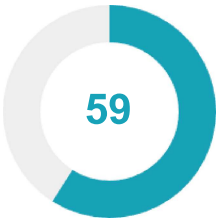
Security Score



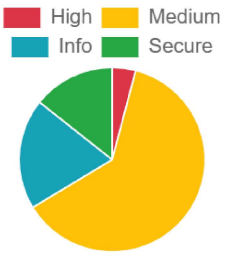
Security Score 59/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High
1

Medium
13

Info

Secure

4

3

Hotspot
0

high Domain config is insecurely configured to permit clear text traffic to these domains in scope	NETWORK
medium Base config is configured to trust system certificates	NETWORK
medium Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [android:exported=true]	MANIFEST
medium Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	MANIFEST
medium Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	MANIFEST
medium Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	MANIFEST
medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium IP Address disclosure	CODE
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 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 MD5 is a weak hash known to have hash collisions.	CODE
medium SHA-1 is a weak hash known to have hash collisions.	CODE
medium This app may contain hardcoded secrets	SECRETS
info This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	CODE
info The App logs information. Sensitive information should never be logged.	CODE
info App can write to App Directory. Sensitive Information should be encrypted.	CODE
info This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	CODE
secure Base config is configured to disallow clear text traffic to all domains	NETWORK
secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
secure This application has no privacy trackers	TRACKERS

MobSF Application Security Scorecard generated for (Pager Rat 0.9.1)

© 2026 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.

Version v4.4.5