ANDROID STATIC ANALYSIS REPORT

InsecureBankv2 (1.0)

File Name:	InsecureBankv2.apk
Package Name:	com.android.insecurebankv2
Scan Date:	April 21, 2022, 5:33 a.m.
App Security Score:	13/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	3/427

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
8	3	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

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
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

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

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.

PERMISSION	STATUS	INFO	DESCRIPTION
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	FINDINGS: Anti-VM Code — DETAILS: Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check FINDINGS: Compiler — DETAILS: dx (possible dexmerge) FINDINGS: Manipulator Found — DETAILS: dexmerge

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.
3	Activity (com.android.insecurebankv2.PostLogin) is not Protected. [android:exported=true]	high	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	Activity (com.android.insecurebankv2.DoTransfer) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.android.insecurebankv2.ViewStatement) is not Protected. [android:exported=true]	high	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	Content Provider (com.android.insecurebankv2.TrackUserContentProvider) is not Protected. [android:exported=true]	high	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
7	Broadcast Receiver (com.android.insecurebankv2.MyBroadCastReceiver) is not Protected. [android:exported=true]	high	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.
8	Activity (com.android.insecurebankv2.ChangePassword) is not Protected. [android:exported=true]	high	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

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

TRACKER	CATEGORIES	URL
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:"

Report Generated by - MobSF v3.5.2 Beta

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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.