APP SCORES

Security Score **28/100**

Trackers Detection **3/432**

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

4 / 10
EXPORTED ACTIVITIES
View All

0 / 0
EXPORTED SERVICES
View All

1 / 2
EXPORTED RECEIVERS
View All

1 / 1
EXPORTED PROVIDERS
View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
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

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
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_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.	
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	

Showing 1 to 9 of 9 entries

Previous 1 Next

ANDROID API

Search:

API	FILES
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
1	0	1

Search:

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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
6	7	0	0

Search:

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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

Showing 1 to 10 of 13 entries

Previous 1 2 Next

</> CODE ANALYSIS

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
No data available in table					

Showing 0 to 0 of 0 entries

Previous Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table									

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check
Compiler	dx (possible dexmerge)
Manipulator Found	dexmerge

Showing 1 to 3 of 3 entries

Previous 1 Next

Showing 1 to 1 of 1 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	7/25	Other Common Permissions	0/44
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			

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS

DOMAIN MALWARE CHECK

URLS

EMAILS

TRACKERS

Search:

TRACKER NAME	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

Showing 1 to 3 of 3 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **25** secrets

"loginscreen_password" : "Password:"
"loginscreen_username" : "Username:"
3mNwt4SZ3Etv5TIhUa/RqouLnZPiat8RAS1ApJt5MxhvfIYxahkXg2hSNsePN+7M
Fych2TPIScbLJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3rf841gO
gcr/blkg3lQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/qqDKEENUU4ZU=
qfDkyRZiTZGguvBzojuWMEqfI8Qqw5CcMB2eo7wr2iH9X2v+qlFOYNd9v9ffS1x0
2RUillTqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsI7+5gLrSInCAebksSHto
KglVFfxGq7C7ko+bqcJ8DTs8uzcctZAmlSX4/fuAvTk=
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMlRzL0PE43M8=
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4lEIre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVIqzQMyOaB4=
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VIuAHdYuT1VPLHst51ZSG89jehZq7ujXyH
M/9MnPtaDnNpsJGLBqvtFaALld0qI4JyMOfQfSncPhI=
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
EwZMQOzAsSbCW+73vnMc0IIAOIXmhdEPDWA4pBmTQFs=

eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
SxPdgyHHu8QFxBqcknBJfZgRiWxxWH3utf4/9iPAviI=
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtIp3TGnIt
VECoKGlOd10uMKpiLFkK46zikCIkVy7m5Sv4INe3KRY=
MU3VGnFcvu612xTEKnGZFJFOwurNoeRHlUpI0GCgSFQ=

A STRINGS

From APK Resource

▶ Show all **3768** strings

From Code

▶ Show all **6474** strings

From Shared Objects

ACTIVITIES

▼ Showing all **10** activities
com.android.insecurebankv2.LoginActivity
com.android.insecurebankv2.FilePrefActivity
com.android.insecurebankv2.DoLogin
com.android.insecurebankv2.PostLogin
com.android.insecurebankv2.WrongLogin
com.android.insecurebankv2.DoTransfer
com.android.insecurebankv2.ViewStatement
com.android.insecurebankv2.ChangePassword
com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.purchase.InAppPurchaseActivity

SERVICES

RECEIVERS

▼ Showing all **2** receivers
com.android.insecurebankv2.MyBroadCastReceiver
com.google.android.gms.wallet.EnableWalletOptimizationReceiver

PROVIDERS

▼ Showing all **1** providers
com.android.insecurebankv2.TrackUserContentProvider

LIBRARIES

SBOM

FILES

▶ Show all **555** files

Version v4.4.0