ANDROID STATIC ANALYSIS REPORT

InsecureBankv2 (2.0)

File Name:	InsecureBankv2.apk
Package Name:	com.android.insecurebankv2
Scan Date:	Dec. 24, 2025, 6:34 a.m.
App Security Score:	27/100 (CRITICAL RISK)
Grade:	F
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
8	10	0	0	1

FILE INFORMATION

File Name: InsecureBankv2.apk
Size: 3.46MB
MD5: 0bb3788ed48ab0960109c39a98923445
SHA1: aecc3e9daffad303cc323b6e21701303ac33257c
SHA256: 771cdae4693b7f33df702074bf9a0dfb6e38bebdbeb74cfd202314d73a516d9e

APP INFORMATION

App Name: InsecureBankv2
Package Name: com.android.insecurebankv2
Main Activity: com.android.insecurebankv2.LoginActivity
Target SDK: 26
Min SDK: 15
Max SDK:
Android Version Name: 2.0

Android Version Code: 2

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: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-07-14 16:26:49+00:00
Valid To: 2048-07-06 16:26:49+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: fa57c5e4cb664e2e1237a1082fbb06e8
sha1: e4647b8ca96ca602bd578679a0c74d07a42221a6
sha256: 2d5b73a0c1f2af143f9a31c65339e0ab79eeab8e7cd4d631eec8880649489feb
sha512: 3ac2c95586ce1df74144937226e0a93ed7d06fdfacbb2596535577aaa08f41c0674a1ca8f1b6d37bad06789536e9fdb56b291ae8f548d1ce00c2212b93d782ed
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 72d45e8af20c45080f644a7db116c25545ecc318cde33b60ee172cd30358dae6
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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
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	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check
	Compiler	r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **2** | 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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

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 (26) 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 (26) of the app to 29 or higher to fix this issue at platform level.

NO	ISSUE	SEVERITY	DESCRIPTION
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 (26) 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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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 (26) 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	10/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SEND_SMS, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.READ_CALL_LOG, 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:"
Fych2TPIScbLJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3rf841gO
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
2RUillTqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
KglVFfxGq7C7ko+bqcJ8DTs8uzcctZAmlSX4/fuAvTk=
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4lEIre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
qfDkyRZiTZGguvBzojuWMEqfI8Qqw5CcMB2eo7wr2iH9X2v+qlFOYNd9v9ffS1x0
VECoKGlOd10uMKpiLFkK46zikCIkVy7m5Sv4INe3KRY=
EwZMQOzAsSbCW+73vnMc0IIAOIXmhdEPDWA4pBmTQFs=
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsI7+5gLrSInCAebksSHto
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtIp3TGnIt
3mNwt4SZ3Etv5TIhUa/RqouLnZPiat8RAS1ApJt5MxhvfIYxahkXg2hSNsePN+7M

POSSIBLE SECRETS
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVIqzQMyOaB4=
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMlRzL0PE43M8=
MU3VGnFcvu612xTEKnGZFJFOwurNoeRHlUpI0GCgSFQ=
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3utf4/9iPAviI=
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/qqDKEENUU4ZU=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VIuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
M/9MnPtaDnNpsJGLBqvtFaALld0qI4JyMOfQfSncPhI=
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=

SCAN LOGS

Timestamp	Event	Error
2025-12-24 06:34:06	Generating Hashes	OK

2025-12-24 06:34:06	Extracting APK	OK
2025-12-24 06:34:06	Unzipping	OK
2025-12-24 06:34:06	Parsing APK with androguard	OK
2025-12-24 06:34:06	Extracting APK features using aapt/aapt2	OK
2025-12-24 06:34:06	Getting Hardcoded Certificates/Keystores	OK
2025-12-24 06:34:06	Parsing AndroidManifest.xml	OK
2025-12-24 06:34:06	Extracting Manifest Data	OK
2025-12-24 06:34:06	Manifest Analysis Started	OK
2025-12-24 06:34:06	Performing Static Analysis on: InsecureBankv2 (com.android.insecurebankv2)	OK
2025-12-24 06:34:08	Fetching Details from Play Store: com.android.insecurebankv2	OK

2025-12-24 06:34:09	Checking for Malware Permissions	OK
2025-12-24 06:34:09	Fetching icon path	OK
2025-12-24 06:34:09	Library Binary Analysis Started	OK
2025-12-24 06:34:09	Reading Code Signing Certificate	OK
2025-12-24 06:34:10	Running APKiD 3.0.0	OK
2025-12-24 06:34:13	Detecting Trackers	OK
2025-12-24 06:34:15	Decompiling APK to Java with JADX	OK
2025-12-24 06:34:43	Converting DEX to Smali	OK
2025-12-24 06:34:44	Code Analysis Started on - java_source	OK
2025-12-24 06:34:44	Android SBOM Analysis Completed	OK
2025-12-24 06:34:45	Android SAST Completed	OK

2025-12-24 06:34:45	Android API Analysis Started	OK
2025-12-24 06:34:46	Android API Analysis Completed	OK
2025-12-24 06:34:47	Android Permission Mapping Started	OK
2025-12-24 06:34:48	Android Permission Mapping Completed	OK
2025-12-24 06:34:48	Android Behaviour Analysis Started	OK
2025-12-24 06:34:49	Android Behaviour Analysis Completed	OK
2025-12-24 06:34:49	Extracting Emails and URLs from Source Code	OK
2025-12-24 06:34:49	Email and URL Extraction Completed	OK
2025-12-24 06:34:49	Extracting String data from APK	OK
2025-12-24 06:34:50	Extracting String data from Code	OK
2025-12-24 06:34:50	Extracting String values and entropies from Code	OK

2025-12-24 06:34:52	Performing Malware check on extracted domains	OK
2025-12-24 06:34:52	Updating Database...	OK

Report Generated by - MobSF v4.4.4

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.