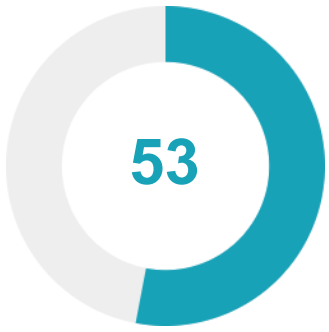
Security Score



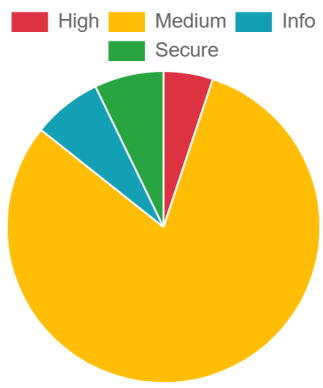
Security Score 53/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High
2

Medium
31

Info
3

Secure
3

Hotspot
1

high App can be installed on a vulnerable upatched Android version	MANIFEST
high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	CODE
medium Application vulnerable to Janus Vulnerability	CERTIFICATE
medium Activity-Alias (com.android.system.app.ui.Launcher2Activity) is not Protected.	MANIFEST
medium Activity-Alias (com.android.system.app.ui.LauncherActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.BatteryLevelReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.BootCompletedReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.ConnectivityReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.DeviceAdministrationReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.PackageChangedReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.PhoneStateReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.PowerConnectionReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.SensorsChangedReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.SimChangedReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.UserPresentReceiver) is not Protected.	MANIFEST
medium Service (com.android.system.app.services.FirebaseInstanceIDService) is not Protected.	MANIFEST
medium Service (com.android.system.app.services.FirebaseMessageService) is not Protected.	MANIFEST
medium Service (com.android.system.app.services.NotificationService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Service (com.android.system.app.services.ScreenReaderService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (com.android.system.app.receivers.LaunchAppReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium High Intent Priority (1000) - {1} Hit(s)	MANIFEST
medium App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	CODE
medium SHA-1 is a weak hash known to have hash collisions.	CODE
medium App creates temp file. Sensitive information should never be written into a temp file.	CODE

medium	The App uses an insecure Random Number Generator.	CODE
medium	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	This App may request root (Super User) privileges.	CODE
medium	MD5 is a weak hash known to have hash collisions.	CODE
medium	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium	Application contains Privacy Trackers	TRACKERS
medium	This app may contain hardcoded secrets	SECRETS
info	The App logs information. Sensitive information should never be logged.	CODE
info	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	CODE
info	App talks to a Firebase database	FIREBASE
secure	This App may have root detection capabilities.	CODE
secure	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
secure	Firebase Remote Config disabled	FIREBASE
hotspot	Found 30 critical permission(s)	PERMISSIONS

MobSF Application Security Scorecard generated for (Play Service Settings 8.1.7)