



ANDROID STATIC ANALYSIS REPORT



 InsecureBankv2 (1.0)

File Name: InsecureBankv2.apk

Package Name: com.android.insecurebankv2

Scan Date: April 4, 2023, 2:41 a.m.






App Security Score: 33/100 (HIGH RISK)

Grade:



Trackers Detection: 3/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	4	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

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=15]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book', 'call lists'].
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
17	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

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:"

Report Generated by - MobSF v3.6.3 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.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).