NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android versionAndroid 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.	Suppression the rule vulnerable_os_version in com.android.insecurebankv2
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.	Suppression the rule app_is_debuggable in com.android.insecurebankv2
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.	Suppression the rule app_allowbackup in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_task_hijacking2 in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_explicitly_exported in com.android.insecurebankv2

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.	Suppression the rule activity_task_hijacking2 in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_explicitly_exported in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_task_hijacking2 in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_explicitly_exported in com.android.insecurebankv2
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.	Suppression the rule provider_explicitly_exported in com.android.insecurebankv2
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.	Suppression the rule receiver_explicitly_exported in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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 (22) of the app to 29 or higher to fix this issue at platform level.	Suppression the rule activity_task_hijacking2 in com.android.insecurebankv2

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	Suppression the rule activity_explicitly_exported in com.android.insecurebankv2