



ANDROID STATIC ANALYSIS REPORT



 OctaApp (4.3.0)

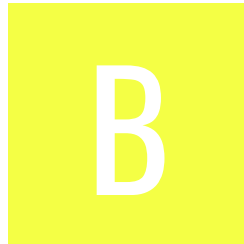
File Name: com.octapharma.OctaApp_14.apk

Package Name: com.octapharma.OctaApp

Scan Date: Sept. 1, 2025, 3:59 a.m.






App Security Score: 52/100 (MEDIUM RISK)

Grade:



Trackers Detection: 3/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	13	3	2	1

FILE INFORMATION

File Name: com.octapharma.OctaApp_14.apk

Size: 7.72MB

MD5: 21f7319cde09593290855955b006a6e1

SHA1: a87b8c6f392a935fa32804be0ccf3a8aef960f80

SHA256: 9b2dd6485cd39beede0a0aa9d0c9aec07981936b778a001cb17e9cac0911aa7

APP INFORMATION

App Name: OctaApp

Package Name: com.octapharma.OctaApp

Main Activity: com.octapharma.OctaApp.MainActivity

Target SDK: 34

Min SDK: 22

Max SDK:

Android Version Name: 4.3.0

Android Version Code: 14

APP COMPONENTS

Activities: 7

Services: 10

Receivers: 5

Providers: 4

Exported Activities: 0

Exported Services: 0

Exported Receivers: 2

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: 2021-06-11 13:25:21+00:00

Valid To: 2051-06-11 13:25:21+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xc32359670bcb924843ae87b082a7cf5cb621fb38

Hash Algorithm: sha256

md5: a080e5b36faa3a2073b9cab2353256f6

sha1: a9a2f9b2b5f1bf6f5681e3c8af1ffeebfe11c0a7

sha256: 5ef9058b6f1bbce8d71075d533e597758b9638e969a69f9e15f66bb1db3cfba0

sha512: dff09c0b87be79db1d632ca40a2c7b230e7c74a2ad479b6d0ef1c0ae1af3a540845444922565dad13841d1899367486937f43a9131fb14d309ce1189214be4b1

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: aa64b3edd39a132279eb2ad3034c22ee8e26048abd5b5e5111ca5e09e4a73e02

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.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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.octapharma.OctaApp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
21f7319cde09593290855955b006a6e1.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check device ID check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.octapharma.OctaApp.MainActivity	Schemes: @string/custom_url_scheme://, https://, mailto://, Hosts: donor.donor360.octapharma.com,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	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.
5	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.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b1/d.java b4/g.java b4/o.java com/bumptechnology/glide/Glide.java com/bumptechnology/glide/load/data/ b.java com/bumptechnology/glide/load/data/j .java com/bumptechnology/glide/load/data/l .java com/bumptechnology/glide/manager/e .java com/bumptechnology/glide/manager/p .java com/bumptechnology/glide/manager/q .java com/capacitorjs/plugins/network/ NetworkPlugin.java com/getcapacitor/community/fir ebasecrashlytics/a.java com/getcapacitor/k0.java cordova/plugin/RequestLocation Accuracy.java d1/h.java d5/b.java de/appplant/cordova/emailcom poser/a.java de/appplant/cordova/emailcom poser/b.java de/mariusbackes/cordova/plugi n/ThemeDetection.java e0/b.java e1/i.java e4/f.java e5/c.java f0/m0.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	g2/a.java g2/c.java h3/a.java h4/m.java i1/a.java i3/a.java j2/b.java j2/c.java j2/g.java j2/q.java j2/r.java j2/t.java j2/w.java j2/x.java k0/b.java k2/b0.java k2/g.java k2/g0.java k2/k.java k2/l.java k2/l0.java k2/o.java k2/x.java l0/d.java l0/e.java l3/c.java l6/f.java m2/h0.java n0/c.java n0/e.java n2/a.java n2/a1.java n2/b0.java n2/c.java n2/c1.java n2/e0.java n2/i0.java n2/i1.java n2/m1.java n2/v0.java n2/y0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n2/z0.java o0/h.java o0/i.java o0/k.java o0/q.java o0/z.java p/g.java p0/i.java p0/k.java q0/e.java q0/i.java q2/b.java r0/a.java r2/g.java r2/o.java r2/p.java s/c.java s0/c.java s0/d.java s0/g.java s0/s.java s0/t.java s0/u.java u0/l.java u3/d.java v0/c.java v0/f.java v0/h0.java v0/l0.java v0/n.java v0/u.java v0/v.java v0/z.java v1/k.java v2/d.java v3/b.java w/c.java y/a.java y1/a.java y3/e.java z0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				z0/c.java r0/c.java z9/p.java
2	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	r9/a.java r9/b.java s9/a.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	a7/d.java com/epicshaggy/biometric/NativeBiometric.java com/getcapacitor/t0.java j4/d.java m0/g.java o0/d.java o0/p.java o0/x.java o5/i.java o5/l.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	c2/m0.java c2/t0.java g7/b.java g7/w.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/z.java d5/c.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	d5/b.java l7/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	f7/g.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	l7/b.java
9	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	l7/b.java
10	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/z.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	h4/g.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/capacitorjs/plugins/pushnotifications/v.java com/getcapacitor/g.java com/phonegap/plugins/nativesettings/NativeSettings.java de/appplant/cordova/emailcomposer/a.java l7/b.java
00096	Connect to a URL and set request method	command network	c7/c.java com/getcapacitor/f1.java e5/c.java
00089	Connect to a URL and receive input stream from the server	command network	c7/c.java com/bumptechnology/load/data/j.java com/getcapacitor/f1.java e5/c.java
00109	Connect to a URL and get the response code	network command	c7/c.java com/bumptechnology/load/data/j.java e5/c.java g2/d.java
00013	Read file and put it into a stream	file	com/bumptechnology/load/a.java com/getcapacitor/a.java d5/c.java de/appplant/cordova/emailcomposer/a.java h4/v.java i4/d.java k0/b.java m4/e.java o4/a.java s0/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/getcapacitor/g.java com/moe/pushlibrary/activities/MoEActivity.java com/moengage/pushbase/internal/j.java l7/b.java q5/s.java
00075	Get location of the device	collection location	com/capacitorjs/plugins/geolocation/c.java
00022	Open a file from given absolute path of the file	file	de/appplant/cordova/emailcomposer/a.java f7/b.java
00024	Write file after Base64 decoding	reflection file	de/appplant/cordova/emailcomposer/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	n0/c.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/getcapacitor/g.java com/moe/pushlibrary/activities/MoEActivity.java com/phonegap/plugins/nativesettings/NativeSettings.java de/appplant/cordova/emailcomposer/b.java l7/b.java n2/p1.java r5/a.java u7/a.java u8/c.java
00125	Check if the given file path exist	file	com/getcapacitor/g.java
00016	Get location info of the device and put it to JSON object	location collection	w5/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	n2/p1.java r5/a.java
00014	Read file into a stream and put it into a JSON object	file	d5/c.java i4/d.java o4/a.java
00009	Put data in cursor to JSON object	file	a9/d.java f8/d.java y6/e.java
00034	Query the current data network type	collection network	l7/m.java
00202	Make a phone call	control	r5/a.java
00203	Put a phone number into an intent	control	r5/a.java
00094	Connect to a URL and read data from it	command network	com/getcapacitor/f1.java l4/a.java q1/d.java
00030	Connect to the remote server through the given URL	network	com/bumptechnology/load/data/j.java
00128	Query user account information	collection account	de/appplant/cordova/emailcomposer/b.java
00108	Read the input stream from given URL	network command	com/getcapacitor/f1.java
00123	Save the response to JSON after connecting to the remote server	network command	q1/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00153	Send binary data over HTTP	http	q1/c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/470215737336/namespaces/firebase:fetch?key=AlzaSyBITYS4zMkLICUiztQeTY54dGtgIUd3guo . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK
Other Common Permissions	4/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, 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
firebase-settings.crashlytics.com	ok	IP: 216.58.207.195 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
capacitorjs.com	ok	IP: 172.67.203.214 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
update.crashlytics.com	ok	IP: 172.217.20.163 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.
plus.google.com	ok	IP: 142.250.75.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
pagead2.googlesyndication.com	ok	IP: 216.58.213.66 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map



EMAIL	FILE
u0013android@android.com0 u0013android@android.com	k2/w.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MoEngage	Analytics	https://reports.exodus-privacy.eu.org/trackers/268

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "d4da1a385a0a4be18d9c94dee80da031"
"google_api_key" : "AlzaSyBITYS4zMkLICUiztQeTY54dGtgIUd3guo"
"google_crash_reporting_api_key" : "AlzaSyBITYS4zMkLICUiztQeTY54dGtgIUd3guo"
470fa2b4ae81cd56ecbcd9735803434cec591fa

PLAYSTORE INFORMATION

Title: OctaApp – Donate Blood Plasma!

Score: 3.7495682 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [com.octapharma.OctaApp](https://play.google.com/store/apps/details?id=com.octapharma.OctaApp)

Developer Details: Octapharma Plasma Inc., Octapharma+Plasma+Inc., None, None, octa.google@octapharma.com,

Release Date: Sep 28, 2021 **Privacy Policy:** [Privacy link](#)

Description:

OctaApp makes donating plasma faster and easier! Features: Location · Find plasma donation centers near you Next Donation · View your next eligible date to donate plasma OctaPass · Launch Haemonetics Donor360® health history questionnaire to start your visit before you arrive Loyalty Program · Check your status levels and redeem points earned! Refer-a-friend · Quickly and easily refer your friends and family for added bonuses Earnings · Learn how much you will earn with each plasma donation Card Balance · Check your debit card balance and payment history Updates & Promotions · Learn about company updates and upcoming promotions

SCAN LOGS

Timestamp	Event	Error
2025-09-01 03:59:40	Generating Hashes	OK
2025-09-01 03:59:41	Extracting APK	OK
2025-09-01 03:59:41	Unzipping	OK
2025-09-01 03:59:42	Parsing APK with androguard	OK

2025-09-01 03:59:43	Extracting APK features using aapt/aapt2	OK
2025-09-01 03:59:43	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 03:59:45	Parsing AndroidManifest.xml	OK
2025-09-01 03:59:45	Extracting Manifest Data	OK
2025-09-01 03:59:45	Manifest Analysis Started	OK
2025-09-01 03:59:45	Performing Static Analysis on: OctaApp (com.octapharma.OctaApp)	OK
2025-09-01 03:59:47	Fetching Details from Play Store: com.octapharma.OctaApp	OK
2025-09-01 03:59:48	Checking for Malware Permissions	OK
2025-09-01 03:59:48	Fetching icon path	OK
2025-09-01 03:59:48	Library Binary Analysis Started	OK

2025-09-01 03:59:48	Reading Code Signing Certificate	OK
2025-09-01 03:59:49	Running APKiD 2.1.5	OK
2025-09-01 03:59:51	Detecting Trackers	OK
2025-09-01 03:59:52	Decompiling APK to Java with JADX	OK
2025-09-01 04:00:01	Converting DEX to Smali	OK
2025-09-01 04:00:01	Code Analysis Started on - java_source	OK
2025-09-01 04:00:02	Android SBOM Analysis Completed	OK
2025-09-01 04:00:06	Android SAST Completed	OK
2025-09-01 04:00:06	Android API Analysis Started	OK
2025-09-01 04:00:10	Android API Analysis Completed	OK
2025-09-01 04:00:10	Android Permission Mapping Started	OK

2025-09-01 04:00:14	Android Permission Mapping Completed	OK
2025-09-01 04:00:14	Android Behaviour Analysis Started	OK
2025-09-01 04:00:19	Android Behaviour Analysis Completed	OK
2025-09-01 04:00:19	Extracting Emails and URLs from Source Code	OK
2025-09-01 04:00:20	Email and URL Extraction Completed	OK
2025-09-01 04:00:20	Extracting String data from APK	OK
2025-09-01 04:00:20	Extracting String data from Code	OK
2025-09-01 04:00:20	Extracting String values and entropies from Code	OK
2025-09-01 04:00:21	Performing Malware check on extracted domains	OK
2025-09-01 04:00:22	Saving to Database	OK

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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).