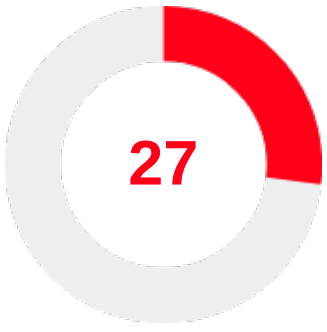
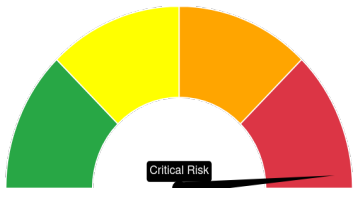
Security Score



Security Score 27/100

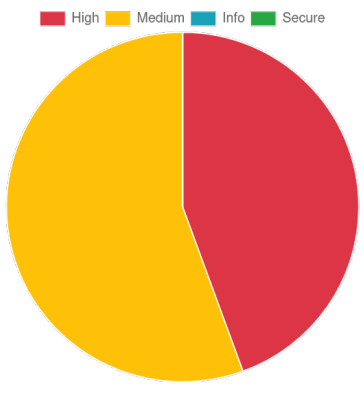
Risk Rating



Grade

A B C **F**

Severity Distribution (%)



Privacy Risk

3

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
8	10	0	0	1

high Application signed with debug certificate	CERTIFICATE
high Certificate algorithm vulnerable to hash collision	CERTIFICATE
high App can be installed on a vulnerable unpatched Android version	MANIFEST
high Debug Enabled For App	MANIFEST
high Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.android.insecurebankv2.DoTransfer) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.android.insecurebankv2.ViewStatement) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.android.insecurebankv2.ChangePassword) is vulnerable to StrandHogg 2.0	MANIFEST
medium Application vulnerable to Janus Vulnerability	CERTIFICATE
medium Application Data can be Backed up	MANIFEST
medium Activity (com.android.insecurebankv2.PostLogin) is not Protected.	MANIFEST
medium Activity (com.android.insecurebankv2.DoTransfer) is not Protected.	MANIFEST
medium Activity (com.android.insecurebankv2.ViewStatement) is not Protected.	MANIFEST
medium Content Provider (com.android.insecurebankv2.TrackUserContentProvider) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.insecurebankv2.MyBroadCastReceiver) is not Protected.	MANIFEST
medium Activity (com.android.insecurebankv2.ChangePassword) is not Protected.	MANIFEST
medium Application contains Privacy Trackers	TRACKERS
medium This app may contain hardcoded secrets	SECRETS
hotspot Found 10 critical permission(s)	PERMISSIONS

```
Ensure that these permissions are required by the application.

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): grants read access to the user's call log. - Allows an application to read the user's call log.

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.
```

MobSF Application Security Scorecard generated for (InsecureBankv2 2.0)

Version v4.4.4