Dynamic Analyst

File Info

File Name: InsecureBankv2.apk

Size: 3.3 MB

MD5: 5ee4829065640f9c936ac861d1650ffc

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
```

Warning

- **Signed Application**: Application is signed with a code signing certificate
- **Application vulnerable to Janus Vulnerability**: 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 Information

Package Name: com.android.insecurebankv2

Main Activity: com.android.insecurebankv2.LoginActivity

Min SDK Version: 15

Check Application Permission

Permission	Security level	Infomation	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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_CALL_LOG	dangerous		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.

The Activities of application:

- 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

Check Manifest Application:

Rule	Title	Severity	Description	Name	Component
app_is_debuggable	Debug Enabled For App<br>[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.	Debug Enabled For App [android:debuggable=true]	()
app_allowbackup	Application Data can be Backed up<br>[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.	Application Data can be Backed up [android:allowBackup=true]	()

Activities that can be activated

Activity Name
com.android.insecurebankv2.PostLogin
com.android.insecurebankv2.DoTransfer
com.android.insecurebankv2.ViewStatement
com.android.insecurebankv2.ChangePassword

Exported Report PDF