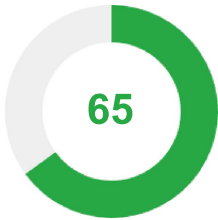
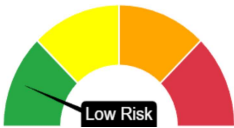


★ Security Score



Security Score 65/100

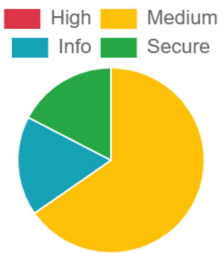
🛡️ Risk Rating



Grade



📊 Severity Distribution (%)



🏠 Privacy Risk



User/Device Trackers

📄 Findings



High  
0



Medium  
11



Info



Secure



3



3



Hotspot  
0

medium

Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

medium

Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

medium

Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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

The App uses an insecure Random Number Generator.

[CODE](#)

medium

SHA-1 is a weak hash known to have hash collisions.

[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

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

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 can write to App Directory. Sensitive Information should be encrypted.

[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 0.8.8)