MOBSF

ANDROID STATIC ANALYSIS REPORT

Modento (1.5.2)

File Name:	com.mobiati.modento_75.apk
Package Name:	com.mobiati.modento
Scan Date:	Aug. 31, 2025, 5:27 a.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	14	2	1	1

FILE INFORMATION

File Name: com.mobiati.modento_75.apk
Size: 5.41MB
MD5: e9595575b5cf0788ed5d1eeae4295e7b
SHA1: 681470ae99831ca00f9ae29f2de2005fcaba374c
SHA256: d225ca241f55476de66a5962c41f6fb0331810f47775200baf1cf219e55c8c0c

APP INFORMATION

App Name: Modento
Package Name: com.mobiati.modento
Main Activity: com.mobiati.dental.activities.StartActivity
Target SDK: 29
Min SDK: 17
Max SDK:
Android Version Name: 1.5.2

Android Version Code: 75

APP COMPONENTS

Activities: 23
Services: 7
Receivers: 3
Providers: 4
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
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: 2017-12-09 22:04:31+00:00
Valid To: 2047-12-09 22:04:31+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x41ca51a9b59eee1c8829dd0be33e22e58201d55d
Hash Algorithm: sha256
md5: 5501df3fd3fbb5fbcbec594392b040d8
sha1: f917ff0cabc134cfac5ce245ddf615331a47cd4a
sha256: 8d4ad0d0e394aaefcf1b9c81b2faab0261896473634ebe7455c8a521de25fa87
sha512: f1d5e84f289c64153fb9f96f765d605d729bd14610351bfd253815eef9a4ec6b3e571fdb3e833466ef08e1666f286851d889b102fce1c632c646cc6decce333a
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e9fb759299dbee3d034c04bf24496086245e448a34b9a84365eb7480cb641ee7
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check SIM operator check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mobiati.dental.activities.StartActivity	Schemes: modento://, https://, Hosts: open, modento.app.link, modento.test-app.link,

NETWORK SECURITY

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

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: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.2-4.2.2, [minSdk=17]	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=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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	App Link assetlinks.json file not found [android:name=com.mobiati.dental.activities.StartActivity] [android:host=https://modento.test-app.link]	high	App Link asset verification URL (https://modento.test-app.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
5	Launch Mode of activity (com.mobiati.dental.activities.StartActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Service (com.mobiati.dental.fcm.MobiatiMessagingService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
7	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.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **7** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

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	android_serialport_api/SerialPort.java com/bbpos/bbdevice/ota/b.java com/bbpos/bbdevice/ota/d.java com/bolt/consumersdk/CCConsumer.java com/bolt/consumersdk/swiper/CCSwiperController.java com/bolt/consumersdk/swiper/core/terminals/idtech/config/ConfigManager.java com/bolt/consumersdk/swiper/core/terminals/idtech/config/Configurations.java com/bolt/consumersdk/utils/LogHelper.java com/journeyapps/barcodescanner/c.java com/journeyapps/barcodescanner/d.java com/journeyapps/barcodescanner/p/a.java com/journeyapps/barcodescanner/p/b.java com/journeyapps/barcodescanner/p/c.java com/journeyapps/barcodescanner/p/g.java com/journeyapps/barcodescanner/p/i.java com/journeyapps/barcodescanner/p/l.java com/mobiati/dental/activities/t.java com/umobilized/helpers/f/a.java i/a/a/b/a.java i/b/a/o.java i/b/b/k.java i/e/a/b/i/v/a.java i/e/a/d/b/e/k.java i/e/a/d/d/a.java i/f/a/k.java i/i/a/m/a.java io/branch/referral/network/a.java j/a/b/c.java j/a/b/g.java j/a/b/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j/a/b/q.java m/b/d.java n/p/c.java
2	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/bolt/consumersdk/androidpay/utils/CCConsumerAndroidPayWalletUtils.java com/bolt/consumersdk/constants/Constants.java com/bolt/consumersdk/network/constanst/Constants.java com/bolt/consumersdk/swiper/core/terminals/bbpos/configuration/BbPosKeys.java
3	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	com/bbpos/bbdevice/ota/i.java com/bbpos/bbdevice001/r.java
4	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/bbpos/bbdevice001/r.java i/b/a/w.java i/h/a/x.java
5	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/bbpos/bbdevice/ota/c.java com/bbpos/bbdevice/ota/h.java com/bbpos/bbdevice001/q.java
6	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/bbpos/bbdevice/ota/d.java i/b/a/o.java i/b/b/k.java i/f/a/a.java i/i/a/m/a.java
7	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	i/e/a/b/i/x/j/b0.java i/e/a/b/i/x/j/f0.java i/e/a/b/i/x/j/h0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	j/a/a/b.java
9	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/bbpos/bbdevice001/a.java com/umobilized/helpers/f/b.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	com/journeyapps/barcodescanner/d.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	i/h/a/t.java j/a/b/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	i/h/a/t.java j/a/b/j.java
00109	Connect to a URL and get the response code	network command	i/h/a/t.java j/a/b/j.java
00022	Open a file from given absolute path of the file	file	android_serialport_api/SerialPort.java com/bbpos/bbdevice/ota/d.java com/journeyapps/barcodescanner/d.java i/b/a/o.java i/b/b/k.java i/i/a/m/a.java
00056	Modify voice volume	control	i/b/a/j.java i/f/a/t/f/b.java
00202	Make a phone call	control	com/umobilized/helpers/h/d.java
00203	Put a phone number into an intent	control	com/umobilized/helpers/h/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/umobilized/helpers/h/d.java j/a/b/c.java j/a/b/g.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/umobilized/helpers/h/d.java j/a/b/c.java
00091	Retrieve data from broadcast	collection	j/a/b/c.java
00036	Get resource file from res/raw directory	reflection	j/a/b/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	android_serialport_api/SerialPort.java com/bbpos/bbdevice/ota/i.java m/r.java
00123	Save the response to JSON after connecting to the remote server	network command	j/a/b/j.java
00030	Connect to the remote server through the given URL	network	j/a/b/j.java
00094	Connect to a URL and read data from it	command network	j/a/b/j.java
00108	Read the input stream from given URL	network command	j/a/b/j.java
00183	Get current camera parameters and change the setting.	camera	com/journeyapps/barcodescanner/p/c.java
00163	Create new Socket and connecting to it	socket	com/bbpos/bbdevice/ota/b.java
00121	Create a directory	file command	i/i/a/m/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://mobiati-dental.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/27168203423/namespaces/firebase:fetch?key=AIzaSyC9iu6XEQxzFtE_Cm-nK7u5cM0SlYESmN4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO
Other Common Permissions	5/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN

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
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
stripe.com	ok	**IP:** 52.89.224.113 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
q.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

DOMAIN	STATUS	GEOLOCATION
api.branch.io	ok	**IP:** 18.238.109.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.stripe.com	ok	**IP:** 52.26.14.11 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
patient.modento.io	ok	**IP:** 104.18.10.31 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.modento.io	ok	**IP:** 206.189.78.234 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobiati-dental.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
m.stripe.com	ok	**IP:** 34.216.79.190 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.modento.com	ok	**IP:** 52.24.64.130 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	i/h/a/t.java

EMAIL	FILE
support@modento.io	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
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
"api_base_url" : "https://api.modento.com/"
"firebase_database_url" : "https://mobiati-dental.firebaseio.com"
"google_api_key" : "AIzaSyC9iu6XEQxzFtE_Cm-nK7u5cM0SlYESmN4"
"google_crash_reporting_api_key" : "AIzaSyC9iu6XEQxzFtE_Cm-nK7u5cM0SlYESmN4"
"oauth_client_secret" : "PSI10qB2TZ4FnpOC6isW84XbreRmGXCBdSBt573K"

POSSIBLE SECRETS
5669564F7465636832000340000096E2
B19939F9099A4B710DB3EEC235061113
235e63955ecbf86af6eef9528c14a27e29c3b97355540e5e7a6eccdd44c9366c4a383064d2c626ae3799052b042c538dadbb35662032e2a40ed02da5b410dc127f6f132a47a77c75a3bd808dae1e837e981b8d03e75bf1ec67c5813ea4eddc939e789f085f3ff97278a0af8aafd28ea1
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

PLAYSTORE INFORMATION

Title: Modento

Score: 3.44 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.mobiati.modento

Developer Details: Modento Inc., Modento+Inc., None, http://www.modento.io, support@modento.io,

Release Date: Mar 27, 2018 **Privacy Policy:** Privacy link

Description:

Modento is a completely secure and HIPAA compliant application that makes the connection between you and your dental office dramatically easier. Secure payments, personalized notifications, insurance updates, forms, and consents- all through the app which is designed to be easy to use. Your dental needs are simple to manage and as transparent as possible, all in the palm of your hand. The best part- you will earn reward points for doing the same things you've always had to do... only now you can do them from the comfort of your couch and whenever works best for you. Modento is here to make dentistry as painless as possible. NOTE: You will be able sign up and use this application only if your dental practice is using Modento platform. Ask your dentist if you are not sure.

SCAN LOGS

Timestamp	Event	Error

2025-08-31 05:27:46	Generating Hashes	OK
2025-08-31 05:27:46	Extracting APK	OK
2025-08-31 05:27:46	Unzipping	OK
2025-08-31 05:27:46	Parsing APK with androguard	OK
2025-08-31 05:27:46	Extracting APK features using aapt/aapt2	OK
2025-08-31 05:27:46	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 05:27:50	Parsing AndroidManifest.xml	OK
2025-08-31 05:27:50	Extracting Manifest Data	OK
2025-08-31 05:27:50	Manifest Analysis Started	OK
2025-08-31 05:27:50	Reading Network Security config from network_security_config.xml	OK
2025-08-31 05:27:50	Parsing Network Security config	OK

2025-08-31 05:27:50	Performing Static Analysis on: Modento (com.mobiati.modento)	OK
2025-08-31 05:27:51	Fetching Details from Play Store: com.mobiati.modento	OK
2025-08-31 05:27:51	Checking for Malware Permissions	OK
2025-08-31 05:27:51	Fetching icon path	OK
2025-08-31 05:27:51	Library Binary Analysis Started	OK
2025-08-31 05:27:51	Reading Code Signing Certificate	OK
2025-08-31 05:27:52	Running APKiD 2.1.5	OK
2025-08-31 05:27:57	Detecting Trackers	OK
2025-08-31 05:27:59	Decompiling APK to Java with JADX	OK
2025-08-31 05:55:02	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/e9595575b5cf0788ed5d1eeae4295e7b/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/e9595575b5cf0788ed5d1eeae4295e7b/e9595575b5cf0788ed5d1eeae4295e7b.apk'], 999.9999197125435)

2025-08-31 05:55:02	Converting DEX to Smali	OK
2025-08-31 05:55:02	Code Analysis Started on - java_source	OK
2025-08-31 05:55:07	Android SBOM Analysis Completed	OK
2025-08-31 05:55:24	Android SAST Completed	OK
2025-08-31 05:55:24	Android API Analysis Started	OK
2025-08-31 05:55:30	Android API Analysis Completed	OK
2025-08-31 05:55:30	Android Permission Mapping Started	OK
2025-08-31 05:55:39	Android Permission Mapping Completed	OK
2025-08-31 05:55:40	Android Behaviour Analysis Started	OK
2025-08-31 05:55:46	Android Behaviour Analysis Completed	OK
2025-08-31 05:55:46	Extracting Emails and URLs from Source Code	OK

2025-08-31 05:55:59	Email and URL Extraction Completed	OK
2025-08-31 05:55:59	Extracting String data from APK	OK
2025-08-31 05:56:00	Extracting String data from Code	OK
2025-08-31 05:56:00	Extracting String values and entropies from Code	OK
2025-08-31 05:56:05	Performing Malware check on extracted domains	OK
2025-08-31 05:56:15	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.