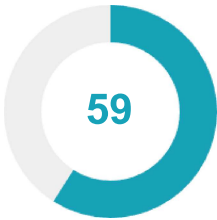


★ Security Score



Security Score 59/100

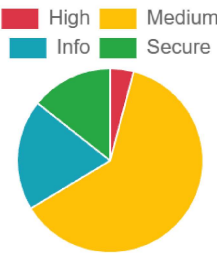
🛡️ Risk Rating



Grade



📊 Severity Distribution (%)



🏠 Privacy Risk



User/Device Trackers

📄 Findings



High
1



Medium
13




Info



Secure

<div><div></div><div>4</div></div> <div><div></div><div>Hotspot</div><div>1</div></div>	<div><div></div><div>3</div></div>
<div><div>high</div><div>Domain config is insecurely configured to permit clear text traffic to these domains in scope</div></div>	NETWORK
<div><div>medium</div><div>Base config is configured to trust system certificates</div></div>	NETWORK
<div><div>medium</div><div>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]</div></div>	MANIFEST
<div><div>medium</div><div>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]</div></div>	MANIFEST
<div><div>medium</div><div>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]</div></div>	MANIFEST
<div><div>medium</div><div>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]</div></div>	MANIFEST
<div><div>medium</div><div>SHA-1 is a weak hash known to have hash collisions.</div></div>	CODE
<div><div>medium</div><div>The App uses an insecure Random Number Generator.</div></div>	CODE
<div><div>medium</div><div>App can read/write to External Storage. Any App can read data written to External Storage.</div></div>	CODE
<div><div>medium</div><div>IP Address disclosure</div></div>	CODE
<div><div>medium</div><div>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.</div></div>	CODE
<div><div>medium</div><div>MD5 is a weak hash known to have hash collisions.</div></div>	CODE
<div><div>medium</div><div>Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</div></div>	CODE
<div><div>medium</div><div>This app may contain hardcoded secrets</div></div>	SECRETS
<div><div>info</div><div>App can write to App Directory. Sensitive Information should be encrypted.</div></div>	CODE
<div><div>info</div><div>The App logs information. Sensitive information should never be logged.</div></div>	CODE
<div><div>info</div><div>This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.</div></div>	CODE
<div><div>info</div><div>This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.</div></div>	CODE
<div><div>secure</div><div>Base config is configured to disallow clear text traffic to all domains</div></div>	NETWORK
<div><div>secure</div><div>This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</div></div>	CODE
<div><div>secure</div><div>This application has no privacy trackers</div></div>	TRACKERS
<div><div>hotspot</div><div>Found 1 critical permission(s)</div></div>	PERMISSIONS

MobSF Application Security Scorecard generated for  (Pager Rat 0.9.2) 