com/apptimize/bo.java com/apptimize/br.java com/apptimize/bs.java com/apptimize/j.java com/bumptech/glide/b.java com/bumptech/glide/k.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/f0.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/l.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/resource/bitmap/b.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/f0.java com/bumptech/glide/load/resource/bitmap/i.java com/bumptech/glide/load/resource/bitmap/k.java com/bumptech/glide/load/resource/bitmap

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/o.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/u.java com/bumptech/glide/load/resource/bitmap/y.java com/bumptech/glide/n.java com/intercom/twig/Twig.java com/iovation/mobile/android/FraudForceConfiguration.java com/journeyapps/barcodescanner/CaptureActivity.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/DecideChecker.java com/mixpanel/android/mpmetrics/MPConfig.java com/mixpanel/android/mpmetrics/MixpanelAPI.java com/mixpanel/android/mpmetrics/ResourceReader.java com/plaid/internal/k3.java com/sadapay/app/App.java com/urbanairship/Autopilot.java com/urbanairship/e.java com/urbanairship/p.java com/veridiumid/sdk/VeridiumSDK.java com/veridiumid/sdk/VeridiumSDKImpl.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/analytics/Analytics.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/crypto/TransactionSigningHelper.java com/veridiumid/sdk/defaultdata/securepreferences/LegacySecurePreferences.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/defaults/biometricsettingsdefaultui/BiometricSettingsFragment.java com/veridiumid/sdk/fourf/ExportConfig.java com/veridiumid/sdk/fourf/FourFLoader.java com/veridiumid/sdk/fourf/camera/Camera1PreviewView.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java com/veridiumid/sdk/fourf/camera/ImageTaggingQueue.java com/veridiumid/sdk/fourf/ui/FourFUIFragment.java com/veridiumid/sdk/internal/licensing/LicensingRepository.java com/veridiumid/sdk/log/Timber.java com/veridiumid/sdk/model/ManifestVeridiumSDKModel.java com/veridiumid/sdk/model/biometrics/engine/impl/DecentralizedBiometricsEngineImpl.java com/veridiumid/sdk/model/biometrics/engine/impl/ModularBiometricProcessor.java com/veridiumid/sdk/model/biometrics/packaging/IBiometricFormats.java com/veridiumid/sdk/model/biometrics/persistence/impl/BytesTemplatesStorage.java com/veridiumid/sdk/model/biometrics/results/BiometricResultsParser.java com/veridiumid/sdk/model/help/AssetsHelper.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/support/help/CustomCountDownTimer.java cp/b.java ct/f.java d/c0.java d/j0.java d/k.java d/k0.java d/o0.java d/v0.java d3/d.java d5/n.java d8/i.java d8/t.java d80/c0.java dj/a.java dk/a.java dl/a.java dl/c.java dl/d.java dq/g.java e0/b.java e3/e.java e7/f.java e7/g.java e7/l.java e7/n.java e8/o.java ee/c.java ei/b.java ep/c.java ep/f.java f3/f.java fe/h.java fe/i.java ff/p.java fi/h.java fj/a.java fk/e.java fk/g.java fp/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	fp/c.java fp/e.java fp/g.java fp/h.java fp/k.java fp/m.java g2/a3.java g2/p0.java g5/h.java g7/b.java g7/c.java g9/f.java ge/i.java gj/a.java h/h.java h/i.java h3/e.java h3/j.java h3/o.java h9/b0.java h9/f.java hb/b.java hi/b.java hi/c.java hi/f.java hi/g.java hi/j.java hi/k.java hi/l.java hi/n.java hi/o.java hk/f.java hk/j.java hl/q.java i3/b0.java i3/d.java i3/h.java i3/o.java i3/u.java i3/w.java id0/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ie/g.java ie/j.java ie/l.java ii/e.java ii/f.java ii/h.java ii/i.java ii/j.java ii/m.java ii/q.java ii/t.java il/g.java in/a.java io/sentry/android/core/k0.java io/sentry/e3.java io/sentry/p1.java j7/f.java jf/g.java jj/c.java jk/h.java jn/c.java jn/j.java jn/n.java k20/a.java k5/c0.java k60/b.java ke/b.java ki/d.java ki/f.java ki/k0.java ki/w.java kw/x.java kz/b.java l/f0.java l/h.java l/i.java l/s.java l10/f.java l7/c.java l8/g.java lb/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				li/e.java li/i.java li/i0.java li/j0.java li/l0.java li/o0.java li/u.java li/x.java lm/e.java lz/b.java m3/f.java m8/c.java m8/l.java me/a.java me/g.java me/j.java mk/c.java mk/m.java mv/f.java mx/d.java n0/r.java n6/f.java n6/i.java n8/f.java n8/g.java nb/k.java ng/c.java ng/e0.java ng/l.java ng/r.java nn/f0.java nn/l0.java nn/o.java nn/p.java nn/s0.java nn/u0.java nn/z.java nv/a.java o3/q.java o4/t.java oe/s.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				oe/t.java og/g.java og/h.java og/v.java oi/a.java om/c.java p/y0.java p00/e.java p3/j.java p3/k.java p3/l.java p3/m.java p3/n.java pi/f.java pl/c.java pl/g.java pm/b.java pn/d.java pn/e.java pn/f.java pn/j.java pv/e.java q/f.java q20/b.java q3/c.java q4/c.java q4/g.java qf0/l.java qi/a.java qk/e.java qm/c.java r7/c.java r9/c.java re/h.java rf0/d.java rg/j.java rk/g.java rt/c.java rv/t.java s10/g.java s7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				se/d.java se/e.java se/k.java sg/g.java si/c.java si/e.java siftscience/android/AppStateCollector.java siftscience/android/DevicePropertiesCollector.java siftscience/android/Sift.java siftscience/android/SiftImpl.java siftscience/android/TaskManager.java siftscience/android/Uploader.java sj/b.java sl/d.java t2/v.java t5/g.java t5/i.java t9/b.java tk/a.java tk/g.java tk/h.java u0/j0.java u3/m.java ug/b.java ug/c.java ug/l.java um/c.java up/l.java uq/d.java v/r.java v3/a.java v3/c.java v4/e.java vl/j.java vl/n.java vv/b.java w/j.java w00/c.java w3/f.java w9/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w9/o.java wl/a.java wg/e.java wg/g.java wg/k.java x7/m.java x9/g.java xa/k.java y3/a0.java y3/b.java y3/e.java y3/i2.java y3/j1.java y3/j2.java y3/n1.java y3/o2.java y3/t.java y3/x0.java y7/q.java y90/b.java yg/a.java yh/c.java yh/g.java ym/a.java z30/d.java z4/b.java za/n.java zd/c.java zg/b.java zj/c.java zk/e.java zl/b.java zs/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/d0.java com/bumptech/glide/load/engine/e.java com/bumptech/glide/load/engine/w.java com/mixpanel/android/mpmetrics/PersistentIdentity.java com/sadapay/login/pin/OtpValidationData.java com/sadapay/models/DeleteAttachmentResponseSuccess.java com/sadapay/models/DeleteUserLoginPinRequest.java com/sadapay/models/Flag.java com/sadapay/models/OtpAuthorizationResponse.java com/sadapay/models/RewardStatuses.java com/sadapay/models/UploadAttachmentResponseSuccess.java com/urbanairship/UAirship.java com/urbanairship/channel/AirshipChannel.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java de/m.java e5/a.java ef0/t0.java i20/a.java i20/e.java i20/h.java l20/a.java m8/d.java s2/m0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	ab/h.java cb0/d.java com/apptimize/f.java com/mixpanel/android/mpmetrics/MPDbAdapter.java db0/g.java e0/b.java i5/j.java p/l1.java p/n.java pc0/d.java pc0/n6.java qf/d.java qf/f.java v50/h.java wv/b.java yh/c.java yh/g.java zh/h.java zh/n.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/apptimize/c.java com/urbanairship/l.java ct/f.java g2/l.java uk/b.java v3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/apptimize/cl.java com/apptimize/fd.java com/apptimize/fq.java com/veridiumid/sdk/model/help/EncryptionUtils.java io/sentry/u3.java mx/d.java pi/c.java pm/b.java vl/g.java zl/b.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	ah/b.java com/plaid/internal/zc.java ng/b.java ng/e0.java ng/z.java ug/i.java zo/e.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ap/j.java com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java lf/b.java qf0/d.java qf0/g.java qf0/k.java qf0/l.java
9	MD5 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	ff/n.java ia/x.java pt/r.java r9/c.java tc0/c.java wg/k.java x50/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	bh/y.java com/apptimize/c.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java io/sentry/android/core/b0.java oa0/a.java vc0/x2.java zo/a.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/appsamurai/storyly/exoplayer2/hls/a.java ps/a.java rt/c.java vq/b.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java io/sentry/android/core/b0.java io/sentry/android/core/internal/util/d.java jf/y.java mk/m.java pt/g0.java qk/e.java siftscience/android/DevicePropertiesCollector.java vf/a.java vl/g.java
13	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	la/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	ba0/a.java com/veridiumid/sdk/model/help/AndroidHelper.java io/sentry/android/core/internal/util/d.java siftscience/android/DevicePropertiesCollector.java
15	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	com/apptimize/gn.java k10/c.java s8/e0.java
16	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	vc0/s1.java wr/b.java yf0/a.java
17	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/plaid/link/Plaid$maybeSetWebviewDebugging$2.java
18	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	pc0/x6.java
19	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/plaid/internal/p1.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/45	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
analytics.plaid.com	ok	**IP:** 3.209.42.200 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
graph.s	ok	No Geolocation information available.
.urbanairship.com	ok	No Geolocation information available.
sentry.credolab.com	ok	**IP:** 34.200.33.202 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sadapay-app-production.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gcp-stag-tycho.apptimize.co	ok	**IP:** 34.110.248.224 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.66.41.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sadapay.pk	ok	**IP:** 13.200.123.229 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
md-a-c.apptimize.com	ok	**IP:** 130.211.33.132 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plaid.com	ok	**IP:** 65.9.95.37 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
production.plaid.com	ok	**IP:** 100.26.69.162 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
staging-tycho.apptimize.co	ok	**IP:** 34.110.248.224 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.192.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
wallet-api.urbanairship.com	ok	**IP:** 35.244.226.117 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.73.205 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map
staging-md.apptimize.co	ok	**IP:** 34.120.252.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
tycho.apptimize.com	ok	**IP:** 34.160.204.27 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn.plaid.com	ok	**IP:** 65.9.95.74 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
unikrew-faceoff-licensing.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map
mapi.apptimize.eu	ok	**IP:** 34.120.188.235 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
default.url	ok	No Geolocation information available.
mapi.apptimize.com	ok	**IP:** 34.95.120.110 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
md-a-s.apptimize.com	ok	**IP:** 130.211.33.132 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
g.co	ok	**IP:** 142.250.70.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.linkedin.com	ok	**IP:** 13.107.42.14 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
faceoffmobilebackend.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
dashboard.plaid.com	ok	**IP:** 108.156.2.37 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
md-a-s.apptimize.eu	ok	**IP:** 35.241.43.61 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developers.facebook.com	ok	**IP:** 157.240.227.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
faceoffauthentication.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
md-a-d.apptimize.eu	ok	**IP:** 35.241.43.61 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
console.firebase.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
ns.adobe.com	ok	No Geolocation information available.
.asnapieu.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
staging-mapi.apptimize.co	ok	**IP:** 34.102.214.152 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
open.storyly.io	ok	**IP:** 76.223.41.93 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
javax.xml.xmlconstants	ok	No Geolocation information available.
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.77.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
asset.dev.sadapay.com	ok	**IP:** 108.139.59.104 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
tycho.apptimize.eu	ok	**IP:** 35.186.209.154 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
md-a-c.apptimize.eu	ok	**IP:** 35.241.43.61 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.apptimize.com	ok	**IP:** 65.9.95.110 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
docs.airship.com	ok	**IP:** 34.107.238.88 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
combine.asnapieu.com	ok	**IP:** 35.244.242.208 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.tcsexpress.com	ok	**IP:** 193.123.90.186 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gcp-stag-md.apptimize.co	ok	**IP:** 34.120.252.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
mobile.confsettings.com	ok	**IP:** 54.195.39.4 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
bnc.lt	ok	**IP:** 18.64.141.73 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
.youtube.com	ok	No Geolocation information available.
licensing.prod.veridium-dev.com	ok	**IP:** 35.158.19.174 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 216.58.203.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
remote-data.asnapieu.com	ok	**IP:** 34.96.96.216 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
development.plaid.com	ok	No Geolocation information available.
xml.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
schemas.microsoft.com	ok	**IP:** 13.107.246.63 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 18.172.78.127 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
md-a-d.apptimize.com	ok	**IP:** 130.211.33.132 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.storyly.io	ok	**IP:** 54.246.210.42 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
combine.urbanairship.com	ok	**IP:** 34.107.195.75 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
asset.live.sadapay.com	ok	**IP:** 108.159.80.35 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.183.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ugc-trk.storyly.io	ok	**IP:** 52.212.149.41 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 142.251.42.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bf99042ofw.bf.dynatrace.com	ok	**IP:** 63.34.104.173 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
gcp-stag-mapi.apptimize.co	ok	**IP:** 34.102.214.152 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developer.android.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
unikrew-faceoff-telemetry.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
trk.storyly.io	ok	**IP:** 54.229.3.18 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
facebook.com	ok	**IP:** 157.240.227.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api3.siftscience.com	ok	**IP:** 35.244.208.123 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
scoring.credolab.com	ok	**IP:** 99.83.194.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.183.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.mixpanel.com	ok	**IP:** 130.211.34.183 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
device-api.urbanairship.com	ok	**IP:** 34.128.138.27 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
wallet-api.asnapieu.com	ok	**IP:** 34.96.86.174 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
device-api.asnapieu.com	ok	**IP:** 130.211.7.30 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sandbox.plaid.com	ok	**IP:** 54.88.216.247 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
api.live.sadapay.com	ok	**IP:** 172.64.146.133 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.67.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	**IP:** 108.139.59.26 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
remote-data.urbanairship.com	ok	**IP:** 34.144.204.212 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
hello@sadapay.pk	f30/a.java
u0013android@android.com u0013android@android.com0	ii/o.java
44ab8a40fbdaca489654@sentry.credolab	tc0/b.java

TRACKERS

TRACKER	CATEGORIES	URL
Apptimize	Analytics	https://reports.exodus-privacy.eu.org/trackers/135
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447
Urbanairship		https://reports.exodus-privacy.eu.org/trackers/123

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "0d5ff71b4af94d31a1ba27371eb95e52"
"firebase_database_url" : "https://sadapay-app-production.firebaseio.com"
"google_api_key" : "AIzaSyD6oTdKF9Fd7FqPLT3Rg_WhZj9umtqjukw"
"google_crash_reporting_api_key" : "AIzaSyD6oTdKF9Fd7FqPLT3Rg_WhZj9umtqjukw"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"login_phone_number_user_session_expired_continue" : ""
"plaid_sentry_android_consumer_portal_api_key" : "2264cb9517ec4ddab918b90dd4126ae2"
"plaid_sentry_android_link_sdk_api_key" : "e7bf46248ac14774aecfe3a24811e6b4"
no8Y9OWqo7p/UBRVoWmqrI5s3BWOIBUFH18WsNwrDu2RxGrhDHFMiZd+lbuNHC+OL
a1c600df-4e70-44f5-8755-a45704a63650
n6mkZfpR6LKW9MovYqPR9ESuaLdHP3SuwFFYEDoxpPWSWNY6xaXKnscnhGAA57V/m
0b164dc96b9371ee1a040ba59e4aa9cf
b1efdcdf0bd9f4db72a4651af9c481ba

POSSIBLE SECRETS
AB6162D78BD0F524D904CE19DE76054A9E24726B
145abe7a-ac01-4c7d-bdc7-4811e1967833
bbbb42d6a8058409381c7dda80a54606
652c9100-1cbc-4c09-a22e-52f9258d44c4
93e1ac461cee9254319cdc372fa539bf
1146f4c5ff2c986072906aee3af2535f
5181942b9ebc31ce68dacb56c16fd79f
470fa2b4ae81cd56ecbcda9735803434cec591fa
eyJhY2NfaWQiOjM3ODAsImFwcF9pZCI6NTQ2NywiaW5zX2lkIjoxNTkyMX0
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
c56fb7d591ba6704df047fd98f535372fea00211
cc2751449a350f668590264ed76692694a80308a
namCxnUOQ+Y6eXzXdN1aMKXvzoFF8PoIfsuk7eEgt7YebmRr0c0A8GNYYCdWqFnPj
ndFciGY7e+wKBgAqPlIInHFJnXDgWdmdCb/ahTAaMoTlAHXrbZnaUJT6NSCodKLA0
11de2a00-1c3e-11e4-8c21-0800200c9a66

POSSIBLE SECRETS
C94L1Lt633nSeUMIZA96OZljap2srk
nULwplmesZM54QPWKFwAtSJCwIuyjg9Nt3TEVGCFbX5BpHGjH52/jtaJVjUDQf0jK
5f6b901aaf8b0978eef1c05e18a8a2e1
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
n9DF5A7Yy7FLl98FUGNXLxtYdCwKBgQDN79svtMV4c3oTuM9XdlUEqS81q19qPKRx
ff9d4b6aab15b17c7fd7e9a0ef9f18c7
n39Urc8dq0NT8L6sgCddq9fDczl1lN5HV91GGKmc1wJvpgiHZR3jK9Fqn4JZKuTGJ
ea171960-0d73-11e4-9191-0800200c9a66
207c96f5c0531578ea783ce59c607d01
nNyJi5oEQM9gH3xSkO+9TvGshrpGnvRNuQfDatzFVAoGAeMYmWmQZ3NJEPoiBRJvl
fvQtMwCp50KnMw2boKoduKmMEVuLyfMZhrib2Bg
400933b7a06a2d0cdaabbefb93b3eecc
ab825030-6304-11e3-949a-0800200c9a66
ae2044fb577e65ee8bb576ca48a2f06e
f2872b0a-6ce8-4bd3-8bf8-32bedee3961d
n7G19tcRCV8AjI9Fj5Kqb1HnClLsliPLyn4AqYhOPfbvq8wtIZVyFz21cUM2kiQgM

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
nT0aASZbTlgzMa22HaAKSL5iIFpNr+ijOY5aAAXQ0oScNzpnhHOCOWoxgQKJhssxx
85053bf24bba75239b16a601d9387e17
OFsh69VDqzyB1PnxxxE/pjS3FtH6HWmYsIK8tHLO2+Gqz6XwvFcswAg3UgMP5OccYwkQtbS9YWtabe8GBYH5OA==
nHoMZTmP4L+eoNmDodeeV0wbjBacXHFOLPEC7+k4vX7iVVwvNtOQ2FE2NYNJ7VQtC
da7259bff5ad44ab8a40fbdaca489654
b05e367cc67e6caaadf5a14d5c557670
05725dd7-85e2-490f-a4fe-42f4b0df5d64
eyJhY2NfaWQiOjM3ODAsImFwcF9pZCI6NTQ2NywiaW5zX2lkIjoxNTkyM30
nunWllU+GRih4MpCa8fbgnvF+5JODHj7BfahtFZsq25gq+uk9URlnQBTOIPP6hmZ8
945da4fd5ab0a6bc1d7288101d6ea9a6
ab825031-6304-11e3-949a-0800200c9a66
3Oz9ZEDuz8Ahkh3IDsT3o7mKg2UIWang
DcWRXdehUvkTgefxLBHLeubRh7yA7Ga
eyJhY2NfaWQiOjM3ODAsImFwcF9pZCI6NTQ2NywiaW5zX2lkIjoxNTkyMn0
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

POSSIBLE SECRETS
nQ3kNQk5IH4rEQsyg8X4IebRlX99Z0WsunIxx2+0Dv4LHsCy8iNrhy2PWifJPug/y
128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5
nmrYODfik3I5tVL8FmvzlRraLn4KoR9KdWw5QRyr3VuX4uBzHcTpg/yFjMya+i5d+
6458f6a1f669ea6d73add814
nNuETIXjmfpWyv5cYBkX5cncFyenFuKYbKufUUBaTPwojej1p2i9c8NA1AffsJ/WE
4bfc112e4986489ec8dd7db647ee82f8
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDCZ6SbU0TE0MKM
502f898b-02ff-4db6-88ad-8c181499d383
nq6KZSun80AtQVuRSIib71HXsFf3N149tb0cKCcaxqkZkalTKQFLk9VmWNjLj1H2q
35dc8997e1e42159a519f7f02410cda8
-25403e30e2da5f7f022eee8b01d92d844b4abeb8
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
nIUnQOAPJAgMBAAECggEALckRKI/c82mjWDiYm9PXUJnhkd6zrDHWCyDdTVy3lRye
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
4acb6804-0190-439e-a997-55f6a67adf99
sha256/VdOzyzOGBN+PEjEqW3JtQRHKeiVpXISAK5nPszsg4ek=

POSSIBLE SECRETS
3ad896fa3ec863e554b9890fab536763

PLAYSTORE INFORMATION

Title: SadaPay: Money made simple

Score: 4.397351 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.sadapay.app

Developer Details: SadaPay, SadaPay, None, https://sadapay.pk/, hello@sadapay.pk,

Release Date: Apr 18, 2022 **Privacy Policy:** Privacy link

Description:

Register for your SadaPay wallet and Mastercard virtual debit card to seamlessly move money with confidence. Start spending, sending and requesting payments with zero fees. Use your SadaPay card anywhere Your SadaPay card works anywhere around the world, online and in person. Shop online with the lowest foreign exchange rates in the country without a hiccup. Both our physical and virtual cards work everywhere internationally. No hidden fees or minimum amounts There are no hidden deductions, maintenance charges or local transaction fees with SadaPay. All fees charged are transparently shown on the transaction detail screen. Moreover, there's no minimum amount to have an account with us—big or small, we do it all! Enjoy smooth, transparent payments with peace of mind. Speedy transactions with Raast Raast lets you make speedy transactions from your SadaPay without any charges. You can send and receive money to your SadaPay account by providing an account number or an IBAN. The best way for Pakistani freelancers to get paid internationally Apply for a SadaBiz account and get paid by your client from anywhere in the world. We bring your money home (up to 900,000 PKR per month) at the best exchange rates in Pakistan. Just a few taps and get a customized payment link that your clients can use to pay securely via their Apple Pay, Google Pay, or even their debit or credit card. Retain your earnings in USD All your incoming international payments will be received in SadaBiz, and that too in USD! This means you could not only retain your earnings in dollars, but you can also withdraw them to either your Biz wallet, or to your personal wallet whenever you like. Pay people in seconds for free Pay whoever you want, whenever you want, as many times as you want. It's on us. Also, we don't do SMS and email OTP passwords—that means our transfers are as quick as taking a selfie. Request money easily from your SadaPay friends No more awkward conversations where you have to ask your friend to pay you back. Just request the amount via SadaPay and receive payments without any back-and-forth,, asking your friend to pay you the udhaar back. Say hello to effortless bill payments and top-ups Whether it's electricity, phone network, school, hospital or gym payments, we've got you covered! With a list of 900+ billers, such as IESCO, LESCO, KE, PTCL, and Transworld, you can pay your bills seamlessly through SadaPay. Don't worry if you can't find your payee on this list today—we're adding more billers to this over time. You're in safe hands at SadaPay We're constantly strengthening our security protocols so your money stays safe at SadaPay. We use biometric access (using a fingerprint or Face ID) for quick and easy access to your account information. Also, we protect your funds and sensitive personal data with encryption in-flight and at-rest. Proactive & responsive customer support We think getting through to customer service should be as easy as texting a friend. So our team is here for you 24/7 via in-app live chat. We speak English, Urdu, and Emoji! Also, no worries if you're bad at texting. Give us a call. We'll always respond. Always stay in control Your SadaPay card is 100% secure. It's numberless, so your info is safe (your card numbers are only visible to you in the app). In case you lose your card, you don't need to lose any sleep over it—you can freeze it with the push of a button (and unfreeze it if you find it again). No need to call a helpline or visit a branch. Download & Sign Up Now Move your money the Seedha-Sada Way with SadaPay. Keep up with the latest company updates on our Facebook and Instagram pages. facebook.com/sadapaypk instagram.com/sadapay Reach

out to us at hello@sadapay.pk with ideas, feedback, love, or suggestions on how we can improve the user experience.

SCAN LOGS

Timestamp	Event	Error
2024-10-19 11:10:02	Generating Hashes	OK
2024-10-19 11:10:03	Extracting APK	OK
2024-10-19 11:10:03	Unzipping	OK
2024-10-19 11:10:03	Getting Hardcoded Certificates/Keystores	OK
2024-10-19 11:10:06	Parsing AndroidManifest.xml	OK
2024-10-19 11:10:07	Parsing APK with androguard	OK
2024-10-19 11:10:07	Extracting Manifest Data	OK
2024-10-19 11:10:07	Performing Static Analysis on: SadaPay (com.sadapay.app)	OK

2024-10-19 11:10:07	Fetching Details from Play Store: com.sadapay.app	OK
2024-10-19 11:10:08	Manifest Analysis Started	OK
2024-10-19 11:10:08	Checking for Malware Permissions	OK
2024-10-19 11:10:08	Fetching icon path	OK
2024-10-19 11:10:08	Library Binary Analysis Started	OK
2024-10-19 11:10:08	Reading Code Signing Certificate	OK
2024-10-19 11:10:10	Running APKiD 2.1.5	OK
2024-10-19 11:10:18	Detecting Trackers	OK
2024-10-19 11:10:24	Decompiling APK to Java with jadx	OK
2024-10-19 11:11:19	Converting DEX to Smali	OK
2024-10-19 11:11:19	Code Analysis Started on - java_source	OK

2024-10-19 11:12:22	Android SAST Completed	OK
2024-10-19 11:12:22	Android API Analysis Started	OK
2024-10-19 11:13:05	Android Permission Mapping Started	OK
2024-10-19 11:13:37	Android Permission Mapping Completed	OK
2024-10-19 11:13:45	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 11:13:45	Extracting String data from APK	OK
2024-10-19 11:13:45	Extracting String data from Code	OK
2024-10-19 11:13:45	Extracting String values and entropies from Code	OK
2024-10-19 11:13:52	Performing Malware check on extracted domains	OK
2024-10-19 11:14:18	Saving to Database	OK

---

framework capable of performing static and dynamic analysis.