Mobile Application Security Assessment Report

Internship Month 2 Project – Rhombix Technologies
Intern: Syeda Fakiha
Internship Domain: Cybersecurity
App Assessed: InsecureBankv2.apk
Tool Used: Mob SF (Mobile Security Framework)
Date of Report: July 2025

Table of contents

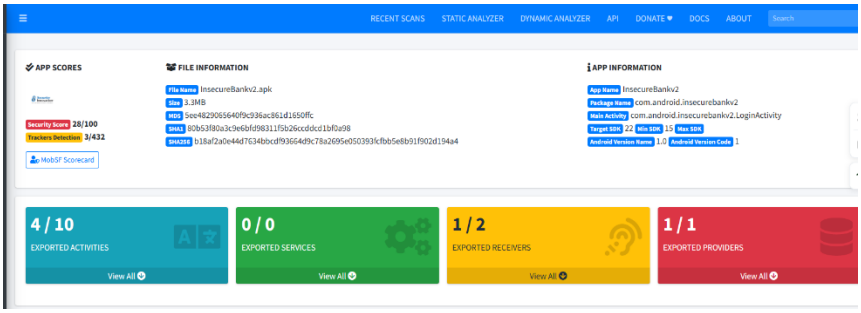
1. Introduction

This report documents a mobile application security assessment of the Android app *InsecureBankv2.apk*. The project was performed as part of my Month 2 internship task in the Cybersecurity domain at Rhombix Technologies. The goal of the project was to analyze the app for potential security vulnerabilities and suggest remediations based on industry standards.

The assessment was conducted using Mob SF (Mobile Security Framework), an open-source security tool for automated static and dynamic analysis of mobile applications.

2. APK Overview

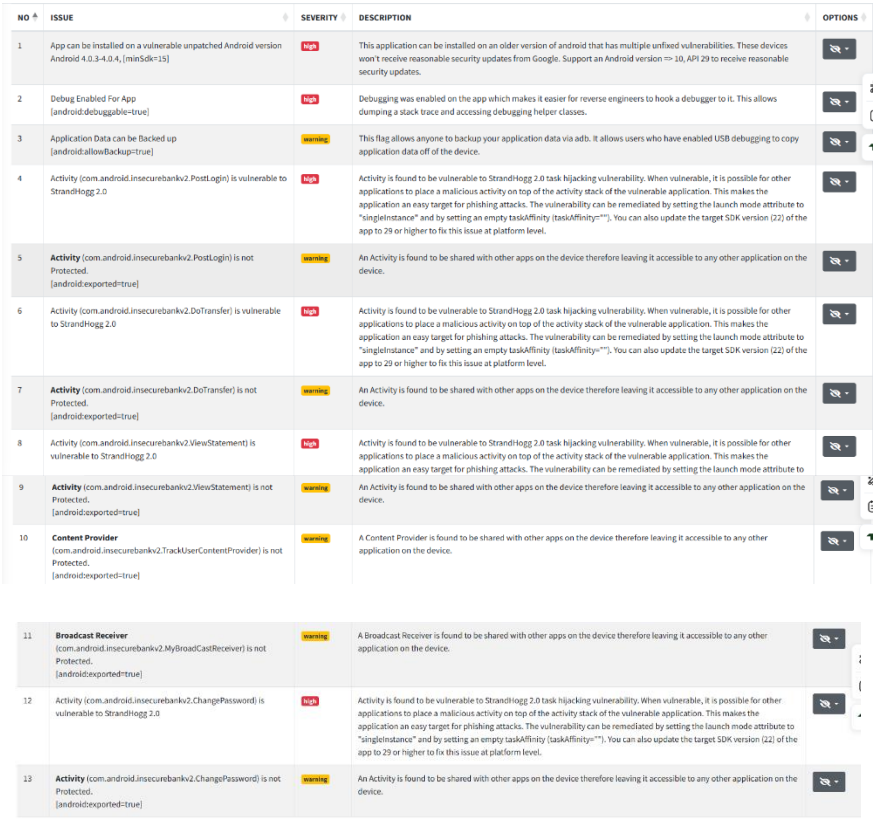
Field	Value
App name	InsecureBankv2
Package name	com.android.insecurebankv2
File size	3.3 MB
Target SKD	22
Min SDK	15
Signature	v1 only (Janus vulnerable)
MobSF Report Date	July 15, 2025
Security Score	28/100 (Critical Risk)



3. Security Analysis Summary

Vulnerability	Severity	Description
StrandHogg 2.0	High	Activities vulnerable to task hijacking (e.g., Do Transfer, Post Login)
Hardcoded Secrets	High	Passwords and usernames are visible in the source code
Insecure Signature Scheme	High	App uses only v1 signing – vulnerable to Janus exploit
Exported Components	Medium	Activities and Broadcast Receivers can be hijacked
Debug Mode Enabled	Medium	App is debug able – easier to reverse engineer

Allow Backup Enabled	Low	App data can be extracted through ADB
Malware Permissions	Medium	SEND_SMS, READ_CONTACTS, WRITE_EXTERNAL_STORAGE
Trackers Found	Low	Google AdMob, Analytics, Tag Manager



NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	
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	Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
5	**Activity** (com.android.insecurebankv2.PostLogin) 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.	
6	Activity (com.android.insecurebankv2.DoTransfer) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
7	**Activity** (com.android.insecurebankv2.DoTransfer) 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.android.insecurebankv2.ViewStatement) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to	
9	**Activity** (com.android.insecurebankv2.ViewStatement) 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	**Content Provider** (com.android.insecurebankv2.TrackUserContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
11	**Broadcast Receiver** (com.android.insecurebankv2.MyBroadCastReceiver) is not Protected. [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.	
12	Activity (com.android.insecurebankv2.ChangePassword) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
13	**Activity** (com.android.insecurebankv2.ChangePassword) 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. Permissions Audit

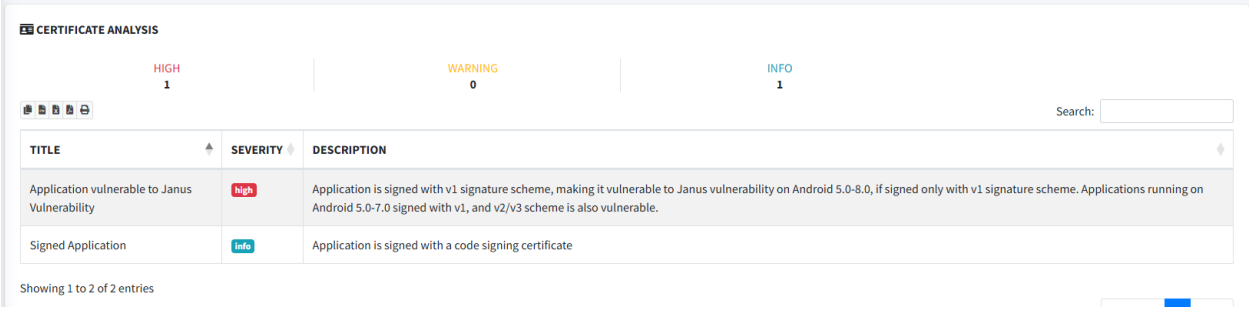
The app requests multiple **dangerous permissions,** which can compromise user privacy and be abused by malicious actors.

- SEND_SMS: Can send SMS without consent (may cost user money)
- READ_CONTACTS: Can steal contact list
- READ_PROFILE: May read personal profile data
- WRITE_EXTERNAL_STORAGE: Allows access to external data
- USE_CREDENTIALS & GET_ACCOUNTS: May access sensitive login tokens

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.

5. Certificate & Signing Issues

The APK was found to be signed using only the **v1 signature scheme**, which is outdated and vulnerable to the **Janus vulnerability** (CVE-2017-13156).
This could allow an attacker to **inject malicious code** into the app without breaking its signature.



6. Detailed Vulnerabilities

StrandHogg 2.0 (Activity Hijacking)

Several activities (DoTransfer, ViewStatement, ChangePassword) are vulnerable to StrandHogg 2.0. This allows malicious apps to hijack the task stack and overlay fake UI, enabling **credential theft or phishing**.

Suggested Fixes:

- Set launchMode "singleInstance"
- Use taskAffinity=""
- Upgrade target SDK to 29+

Hardcoded Secrets

Multiple user credentials and sensitive strings were found in the decompiled source code. This violates secure coding practices and can be exploited by attackers.

Exported Components

Activities, Content Providers, and Broadcast Receivers are exposed to other apps via android: exported "true". These should be made private unless explicitly required.

Debuggable App

The app has android:debuggable=true, allowing attackers to hook into it and reverse-engineer its code during runtime. This should be disabled in production.

7. Recommendations

- Remove hardcoded secrets from source code
- Use secure key storage mechanisms
- Use v2/v3 APK signing schemes
- Minimize dangerous permissions
- Set android:debuggable=false
- Apply android:exported="false" to non-public components
- Fix manifest issues (e.g. StrandHogg risk)
- Upgrade target SDK to Android 10+ (API 29+**)**

8. Conclusion

The application InsecureBankv2 demonstrated several serious vulnerabilities that could lead to data theft, fraud, and user exploitation. By identifying these flaws, I've learned how insecure mobile coding practices can introduce risks, and how security testing tools like Mob SF can be used to mitigate them.
This project helped me understand Android app internals, vulnerability analysis, and reporting methods used by cybersecurity professionals.

ANDROID STATIC ANALYSIS REPORT

InsecureBankv2 (1.0)

File Name:	InsecureBankv2.apk
Package Name:	com.android.insecurebankv2
Scan Date:	July 15, 2025, 8:12 a.m.
App Security Score:	28/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	9	0	0	1

FILE INFORMATION

File Name: InsecureBankv2.apk
Size: 3.3MB
MD5: 5ee4829065640f9c936ac861d1650ffc
SHA1: 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98
SHA256: b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfbb5e8b91f902d194a4

APP INFORMATION

App Name: InsecureBankv2
Package Name: com.android.insecurebankv2
Main Activity: com.android.insecurebankv2.LoginActivity
Target SDK: 22
Min SDK: 15
Max SDK:
Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 10
Services: 0
Receivers: 2
Providers: 1
Exported Activities: 4
Exported Services: 0
Exported Receivers: 1
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: ST=MA, L=Boston, O=SI, OU=Services, CN=Dinesh Shetty
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-24 20:37:08+00:00
Valid To: 2040-07-17 20:37:08+00:00
Issuer: ST=MA, L=Boston, O=SI, OU=Services, CN=Dinesh Shetty
Serial Number: 0x6bb4f616
Hash Algorithm: sha256
md5: 6a736d89abb13d7165e7cff905ac928d
sha1: a1bae91a2b1620f6c9dab425e69fc32ba1e97741
sha256: 8092db81ae717486631a1534977def465ee112903e1553d38d41df8abd57a375
sha512: 53770f3f69916f74ddd6e750ae16fd9b23fa5b2c8e9e53bd5a84202d7d7c44a26ede13e6db450ab0c1d9f64534802b88ebb0b4de1da076b62112d9b122cbbd92
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check</td></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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: **6** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
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	Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity (com.android.insecurebankv2.PostLogin) 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.
6	Activity (com.android.insecurebankv2.DoTransfer) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.
7	Activity (com.android.insecurebankv2.DoTransfer) 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.android.insecurebankv2.ViewStatement) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.
9	Activity (com.android.insecurebankv2.ViewStatement) 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	Content Provider (com.android.insecurebankv2.TrackUserContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider 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
11	Broadcast Receiver (com.android.insecurebankv2.MyBroadCastReceiver) is not Protected. [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.
12	Activity (com.android.insecurebankv2.ChangePassword) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.
13	Activity (com.android.insecurebankv2.ChangePassword) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SEND_SMS, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	0/44	

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

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"loginscreen_password" : "Password:"
"loginscreen_username" : "Username:"
VECoKGlOd10uMKpiLFkK46zikClkVy7m5Sv4lNe3KRY=
KglVFfxGq7C7ko+bqcJ8DTs8uzcctZAmlSX4/fuAvTk=
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsl7+5gLrSInCAebksSHto
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4lEIre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
MU3VGnFcvu612xTEKnGZFJFOwurNoeRHlUpI0GCgSFQ=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
qfDkyRZiTZGguvBzojuWMEqfI8Qqw5CcMB2eo7wr2iH9X2v+qlFOYNd9v9ffS1x0
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3utf4/9iPAviI=
2RUillTqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
3mNwt4SZ3Etv5TIhUa/RqouLnZPiat8RAS1ApJt5MxhvfIYxahkXg2hSNsePN+7M
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW

POSSIBLE SECRETS
EwZMQOzAsSbCW+73vnMc0IIAOIXmhdEPDWA4pBmTQFs=
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtIp3TGnIt
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
Fych2TPIScbLJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3rf841gO
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VIuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/qqDKEENUU4ZU=
M/9MnPtaDnNpsJGLBqvtFaALld0qI4JyMOfQfSncPhI=
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVIqzQMyOaB4=
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMlRzL0PE43M8=

SCAN LOGS

Timestamp	Event	Error
2025-07-15 08:12:48	Generating Hashes	OK

2025-07-15 08:12:48	Extracting APK	OK
2025-07-15 08:12:48	Unzipping	OK
2025-07-15 08:12:48	Parsing APK with androguard	OK
2025-07-15 08:12:50	Extracting APK features using aapt/aapt2	OK
2025-07-15 08:12:51	Getting Hardcoded Certificates/Keystores	OK
2025-07-15 08:12:54	Parsing AndroidManifest.xml	OK
2025-07-15 08:12:54	Extracting Manifest Data	OK
2025-07-15 08:12:54	Manifest Analysis Started	OK
2025-07-15 08:12:54	Performing Static Analysis on: InsecureBankv2 (com.android.insecurebankv2)	OK
2025-07-15 08:12:55	Fetching Details from Play Store: com.android.insecurebankv2	OK

2025-07-15 08:12:55	Checking for Malware Permissions	OK
2025-07-15 08:12:55	Fetching icon path	OK
2025-07-15 08:12:55	Library Binary Analysis Started	OK
2025-07-15 08:12:55	Reading Code Signing Certificate	OK
2025-07-15 08:12:55	Running APKiD 2.1.5	OK
2025-07-15 08:12:57	Detecting Trackers	OK
2025-07-15 08:12:59	Decompiling APK to Java with JADX	OK
2025-07-15 08:13:34	Converting DEX to Smali	OK
2025-07-15 08:13:34	Code Analysis Started on - java_source	OK
2025-07-15 08:13:35	Android SBOM Analysis Completed	OK
2025-07-15 08:13:35	Android SAST Completed	OK

2025-07-15 08:13:35	Android API Analysis Started	OK
2025-07-15 08:13:37	Android API Analysis Completed	OK
2025-07-15 08:13:40	Android Permission Mapping Started	OK
2025-07-15 08:13:42	Android Permission Mapping Completed	OK
2025-07-15 08:13:43	Android Behaviour Analysis Started	OK
2025-07-15 08:13:44	Android Behaviour Analysis Completed	OK
2025-07-15 08:13:44	Extracting Emails and URLs from Source Code	OK
2025-07-15 08:13:44	Email and URL Extraction Completed	OK
2025-07-15 08:13:44	Extracting String data from APK	OK
2025-07-15 08:13:44	Extracting String data from Code	OK
2025-07-15 08:13:44	Extracting String values and entropies from Code	OK

2025-07-15 08:13:47	Performing Malware check on extracted domains	OK
2025-07-15 08:13:47	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.