MOBSF

ANDROID STATIC ANALYSIS REPORT

Client Portal (1.7.5)

File Name:	com.simplepractice.clients_1867.apk
Package Name:	com.simplepractice.clients
Scan Date:	Sept. 1, 2025, 8:57 a.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	22	2	3	2

FILE INFORMATION

File Name: com.simplepractice.clients_1867.apk
Size: 39.27MB
MD5: 6c272c04f35faceea75bebff4753ce61
SHA1: 72fa9b4a7fef814a4f1e0b5d86245e8a9783fcbd
SHA256: acf95c73bae1d1e8eab4e4afc3b91b7e038bb261a5cece0f165ae6d0abefe4a7

APP INFORMATION

App Name: Client Portal
Package Name: com.simplepractice.clients
Main Activity: com.simplepractice.clients.module.splash.SplashScreenActivity
Target SDK: 35
Min SDK: 24
Max SDK:
Android Version Name: 1.7.5

Android Version Code: 1867

APP COMPONENTS

Activities: 48
Services: 8
Receivers: 3
Providers: 6
Exported Activities: 9
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
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: 2022-10-19 20:33:04+00:00
Valid To: 2052-10-19 20:33:04+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xeb5880001f1f97b033fdfdfa1115bfce32467712
Hash Algorithm: sha256
md5: 466c329cc02c89a31ad5eb14b0c94e71
sha1: 831c3c3b2eb098299c447086dc5592273f6bfb1c
sha256: 57d2e1d57038f67e441c8af50195dce08cc0f86e4177f43f311602fd4887c14f
sha512: f823b9619fe5d10feebcdc328b2e4cdbb224afa87d4e3c4ec11167b57dae196a2f8ee16dc906606422b1afde8644d7c0005885b19d7efa8072854d540d941302
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 4cfb095ed953449cec8971e7cf259f2894f60102b6f04e438d6eba942d7212a2
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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_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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.simplepractice.clients.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
possible ro.secure 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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT 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>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
Build.HARDWARE check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.simplepractice.clients.module.login.LoginRouterActivity	Schemes: https://, Hosts: clientsecure.me, clientportalandroid.page.link, Path Patterns: /client-portal-api/sign-in/.*, /client-app.*,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.simplepractice.clients,
com.simplepractice.auth.AuthActivity	Schemes: telehealth-internal://,

ACTIVITY	INTENT
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.simplepractice.clients/success, /com.simplepractice.clients/cancel, Path Prefixes: /com.simplepractice.clients/authentication_return, /com.simplepractice.clients,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.simplepractice.clients.module.login.LoginRouterActivity) 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.simplepractice.clients.module.dashboard.ui.DashboardActivity) 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	Activity (net.openid.appauth.RedirectUriReceiverActivity) 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.
7	Activity (com.simplepractice.clients.module.lock.LockScreenActivity) 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.
8	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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.
9	Activity (com.simplepractice.auth.AuthActivity) 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 (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) 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	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
12	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
13	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
14	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.
15	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: 1 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	Ae/C0011w.java Ae/C0040z2.java Ae/C0085q1.java Ae/C0121z2.java Ae/H1.java Ae/K0.java Ae/q1.java B0/C0133f0.java B1/Q.java Bf/N.java Bf/r.java Ee/d.java Le/m.java Le/t.java Oe/d.java Oe/e.java Oe/f.java Oe/h.java Pe/C0210k0.java Pe/D0.java Pe/j0.java Pe/z.java Qe/C0278i.java Qe/C0843i.java Qe/C0854u.java Qe/u.java U3/h.java Ud/C1192t0.java Ud/t0.java Xf/C0340p.java Xf/C0341q.java Ye/A.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cl/C0511o.java com/simplepractice/clients/settings/PreferenceRepository.java fe/C0512p.java fe/C2756p.java fe/S.java gf/e.java he/x.java m3/C1488b.java m3/C3589b.java of/C3965a.java of/a.java wf/C5055p.java wf/p.java
				A/b.java A/f.java A/i.java A5/F.java A6/d.java Ad/d.java Af/g.java Af/h.java Af/l.java Ai/a.java B/a.java B2/b.java B2/c.java B2/g.java C1/z.java C2/d.java C4/a.java D/G.java D/N.java D/e.java De/C0042c.java Df/e.java E/d.java E5/b.java E5/g.java E5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				F4/a.java F5/j.java F5/n.java F6/g.java G4/e.java G6/h.java G6/j.java G6/o.java G6/p.java H/e.java H3/d.java I5/d.java I5/v.java Ie/e.java J2/c.java K2/b.java K4/a.java Ki/C.java L2/C0158c.java L2/C0168p.java L2/C0169q.java L2/I.java L7/b.java M/d.java M/j.java M/r.java Me/l.java N2/c.java N2/e.java Ni/d.java Ni/n.java O/a.java O1/c.java Oi/c.java P/e.java P0/f.java P1/e.java P2/g.java Q1/i.java Q5/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Q5/b.java Q5/j.java R5/m.java Rc/d.java T1/f.java T1/k.java T1/p.java T1/q.java T4/a.java U1/C0288d.java U1/D.java U1/i.java U1/v.java U1/x.java U1/z.java U4/a.java V3/a.java V4/AbstractC0340c.java V4/AbstractC1244c.java V4/E.java V4/y.java W1/e.java W1/f.java X1/a.java Xg/O.java Y1/AbstractC0451j.java Y1/AbstractC1510j.java Y1/C0449h.java Y1/K.java Y1/V.java Y4/c.java Z1/f.java Z1/h.java Z2/j.java Z5/f.java Z5/h.java a2/AbstractC1640b.java a2/b.java a2/q.java b2/C0706h.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	b2/C0707i.java b2/f.java b2/g.java b2/j.java bg/d.java bg/t.java c2/AbstractC2036c.java c2/c.java ci/C0072q0.java com/biba/bibacommon/ProxyConfig.java com/bugsnag/android/B.java com/bugsnag/android/C0746b0.java com/bugsnag/android/C0778x.java com/bugsnag/android/p.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java com/simplepractice/clients/core/dialog/bottom/b.java com/simplepractice/clients/module/dashboard/ui/DashboardActivity.java com/simplepractice/clients/module/lock/LockScreenActivity.java com/simplepractice/shared/ui/session/ui/waitingroom/WaitingRoomControlsDialogView.java com/stripe/android/camera/a.java com/stripe/android/stripecardscan/scanui/r.java com/twilio/video/Logger.java com/xodee/client/audio/audioclient/AudioClient.java d/RunnableC0922k.java d6/B.java d6/C.java d6/E.java d6/u.java d6/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dh/C0463b.java e6/C1348c.java e6/l.java e6/v.java f1/c.java f6/C1084c.java f6/C1087f.java g/j.java g2/m.java h2/AbstractC1191a.java i/AbstractActivityC1219m.java i/AbstractC1223q.java i/AbstractC3108q.java i/C1198A.java i/LayoutInflaterFactory2C1201D.java i/t.java jd/AbstractC0614h.java jd/C3252d.java jd/d.java k4/d.java k4/j.java kd/C0658f.java kd/C0660h.java kd/t.java l2/AbstractC1398L.java l2/AbstractC1410Y.java l2/AbstractC1416c0.java l2/AbstractC3454Y.java l2/AbstractC3461c0.java l2/C1413b.java l2/C3485s.java l2/J0.java l2/r0.java l2/s.java l2/s0.java l2/w0.java lb/c.java m/C1458i.java m/j.java ma/C0685b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mg/f.java mi/E.java n/f.java n/l.java n1/w.java net/danlew/android/joda/a.java o/A1.java o/AbstractC1627h0.java o/AbstractC3792h0.java o/C1635l0.java o/C1653v.java o/C3800l0.java o/C3818v.java o/K0.java o/N.java o/Q0.java o/U.java o/d0.java o/g1.java o/i1.java o/m1.java o/w1.java o1/C1713v.java o1/H.java o7/C1740a.java o7/C3909a.java of/C0727P.java org/tensorflow/lite/NativeInterpreterWrapper.java p5/h.java q0/T.java r2/q.java r6/d.java rd/C0821d.java rd/C4317d.java s/h.java s/x.java s2/c.java s6/b.java t5/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t6/c.java tv/twilio/webrtc/DefaultVideoEncoderFactory.java u5/AbstractC2020a.java u5/AbstractC4669a.java v2/C2125c.java w/C2150u.java w/s.java w1/A.java w5/C2190g.java w5/C5004g.java x2/b.java x4/d.java x4/i.java x4/l.java y4/C2350b.java y4/C5305a.java y4/C5306b.java y4/HandlerC5307c.java y4/a.java y4/c.java y4/e.java y4/h.java y4/i.java y4/j.java y4/k.java y4/l.java y5/d.java y5/g.java y6/BinderC2353A.java y6/C.java y6/e.java y6/g.java y6/i.java y6/j.java y6/m.java y6/q.java y6/r.java y6/s.java y6/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y6/w.java y6/x.java y6/y.java z4/AbstractBinderC2410l.java z4/AbstractBinderC5538l.java z4/C2406h.java z4/C5531e.java z4/C5532f.java z4/C5534h.java z4/HandlerC2408j.java z4/HandlerC5536j.java z4/e.java z4/f.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	zd/C1064a.java zd/C5569a.java af/InterfaceC1755a.java af/a.java bj/InterfaceC0370a.java bj/InterfaceC2021a.java cj/InterfaceC2145a.java cj/a.java qj/InterfaceC0715e.java qj/InterfaceC4221e.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	D/RunnableC0124c.java G/b.java Lg/a.java Lg/b.java Mg/a.java Si/e.java Si/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Hb/Y.java Kb/d.java Ni/e.java Ni/h.java Ni/m.java Ni/n.java a7/r.java sc/p.java tc/f.java yc/C0977U.java
6	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	M6/e.java
7	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	G4/b.java J6/e.java R5/m.java com/bugsnag/android/C0452y.java s6/b.java
8	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	Ka/c.java O7/b.java Ra/b.java o1/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	A/h.java A5/D.java G6/l.java G6/n.java L3/d.java M/d.java g6/C2881b.java g6/b.java k4/d.java k4/i.java k4/j.java l4/k.java l4/l.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	n1/w.java
11	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	x4/i.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	E5/i.java I5/d.java com/bugsnag/android/RootDetector.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	Ff/c.java G6/f.java
00056	Modify voice volume	control	org/amazon/chime/webrtc/audio/WebRtcAudioTrack.java org/amazon/chime/webrtc/voiceengine/WebRtcAudioTrack.java tvi/webrtc/audio/WebRtcAudioTrack.java tvi/webrtc/voiceengine/WebRtcAudioTrack.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	Ba/d.java Cd/C0022f.java Cd/D.java Cd/L.java D7/p.java L2/C0156a.java L2/C0158c.java L2/C0421a.java L2/l.java Uc/c.java Wi/e.java ae/g.java b7/C0715d.java cd/i.java com/simplepractice/clients/fcm/FcmService.java com/simplepractice/clients/module/dashboard/ui/DashboardActivity.java com/simplepractice/clients/module/messenger/conversation/view/ConversationActivity.java com/simplepractice/clients/module/notifications/ui/NotificationsSettingsFragment.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java eg/C0516y0.java o1/C1681d0.java o1/C3847d0.java x2/b.java xi/C0921f.java xi/C5218f.java z4/C5532f.java z4/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/simplepractice/clients/module/NotificationRouterActivity.java com/simplepractice/clients/module/dashboard/ui/DashboardActivity.java l2/J0.java net/openid/appauth/AuthorizationManagementActivity.java y6/j.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Cd/L.java L2/C0156a.java L2/C0158c.java L2/C0421a.java com/simplepractice/clients/module/dashboard/ui/DashboardActivity.java com/simplepractice/clients/module/notifications/ui/NotificationsSettingsFragment.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java x2/b.java z4/C5532f.java z4/f.java
00096	Connect to a URL and set request method	command network	N3/g.java N3/l.java dh/C0463b.java f1/c.java ff/i.java k4/j.java
00123	Save the response to JSON after connecting to the remote server	network command	dh/C0463b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	N3/g.java N3/l.java com/bugsnag/android/C0452y.java dh/C0463b.java f1/c.java k4/j.java of/Z.java t6/c.java
00030	Connect to the remote server through the given URL	network	dh/C0463b.java of/Z.java
00109	Connect to a URL and get the response code	network command	N3/g.java N3/l.java com/bugsnag/android/C0452y.java dh/C0463b.java f1/c.java k4/j.java of/Z.java t6/c.java x4/c.java
00022	Open a file from given absolute path of the file	file	G/f.java Xg/O.java com/bugsnag/android/NativeInterface.java com/bugsnag/android/f0.java com/bugsnag/android/ndk/NativeBridge.java com/simplepractice/clients/module/billing/document/BillingDocumentFragment.java com/simplepractice/clients/module/documents/pdfviewer/DocumentPdfViewerFragment.java com/simplepractice/clients/module/documents/viewall/DocumentsViewAllFragment.java g3/C1149a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	Ni/c.java Ni/n.java
00163	Create new Socket and connecting to it	socket	Ni/c.java Ni/n.java
00054	Install other APKs from file	reflection	G/f.java
00005	Get absolute path of file and put it to JSON object	file	G/f.java
00004	Get filename and put it to JSON object	file collection	A5/F.java G/f.java a/a.java com/bugsnag/android/B.java x4/i.java
00036	Get resource file from res/raw directory	reflection	L2/C0156a.java L2/C0421a.java Uc/c.java com/simplepractice/clients/module/notifications/ui/NotificationsSettingsFragment.java l3/C1446a.java o/g1.java x2/b.java z4/C5532f.java z4/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B2/g.java Ci/H.java F6/g.java F6/i.java L7/c.java P2/b.java P2/g.java P2/l.java Q6/f.java Vi/x.java Xi/m0.java Z1/h.java b2/C0706h.java b2/C0707i.java c2/AbstractC2036c.java c2/c.java com/bugsnag/android/B.java com/bugsnag/android/C0451i0.java com/bugsnag/android/C0759k0.java com/bugsnag/android/C2164i0.java com/bugsnag/android/RootDetector.java com/bugsnag/android/ndk/NativeBridge.java com/bugsnag/android/q0.java f1/c.java n1/w.java org/joda/time/tz/h.java x4/i.java zf/d.java
00102	Set the phone speaker on	command	H3/d.java
00026	Method reflection	reflection	dh/C0457B.java dh/C2497B.java kh/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	o/g1.java
00189	Get the content of a SMS message	sms	com/simplepractice/clients/module/documents/viewall/b.java
00188	Get the address of a SMS message	sms	com/simplepractice/clients/module/documents/viewall/b.java
00200	Query data from the contact list	collection contact	com/simplepractice/clients/module/documents/viewall/b.java
00201	Query data from the call log	collection calllog	com/simplepractice/clients/module/documents/viewall/b.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/simplepractice/clients/module/documents/viewall/b.java
00014	Read file into a stream and put it into a JSON object	file	Q6/f.java com/bugsnag/android/B.java n1/w.java x4/i.java
00183	Get current camera parameters and change the setting.	camera	com/twilio/video/CameraCapturer.java jd/C3252d.java jd/d.java org/amazon/chime/webrtc/Camera1Session.java tvi/webrtc/Camera1Session.java
00208	Capture the contents of the device screen	collection screen	org/amazon/chime/webrtc/ScreenCapturerAndroid.java tvi/webrtc/ScreenCapturerAndroid.java
00009	Put data in cursor to JSON object	file	A6/d.java G6/l.java G6/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	f1/c.java
00094	Connect to a URL and read data from it	command network	f1/c.java
00108	Read the input stream from given URL	network command	f1/c.java
00147	Get the time of current location	collection location	i/C1198A.java
00075	Get location of the device	collection location	i/C1198A.java
00115	Get last known location of the device	collection location	i/C1198A.java
00112	Get the date of the calendar event	collection calendar	com/bugsnag/android/a0.java
00012	Read data and put it into a buffer stream	file	B2/g.java
00046	Method reflection	reflection	u3/n.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/480606925588/namespaces/firebase:fetch?key=AIzaSyBbAHgWWA3rAnvcd_Bml6D2a0Tp5KPurRc. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	6/44	android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BROADCAST_STICKY, com.google.android.c2dm.permission.RECEIVE

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
support.link.co	ok	**IP:** 18.238.109.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.simplepractice.com	ok	**IP:** 76.76.21.61 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
api.stripe.com	ok	**IP:** 52.26.11.205 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
secure.simplepractice.com	ok	**IP:** 54.191.145.95 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nearest-media-region.l.chime.aws	ok	**IP:** 99.77.190.2 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
video.simplepractice.com	ok	**IP:** 35.155.44.99 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bugsnag.com	ok	**IP:** 18.238.96.82 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
m.stripe.com	ok	**IP:** 52.27.196.179 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
link.co	ok	**IP:** 13.224.53.87 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 142.250.74.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
static.afterpay.com	ok	**IP:** 104.16.223.179 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.simplepractice.com	ok	**IP:** 44.239.115.115 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
support.stripe.com	ok	**IP:** 198.202.176.111 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
clientsecure.me	ok	**IP:** 35.155.44.99 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
docs.bugsnag.com	ok	**IP:** 18.155.173.102 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	**IP:** 44.235.152.108 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
support.simplepracticeclient.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
stripe.com	ok	**IP:** 52.10.212.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
q.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
dashboard.stripe.com	ok	**IP:** 35.166.203.173 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
r.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	De/C0041b.java
u0013android@android.com0 u0013android@android.com	z4/BinderC5537k.java
u0013android@android.com0 u0013android@android.com	z4/BinderC2409k.java
email@example.com	pe/C0766d.java

EMAIL	FILE
email@example.com	pe/C0768f.java
support@stripe.com	yd/C5436j.java
support@stripe.com	yd/j.java
name@mail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBbAHgWWA3rAnvcd_Bml6D2a0Tp5KPurRc"
"google_crash_reporting_api_key" : "AIzaSyBbAHgWWA3rAnvcd_Bml6D2a0Tp5KPurRc"
759b1054a8013b791bfed66c8787fc12

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
115792089237316195423570985008687907853269984665640564039457584007908834671663
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057 5
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
8d8e3f79aa0783ab0cfa5c8d65d663a9da6ba99401efb2298aaaee387c3b00d6
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
dcb428fea25c40e7b99f81ae5981ee6a
af60eb711bd85bc1e4d3e0a462e074eea428a8
3267051002075881697808308513050704318447127338065924327593890433575733748242 4
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
96990def30f5890559bfc12626b1a42d676b2b78a3f673664c3a9f886e205774
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
deca87e736574c5c83c07314051fd93a
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
36864200e0eaf5284d884a0e77d31646
55066263022277343669578718895168534326250603453777594175500187360389116729240
484395612939064517590525852527979142027629495260417479958440807170824046352 86
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316
85053bf24bba75239b16a601d9387e17
7bf492cba0ed69fea51e641941c2632c
1157920892373161954235709850086879078528375642790749043826051631415181614943337
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
ea51ca5c693a4b8733b1cf1a63557a713a13fabf0bcb724385077694e63a51a7

POSSIBLE SECRETS
361342509567497957985851279195878819566111066729850150718771982535684144051 09
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: SimplePractice Client Portal

Score: 4.401961 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.simplepractice.clients

Developer Details: SimplePractice, SimplePractice, None, https://support.simplepracticeclient.com/hc/en-us, developer-info@simplepractice.com,

Release Date: Oct 26, 2023 **Privacy Policy:** Privacy link

Description:

If you’re receiving services for behavioral health, counseling, speech pathology, occupational therapy, physical therapy, or any other wellness service by a practitioner who uses SimplePractice, this app is for you! The SimplePractice Client Portal Android app empowers you to manage care for you or your loved ones from one secure place. Stay connected with your practitioner between appointments from the convenience of your phone. Your personal information is kept private, yet easily accessible for your convenience. Simplify how you access care with features like: • Passwordless login – Securely log into your Client Portal without the hassle of a username or password by setting up a passcode or turn on biometrics (if enabled on your Android device) • Personalized notifications – Get push notifications sent right to your phone regarding any new messages, invoices, or documents that have been sent to you by your practitioner. • Secure messaging – Message your practitioner directly from your phone knowing that all communication is secure and private. • Upcoming appointments and requests – View all your upcoming appointments, and request a new appointment with your practitioner directly from the app. • Digital payments – Add new payment methods to pay your bills including HSA and FSA cards. You can even pay directly from the app. • Digital paperwork – Complete documents and questionnaires related to care on your own time. • Telehealth – Join virtual appointments with your practitioner directly from the app, so you never have to find a link buried in your inbox again. • Profile switching – Quickly toggle between any Client Portal you’re managing—whether you’re seeing different providers who use SimplePractice for practice management or are managing care for multiple individuals. To access the SimplePractice Client Portal Android app, you must be invited to use the SimplePractice Client Portal by your practitioner. When you first log into the app, the email you

provided to your practitioner will be used to authenticate your Client Portal access. After you've signed up, turn on biometrics or a four-digit passcode for hassle-free login. Please note: what you can see and do within the SimplePractice Client Portal app may vary, and is limited to the specific features your practitioner has enabled for your profile. Are you currently looking for therapy services? To find a behavioral health therapist that uses SimplePractice near you, visit www.meetmonarch.com.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:57:38	Generating Hashes	OK
2025-09-01 08:57:40	Extracting APK	OK
2025-09-01 08:57:40	Unzipping	OK
2025-09-01 08:57:43	Parsing APK with androguard	OK
2025-09-01 08:57:43	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:57:44	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:57:46	Parsing AndroidManifest.xml	OK
2025-09-01 08:57:46	Extracting Manifest Data	OK

2025-09-01 08:57:46	Manifest Analysis Started	OK
2025-09-01 08:57:46	Reading Network Security config from network_security_config.xml	OK
2025-09-01 08:57:46	Parsing Network Security config	OK
2025-09-01 08:57:46	Performing Static Analysis on: Client Portal (com.simplepractice.clients)	OK
2025-09-01 08:57:48	Fetching Details from Play Store: com.simplepractice.clients	OK
2025-09-01 08:57:50	Checking for Malware Permissions	OK
2025-09-01 08:57:50	Fetching icon path	OK
2025-09-01 08:57:50	Library Binary Analysis Started	OK
2025-09-01 08:57:50	Reading Code Signing Certificate	OK
2025-09-01 08:57:50	Running APKiD 2.1.5	OK
2025-09-01 08:57:56	Detecting Trackers	OK

2025-09-01 08:57:59	Decompiling APK to Java with JADX	OK
2025-09-01 08:58:13	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 08:58:13	Decompiling classes2.dex with JADX	OK
2025-09-01 08:58:18	Decompiling classes.dex with JADX	OK
2025-09-01 08:58:28	Decompiling classes3.dex with JADX	OK
2025-09-01 08:58:37	Decompiling classes2.dex with JADX	OK
2025-09-01 08:58:42	Decompiling classes.dex with JADX	OK
2025-09-01 08:59:11	Decompiling with JADX failed for classes.dex	OK
2025-09-01 08:59:11	Decompiling classes3.dex with JADX	OK
2025-09-01 08:59:20	Some DEX files failed to decompile	OK

2025-09-01 08:59:20	Converting DEX to Smali	OK
2025-09-01 08:59:20	Code Analysis Started on - java_source	OK
2025-09-01 08:59:26	Android SBOM Analysis Completed	OK
2025-09-01 08:59:39	Android SAST Completed	OK
2025-09-01 08:59:39	Android API Analysis Started	OK
2025-09-01 08:59:54	Android API Analysis Completed	OK
2025-09-01 08:59:54	Android Permission Mapping Started	OK
2025-09-01 09:00:21	Android Permission Mapping Completed	OK
2025-09-01 09:00:22	Android Behaviour Analysis Started	OK
2025-09-01 09:00:40	Android Behaviour Analysis Completed	OK

2025-09-01 09:00:40	Extracting Emails and URLs from Source Code	OK
2025-09-01 09:00:48	Email and URL Extraction Completed	OK
2025-09-01 09:00:48	Extracting String data from APK	OK
2025-09-01 09:00:48	Extracting String data from Code	OK
2025-09-01 09:00:48	Extracting String values and entropies from Code	OK
2025-09-01 09:00:53	Performing Malware check on extracted domains	OK
2025-09-01 09:00:55	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.