MOBSF

ANDROID STATIC ANALYSIS REPORT

Soneri Digital (1.8.3)

File Name:	Soneri Digital.apk
Package Name:	com.p3.soneridigital
Scan Date:	Nov. 14, 2024, 9:33 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	21	4	3	2

FILE INFORMATION

File Name: Soneri Digital.apk
Size: 25.89MB
MD5: 77e34d2d4fcd9c3225d93e94e7969dd6
SHA1: b063564047e06bbf1df094cc5f5eee75c1945f6a
SHA256: be28e9e6ee3d06c2c38fe1646cd40c2dd91fec11084118e222db4caa21e1c084

APP INFORMATION

App Name: Soneri Digital
Package Name: com.p3.soneridigital
Main Activity: com.p3.soneridigital.ui.splash.SplashActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 1.8.3

Android Version Code: 85

APP COMPONENTS

Activities: 72
Services: 13
Receivers: 7
Providers: 6
Exported Activities: 3
Exported Services: 1
Exported Receivers: 4
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: 2021-07-02 15:33:30+00:00
Valid To: 2051-07-02 15:33:30+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x362a9dc70250633bf35732766f2bc468c59302b8
Hash Algorithm: sha256
md5: 0ed6ed34d9dcf4a7a3f356ec0a2e4bed
sha1: 271b43837a75e4ba993f957559a2d03d3e44521c
sha256: a7749aca58790f00a9d24e008ff7d581d946b013e6f7b40ddf4fd496f02bd33f
sha512: 6fd09fca29d3e4cc78646475ea40a7442c0a3b344288f402ba335b5614625199b51338bafa3164cb7f47ef8ef248fb9037028ccc1f3e8cd181dcd82a1d3a2ee4
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: bfc8e0b8fd1136d9f168d41f446646694756c2b39d249cae2a27cb604e3e6834
Found 1 unique certificates

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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.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.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ALL_DOWNLOADS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_DOWNLOAD_MANAGER	unknown	Unknown permission	Unknown permission from android reference
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.p3.soneridigital.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check SIM operator check FINDINGS: Anti Debug Code DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler DETAILS: r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

HIGH: 1 | WARNING: 1 | INFO: 2 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	soneri.cloudasset.com soneriqa.cloudasset.com apiuat.soneribank.com apiprod.soneribank.com mbanking.soneridigital.com	info	Domain config is configured to trust bundled certs @raw/pinning_pubkey_mbanking_soneridigital_com.
2	soneri.cloudasset.com soneriqa.cloudasset.com apiuat.soneribank.com apiprod.soneribank.com mbanking.soneridigital.com	info	Domain config is configured to trust bundled certs @raw/certificate_prod.

NO	SCOPE	SEVERITY	DESCRIPTION
3	soneri.cloudasset.com soneriqa.cloudasset.com apiuat.soneribank.com apiprod.soneribank.com mbanking.soneridigital.com	warning	Domain config is configured to trust system certificates.
4	soneri.cloudasset.com soneriqa.cloudasset.com apiuat.soneribank.com apiprod.soneribank.com mbanking.soneridigital.com	high	Domain config is configured to trust user installed certificates.

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: **8** | 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.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.p3.soneridigital.ui.applyAccount.ui.login.DOBLoginActivity) 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.p3.soneridigital.ui.applyAccount.ui.ApplyAccountDashboard) 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	Activity (com.p3.soneridigital.ui.applyAccount.ApplyAccountActivity) 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
6	Broadcast Receiver (com.p3.soneridigital.utils.MySMSBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.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.
7	Broadcast Receiver (com.p3.soneridigital.utils.sms_retrival.SMSReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.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.
8	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]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	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: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/f.java a0/o.java a1/g.java a1/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/i.java a2/a.java a2/c.java a3/a.java a5/j.java a5/k.java a7/a.java a8/a.java a9/a.java aa/b.java b1/h.java b1/i.java b1/j.java b1/k.java b1/l.java b1/q.java b2/a.java b2/c.java b3/c.java b3/e.java b3/u.java b7/f8.java b7/i3.java b7/n3.java b7/q7.java be/o.java c6/a.java c8/f.java ce/h.java cf/b.java cg/f.java cg/p.java cj/f.java com/archit/calendardaterangepicker/customviews/DateRangeMonthView.java com/bumptech/glide/b.java com/bumptech/glide/k.java com/bumptech/glide/l.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/GlideExceptio n.java com/bumptech/glide/load/resource/bitmap/Def aultImageHeaderParser.java com/ncorti/slidetoact/SlideToActView.java com/p3/soneridigital/core/base/SoneriApp.java com/p3/soneridigital/fcm/MyFirebaseMessagin gService.java com/p3/soneridigital/ui/accountdetail/Account DetailActivity.java com/p3/soneridigital/ui/applyAccount/ApplyAcc ountActivity.java com/p3/soneridigital/ui/applyAccount/ui/Apply AccountDashboard.java com/p3/soneridigital/ui/applyAccount/ui/login/ DOBLoginActivity.java com/p3/soneridigital/ui/dashboard/Dashboard ParallaxActivity.java com/p3/soneridigital/ui/digitalbankinglimit/Digi talBankingLimit.java com/p3/soneridigital/ui/dynamicformLists/Dyn amicFormListing.java com/p3/soneridigital/ui/dynamicformcreation/ DynamicFormCreation.java com/p3/soneridigital/ui/dynamicforms/PayOrd er.java com/p3/soneridigital/ui/editbeneficiary/EditBen eficiaryActivity.java com/p3/soneridigital/ui/forgetpassword/fragme nts/smsotp/FragmentSMSOTP.java com/p3/soneridigital/ui/forgetpassword/fragme nts/termsandcondiion/FragmentTermsAndCond ition.java com/p3/soneridigital/ui/forgetusername/fragm ents/smsotp/FragmentSMSOTP.java com/p3/soneridigital/ui/locatoractivity/Locator Activity.java com/p3/soneridigital/ui/login/LoginActivity.java com/p3/soneridigital/ui/merchantpaymenttrans fer/MerchantPaymentTransfer.java com/p3/soneridigital/ui/newFundTransfer/New

NO	ISSUE	SEVERITY	STANDARDS	FILES
				FundTransferActivity.java com/p3/soneridigital/ui/newPayee/NewPayeeActivity.java com/p3/soneridigital/ui/newSaveBeneficiary/NewSavedBeneficiaryActivity.java com/p3/soneridigital/ui/newbeneficiacrypayment/NewBeneficiaryPaymentActivity.java com/p3/soneridigital/ui/newbeneficiary/NewBeneficiaryActivity.java com/p3/soneridigital/ui/newpayment/NewBillPaymentActivity.java com/p3/soneridigital/ui/newpayment/NewPaymentActivity.java com/p3/soneridigital/ui/newpayment/newbillpayee/NewBillPayeeActivity.java com/p3/soneridigital/ui/newraastbeneficiary/NewRaastBeneficiaryActivity.java com/p3/soneridigital/ui/notification/NotificationActivity.java com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java com/p3/soneridigital/ui/raastpaymentdetails/RaastPaymentDetailsActivity.java com/p3/soneridigital/ui/savedcontactsdetails/SavedContactDetailActivity.java com/p3/soneridigital/ui/settings/fragments/devicesetting/DeviceSettingFragment.java com/p3/soneridigital/ui/settings/fragments/profilesetting/ProfileSettingFragment.java com/p3/soneridigital/ui/settings/fragments/verificationsetting/VerificationSettingFragment.java com/p3/soneridigital/ui/signupprocess/fragments/fargmentbiometric/FragmentSignUpBiometric.java com/p3/soneridigital/ui/signupprocess/fragments/fragmenttermsandcondition/FragmentTermsAndCondition.java com/p3/soneridigital/ui/smsotp/fragmentsmsotp/FragmentSMSOTP.java com/p3/soneridigital/ui/splash/SplashActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/p3/soneridigital/ui/transactiondeatail/TransactionDetailActivity.java com/p3/soneridigital/ui/transactionhistory/TransactionHistoryActivity.java com/p3/soneridigital/ui/transactionhistory/a.java com/p3/soneridigital/ui/transfer/TransferActivity.java com/p3/soneridigital/ui/zakatdetails/ZakatDetailsActivity.java com/p3/soneridigital/utils/MenuHidingEditText.java com/p3/soneridigital/utils/PastEnableEditText.java com/p3/soneridigital/utils/h.java com/shockwave/pdfium/PdfiumCore.java com/unikrew/faceoff/fingerprint/SecureStorage/b.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/LoggingVeridium.java com/veridiumid/sdk/crypto/TransactionSigningHelper.java com/veridiumid/sdk/defaultdata/DataStorage.java com/veridiumid/sdk/defaults/biometricsettingsdefaultui/BiometricSettingsFragment.java com/veridiumid/sdk/fourf/ExportConfig.java com/veridiumid/sdk/fourf/FourFLoader.java com/veridiumid/sdk/fourf/VeridiumSDKFourFInitializer.java com/veridiumid/sdk/fourf/camera/Camera1PreviewView.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/fourf/camera/ImageTaggingQueue.java com/veridiumid/sdk/fourf/ui/FourFUIFragment.java com/veridiumid/sdk/fourf/ui/InstructionalDialog.java com/veridiumid/sdk/internal/licensing/LicensingRepository.java com/veridiumid/sdk/licensing/LicensingManager.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/engine/processing/handling/impl/AdaptiveEnrollmentHandler.java com/veridiumid/sdk/model/biometrics/engine/processing/handling/impl/AuthenticationHandler.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/model/help/Devices.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java com/veridiumid/sdk/support/help/CustomCountDownTimer.java com/veridiumid/sdk/support/ui/AspectRatioSafeFrameLayout.java d3/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d5/d.java d6/j.java d6/k.java d7/a.java d9/c.java d9/d.java de/b.java dg/i.java dg/n.java e/e.java e/f.java e/g.java e/v.java e/w.java e3/a0.java e3/b.java e3/c.java e3/i.java e3/k.java e3/l.java e3/p.java e3/x.java e4/b.java e4/c.java e5/j.java e7/a.java ed/b.java ee/g.java ee/g1.java ee/j.java ee/o0.java ee/w.java f1/g.java f1/l.java fd/e0.java fd/m0.java fd/n1.java fd/s.java fd/w.java fd/w0.java g4/k.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	g6/h.java g9/a.java gg/j.java h6/c.java h7/g.java h9/a.java hd/c1.java hd/c4.java hd/f2.java hd/j2.java hd/j3.java hd/l0.java hd/l2.java hd/m.java hd/m1.java hd/o1.java hd/p1.java hd/s.java hi/d0.java i/f.java i1/c.java i2/a.java i3/a.java i3/i.java ie/h.java ie/i.java ig/e.java j2/s.java j2/u.java j5/a.java j5/b.java j8/g.java jd/f.java jd/j.java k/a0.java k/a1.java k/d1.java k/h.java k/i0.java k/k0.java k/l0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k/o0.java k/p0.java k/v.java k1/a.java k1/b.java k1/e0.java k1/g0.java k1/o0.java k1/r.java k2/b.java k2/f.java k3/k.java k3/l.java k3/o.java k3/q.java k5/m.java k8/g.java k8/j.java k8/m.java kj/u.java ld/d.java ld/g.java ld/k.java ld/n.java ld/s.java m4/a.java md/q0.java n1/k.java n2/h.java n2/o.java n3/i.java n8/c.java nd/a.java ne/c.java o1/b.java o3/h.java o4/f.java od/i.java od/j.java oj/c.java org/conscrypt/Platform.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/conscrypt/ct/CTVerifier.java p0/c.java p2/d.java pd/s0.java pd/x0.java q0/d.java q0/e.java q0/g.java q0/h.java q0/i.java q0/k.java q0/l.java q0/m.java q0/n.java q0/q.java q0/r.java q1/c.java q5/e.java q5/o.java q9/d.java qa/c.java qa/u.java qa/w.java qd/f.java qd/h.java qd/i.java qd/k.java qd/o.java qg/e.java r/d0.java r/l.java r/v.java r/x.java r/y.java r/z.java r0/d.java r5/b.java r5/c.java r5/d.java r5/h.java r5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r5/l.java r5/m.java r5/n.java r5/q.java r5/r.java r5/s.java r5/u.java r5/v.java r5/y.java r8/e.java r8/k.java rd/a.java s0/f.java s3/a.java s5/b0.java s5/e.java s5/f.java s5/h.java s5/i.java s5/k.java s5/s.java s5/w.java s6/b0.java s8/b.java s8/c.java s9/b.java sg/a.java sg/g.java t2/a.java t3/c.java t3/e.java t8/b.java t9/c.java td/a.java u0/a.java u0/e.java u1/a.java u2/d.java u2/e.java u5/c0.java u5/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u5/a.java u5/d1.java u5/e0.java u5/s.java u5/w0.java u6/r9.java u8/c.java u8/d.java ud/a.java uf/m.java uh/b0.java uh/o.java v/d.java v/k.java v/q.java v4/n.java v5/b.java v5/b0.java v5/d1.java v5/f.java v5/f1.java v5/m.java v5/m0.java v5/t0.java v5/x0.java v5/y.java v8/c.java v9/a.java v9/a0.java v9/b0.java v9/c.java v9/c0.java v9/e.java v9/f0.java v9/g0.java v9/j0.java v9/l.java v9/l0.java v9/m.java v9/q.java v9/r.java v9/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v9/t.java v9/u.java v9/v.java v9/z.java va/j.java va/l.java vf/c.java vf/m.java vg/g.java w/d.java w2/a.java w8/c0.java w8/d0.java w8/e.java w8/f0.java w8/h0.java w8/j0.java w8/k.java w8/l.java w8/m.java w8/o.java w8/p.java w8/t.java w8/x.java w8/y.java w8/z.java wd/a.java wf/c.java wf/d.java wh/e.java wj/h.java x/j0.java x2/j.java x2/k.java x2/m.java x2/z.java x4/c.java x6/b.java x8/b.java x8/e.java xa/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xa/g.java xd/d.java xf/a.java xf/b.java xf/y.java xj/d.java y/e0.java y/v.java y0/d.java y0/e.java y0/k.java y0/w.java y2/i.java y2/j.java y5/a.java y6/n.java ya/d0.java ya/k.java ya/o.java ya/o0.java ya/p.java ya/s.java ya/y.java yf/d.java yf/f.java yf/g.java yf/m.java yh/i.java yh/t.java z0/a.java z2/d.java z2/i.java z4/i.java z7/d.java zf/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/p3/soneridigital/ui/accountdetail/AccountDetailActivity.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java hd/r.java qd/j.java vg/g.java yh/l.java
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/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java com/veridiumid/sdk/internal/licensing/domain/model/License.java com/veridiumid/sdk/internal/licensing/domain/model/SdkLicense.java ic/b.java jb/e.java jb/e0.java jb/g.java jb/h.java mb/d0.java mb/f0.java mb/g1.java mb/h1.java mb/j1.java mb/k1.java mb/l.java mb/n.java mb/n1.java mb/n2.java mb/o.java mb/q1.java mb/r1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mb/s2.java mb/t0.java mb/u1.java mb/v2.java mb/w.java mc/e.java ob/b1.java ob/w0.java ob/y0.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java sc/c.java v2/f.java x2/f.java x2/q.java x2/w.java yc/a.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java wj/c.java wj/d.java wj/g.java wj/h.java yh/z.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/p3/soneridigital/ui/splash/SplashActivity.java com/veridiumid/sdk/model/help/AndroidHelper.java j2/s.java j8/g.java w8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	b7/e8.java b7/h3.java b7/j.java b7/k.java b7/q7.java e5/j.java e5/l.java e5/m.java e5/n.java e5/o.java e5/p.java x/t0.java z/b1.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
8	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	com/unikrew/faceoff/fingerprint/SecureStorage/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	u6/r9.java
10	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	b2/c.java hd/r.java qd/j.java qd/o.java s9/c.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java
12	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	b7/x7.java ru/lazard/tamperingprotection/TamperingProtection.java
13	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	b7/x7.java com/p3/soneridigital/utils/h.java ej/a.java ej/b.java fj/a.java k5/d.java k6/c.java o8/a.java s/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java
15	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	fd/p1.java
16	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/veridiumid/sdk/model/help/EncryptionUtils.java s9/b.java t9/c.java v9/q.java w8/e.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b2/c.java com/p3/soneridigital/ui/dashboard/DashboardParallaxActivity.java com/p3/soneridigital/ui/dynamicformcreation/DynamicFormCreation.java com/p3/soneridigital/ui/editbeneficiary/EditBeneficiaryActivity.java com/p3/soneridigital/ui/newPayee/NewPayeeActivity.java com/p3/soneridigital/ui/newbeneficiary/NewBeneficiaryActivity.java com/p3/soneridigital/ui/newraastbeneficiary/NewRaastBeneficiaryActivity.java com/p3/soneridigital/ui/notification/NotificationActivity.java com/p3/soneridigital/ui/promotions/PromoActivity.java com/p3/soneridigital/ui/settings/fragments/profilesetting/ProfileSettingFragment.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/LoggingVeridium.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java gb/k.java hd/r.java hi/r.java ie/n.java qd/j.java qd/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/p3/soneridigital/ui/accountdetail/AccountDetailActivity.java com/p3/soneridigital/ui/cardlist/CardListActivity.java com/p3/soneridigital/ui/cardtransaction/CardTransactionHistoryActivity.java com/p3/soneridigital/ui/dashboard/DashboardParallaxActivity.java com/p3/soneridigital/ui/editbeneficiary/EditBeneficiaryActivity.java com/p3/soneridigital/ui/editbillpayee/EditBillPayeeActivity.java com/p3/soneridigital/ui/editfavourite/EditFavouriteActivity.java com/p3/soneridigital/ui/favouritedetail/FavoriteDetailActivity.java com/p3/soneridigital/ui/login/LoginActivity.java com/p3/soneridigital/ui/newFundTransfer/NewFundTransferActivity.java com/p3/soneridigital/ui/newPayee/NewPayeeActivity.java com/p3/soneridigital/ui/newSaveBeneficiary/NewSavedBeneficiaryActivity.java com/p3/soneridigital/ui/newbeneficiary/NewBeneficiaryActivity.java com/p3/soneridigital/ui/newpayment/NewBillPaymentActivity.java com/p3/soneridigital/ui/newpayment/NewPaymentActivity.java com/p3/soneridigital/ui/newraastbeneficiary/NewRaastBeneficiaryActivity.java com/p3/soneridigital/ui/newraastpaymenttransfer/NewRaastPaymentTransferActivity.java com/p3/soneridigital/ui/newzakattransfer/NewZakatTransferActivity.java com/p3/soneridigital/ui/notification/NotificationActivity.java com/p3/soneridigital/ui/promotions/PromoActivity.java com/p3/soneridigital/ui/raastaliasdetails/RaastAliasDetailActivity.java com/p3/soneridigital/ui/raastpaymentdetails/RaastPaymentDetailsActivity.java com/p3/soneridigital/ui/savedcontactsdetails/SavedContactDetailActivity.java com/p3/soneridigital/ui/settings/fragments/profilesetting/ProfileSettingFragment.java com/p3/soneridigital/ui/transactiondeatail/TransactionDetailActivity.java com/p3/soneridigital/ui/transactionhistory/TransactionHistoryActivity.java com/p3/soneridigital/ui/zakatdetails/ZakatDetailsActivity.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java r/d0.java v9/m.java v9/t.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java pd/y0.java t9/c.java x4/c.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java pd/y0.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java j5/b.java pd/y0.java q5/e.java t9/c.java x4/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	b7/a6.java com/p3/soneridigital/ui/accountdetail/AccountDetailActivity.java com/p3/soneridigital/ui/applyAccount/ApplyAccountActivity.java com/p3/soneridigital/ui/cheques/ChequeActivity.java com/p3/soneridigital/ui/locatoractivity/LocatorActivity.java com/p3/soneridigital/ui/raastpaymentdetails/RaastPaymentDetailsActivity.java com/p3/soneridigital/ui/savedcontactsdetails/SavedContactDetailActivity.java com/p3/soneridigital/ui/scanAndPay/ScanAndPayActivity.java com/p3/soneridigital/ui/transactiondeatail/TransactionDetailActivity.java com/p3/soneridigital/ui/transactionhistory/TransactionHistoryActivity.java com/p3/soneridigital/ui/zakatdetails/ZakatDetailsActivity.java com/p3/soneridigital/utils/h.java de/c.java ed/a.java ed/b.java gb/h.java gb/l.java hd/n1.java hd/v2.java qd/f.java qd/h.java r/y.java rd/a.java s5/f.java uf/b.java v9/c.java yd/b.java yd/z.java
00125	Check if the given file path exist	file	com/p3/soneridigital/ui/accountdetail/AccountDetailActivity.java com/p3/soneridigital/ui/splash/SplashActivity.java j2/s.java r/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/p3/soneridigital/ui/scanAndPay/ScanAndPayActivity.java ed/a.java ed/b.java gb/h.java gb/l.java hd/v2.java s5/f.java uf/b.java v9/c.java yd/b.java yd/z.java
00036	Get resource file from res/raw directory	reflection	com/p3/soneridigital/ui/scanAndPay/ScanAndPayActivity.java k/o0.java s5/f.java v9/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b1/j.java b1/k.java b1/q.java b3/g.java b9/f.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java d2/c.java d2/f.java e/v.java e3/q.java j2/s.java nj/z.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java s9/c.java t2/a.java t2/b.java u1/a.java v/d.java vj/a.java
00147	Get the time of current location	collection location	com/p3/soneridigital/ui/dashboard/DashboardParallaxActivity.java com/p3/soneridigital/ui/locatoractivity/LocatorActivity.java e/f.java
00108	Read the input stream from given URL	network command	b7/a6.java b7/r3.java
00075	Get location of the device	collection location	com/p3/soneridigital/ui/locatoractivity/LocatorActivity.java e/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	com/p3/soneridigital/ui/locatoractivity/LocatorActivity.java e/f.java
00115	Get last known location of the device	collection location	com/p3/soneridigital/ui/locatoractivity/LocatorActivity.java e/f.java
00191	Get messages in the SMS inbox	sms	com/p3/soneridigital/utils/h.java k/o0.java
00192	Get messages in the SMS inbox	sms	qd/h.java yh/l.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java wj/b.java wj/h.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java wj/b.java wj/h.java
00112	Get the date of the calendar event	collection calendar	com/p3/soneridigital/utils/h.java
00189	Get the content of a SMS message	sms	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java qg/e.java
00188	Get the address of a SMS message	sms	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java qg/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java qg/e.java
00187	Query a URI and check the result	collection sms calllog calendar	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java qg/e.java
00201	Query data from the call log	collection calllog	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java qg/e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/p3/soneridigital/ui/raastmanagement/RaastManagementActivity.java g1/d.java hi/p.java
00014	Read file into a stream and put it into a JSON object	file	s9/c.java
00012	Read data and put it into a buffer stream	file	org/conscrypt/DefaultSSLContextImpl.java u1/a.java
00096	Connect to a URL and set request method	command network	pd/y0.java x4/c.java
00114	Create a secure socket connection to the proxy address	network command	rj/i.java
00005	Get absolute path of file and put it to JSON object	file	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00028	Read file from assets directory	file	com/veridiumid/sdk/model/help/AssetsHelper.java
00094	Connect to a URL and read data from it	command network	a9/a.java
00002	Open the camera and take picture	camera	com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00183	Get current camera parameters and change the setting.	camera	com/veridiumid/sdk/fourf/camera/FourFCamera1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/107501321551/namespaces/firebase:fetch?key=AIzaSyBvSSx9ilBpQ87xUNA0Sgd7i3gURoXnqLg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.GET_TASKS, android.permission.READ_CONTACTS, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	3/44	android.permission.CALL_PHONE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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

DOMAIN	STATUS	GEOLOCATION
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
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 108.177.119.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **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
maps.google.com	ok	**IP:** 142.250.187.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
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

DOMAIN	STATUS	GEOLOCATION
www.soneribank.com	ok	**IP:** 104.18.11.111 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 172.217.169.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.187.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.251.140.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 142.250.184.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.9.35 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map
instagram.com	ok	**IP:** 157.240.9.174 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map
developer.android.com	ok	**IP:** 142.251.140.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 216.58.212.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
update.crashlytics.com	ok	**IP:** 142.250.187.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
reports.crashlytics.com	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 142.250.187.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
wa.me	ok	**IP:** 157.240.9.53 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.whatsapp.com	ok	**IP:** 157.240.9.53 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.251.141.34 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
soneri-assets.s3.me-south-1.amazonaws.com	ok	**IP:** 52.95.172.62 **Country:** Bahrain **Region:** Al 'Asimah **City:** Manama **Latitude:** 26.215361 **Longitude:** 50.583199 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.251.140.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 216.58.212.36 **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.
docs.google.com	ok	**IP:** 142.251.141.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 142.251.140.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	s5/r.java
example@email.com complaint.suggestion@soneribank.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
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

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "dbd7b68016434adeb2c02fe2d9d8c53e"

POSSIBLE SECRETS
"credentials" : "Credentials"
"gmapi" : "AIzaSyDX2Q6R7ZcR8z5iBsXZV3uAZxoHctbP_Ko"
"google_api_key" : "AIzaSyBvSSx9ilBpQ87xUNA0Sgd7i3gURoXnqLg"
"google_crash_reporting_api_key" : "AIzaSyBvSSx9ilBpQ87xUNA0Sgd7i3gURoXnqLg"
"password" : "Password"
"username" : "Username"
sha256/HeF1u4dHs2DcepCOm0pIPTR7B0Gh1X0HcRcY8Hi2rig=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
sha256/Ko8tivDrEjiY90yGasP6ZpBU4jwXvHqVvQI0GS3GNdA=
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
sha256/lH8RVpSJLj3jdBCr4PlA360uhRAyvapH+rvi0GnZBwI=
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
sha256/Wec45nQiFwKvHtuHxSAMGkt19k+uPSw9JlEkxhvYPHk=
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
sha256/IB7ihC4ThcIB0VCYy+YwVMzBEzR3NXZCmkmceCpWNTI=
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
5f855877f69b5a75d7ec5e36
470fa2b4ae81cd56ecbcda9735803434cec591fa
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

PLAYSTORE INFORMATION

Title: Soneri Digital

Score: 4.4 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.p3.soneridigital

Developer Details: Soneri Bank Limited, Soneri+Bank+Limited, None, https://www.soneribank.com/, complaint.suggestion@soneribank.com,

Release Date: Nov 10, 2021 **Privacy Policy:** Privacy link

Description:

Soneri Bank always bring innovative solutions to strengthen its customer relationship via our brand proposition of 'Roshan Har Qadam'. In continuation of these aspirations, a fresh new Digital App is launched. All your banking needs is now on your fingertips. Packed with all smart features, Soneri Digital App provides secure on the go access to your account and providing safer and quicker access to all your banking needs. REGISTRATION & LOGIN MADE EASY All New Soneri Digital offers quick registration and login with biometric and face recognition support, we provide easy and safe authentication process as your security is our priority. Salient Features! - Feel secure when you login with your Finger print - Manage multiple accounts in one place - Check your balance and view your account statement - Transfer both local i.e. (within bank) and between switch member banks i.e. (Interbank) - Pay Zakat and Donation - Pay your utilities, Telecos and Govt. Bills -Top-up your mobile - Manage your contacts - View you activity logs - Locate Soneri ATM and Branches Permissions! - Camera & Gallery, for profile picture - Location, to locate nearest ATM and Branches Contact Us! Please feel free to contact us via any of the following channels for all your queries and feedback: UAN: +92 021-111-766-374 (SONERI) Email: complaint.suggestion@soneribank.com Facebook, https://www.facebook.com/SoneriBankPK/

SCAN LOGS

Timestamp	Event	Error

2024-11-14 21:33:07	Generating Hashes	OK
2024-11-14 21:33:07	Extracting APK	OK
2024-11-14 21:33:07	Unzipping	OK
2024-11-14 21:33:08	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 21:33:08	Parsing APK with androguard	OK
2024-11-14 21:33:10	Parsing AndroidManifest.xml	OK
2024-11-14 21:33:10	Extracting Manifest Data	OK
2024-11-14 21:33:10	Performing Static Analysis on: Soneri Digital (com.p3.soneridigital)	OK
2024-11-14 21:33:10	Fetching Details from Play Store: com.p3.soneridigital	OK
2024-11-14 21:33:13	Manifest Analysis Started	OK
2024-11-14 21:33:13	Reading Network Security config from network_security_config.xml	OK

2024-11-14 21:33:13	Parsing Network Security config	OK
2024-11-14 21:33:13	Checking for Malware Permissions	OK
2024-11-14 21:33:13	Fetching icon path	OK
2024-11-14 21:33:13	Library Binary Analysis Started	OK
2024-11-14 21:33:13	Reading Code Signing Certificate	OK
2024-11-14 21:33:13	Running APKiD 2.1.5	OK
2024-11-14 21:33:16	Detecting Trackers	OK
2024-11-14 21:33:17	Decompiling APK to Java with JADX	OK
2024-11-14 21:33:33	Converting DEX to Smali	OK
2024-11-14 21:33:33	Code Analysis Started on - java_source	OK
2024-11-14 21:33:40	Android SAST Completed	OK

2024-11-14 21:33:40	Android API Analysis Started	OK
2024-11-14 21:33:45	Android API Analysis Completed	OK
2024-11-14 21:33:45	Android Permission Mapping Started	OK
2024-11-14 21:33:52	Android Permission Mapping Completed	OK
2024-11-14 21:33:54	Email and URL Extraction Completed	OK
2024-11-14 21:33:54	Android Behaviour Analysis Started	OK
2024-11-14 21:34:01	Android Behaviour Analysis Completed	OK
2024-11-14 21:34:01	Extracting String data from APK	OK
2024-11-14 21:34:02	Extracting String data from Code	OK
2024-11-14 21:34:02	Extracting String values and entropies from Code	OK
2024-11-14 21:34:04	Performing Malware check on extracted domains	OK

2024-11-14 21:34:18	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.