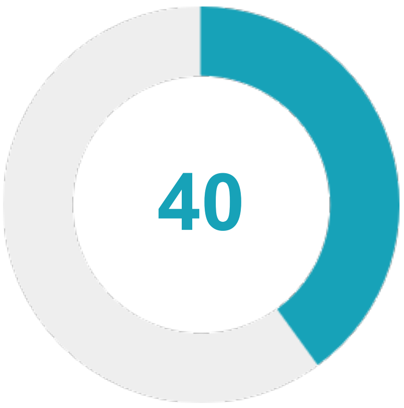
Security Score



Security Score 40/100

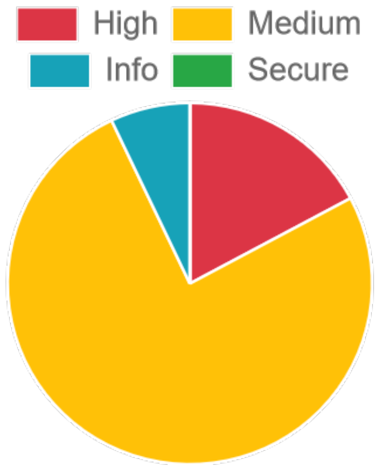
Risk Rating

Medium Risk

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

1

User/Device Trackers

Findings

High	7
Medium	31
Info	3
Secure	0
Hotspot	2

high Application signed with debug certificate — CERTIFICATE

high Base config is configured to trust user installed certificates — NETWORK

high Domain config is insecurely configured to permit clear text traffic to these domains in scope — NETWORK

high App can be installed on a vulnerable upatched Android version — MANIFEST

high Clear text traffic is Enabled For App — MANIFEST

high Debug Enabled For App — MANIFEST

high Debug configuration enabled. Production builds must not be debuggable. — CODE

medium Application vulnerable to Janus Vulnerability — CERTIFICATE

medium Certificate algorithm might be vulnerable to hash collision — CERTIFICATE

medium Base config is configured to trust system certificates — NETWORK

medium Application Data can be Backed up — MANIFEST

medium Activity (app.spy24.systemwifi.view.RegisterActivity) is not Protected. — MANIFEST

medium Activity (app.spy24.systemwifi.view.MainActivity) is not Protected. — MANIFEST

medium Activity (app.spy24.systemwifi.view.QrActivity) is not Protected. — MANIFEST

medium Broadcast Receiver (app.spy24.systemwifi.controller.receiver.AppReceiver) is not Protected. MANIFEST

medium Broadcast Receiver (app.spy24.systemwifi.controller.receiver.SMSReceiver) is not Protected. MANIFEST

medium Broadcast Receiver (app.spy24.systemwifi.controller.receiver.CallReceiver) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Broadcast Receiver (app.spy24.systemwifi.controller.receiver.DeviceAdmin) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.NotificationReceiver) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.receiver.CallAppService) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.receiver.CallRedirection) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.functionality.AudioService) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.accessibillity.Accessibility) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.accessibillity.UpdateAccessibillity) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.notification.NotificationListener) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (app.spy24.systemwifi.controller.service.functionality.ScreenService) is not Protected. 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 (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. MANIFEST

medium App can read/write to External Storage. Any App can read data written to External Storage. 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 Files may contain hardcoded sensitive information like usernames, passwords, keys etc. CODE

medium The App uses an insecure Random Number Generator. CODE

medium App creates temp file. Sensitive information should never be written into a temp file. CODE

medium MD5 is a weak hash known to have hash collisions. 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 listens to Clipboard changes. Some malware also listen to Clipboard changes. CODE

info This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files. CODE

hotspot Found 26 critical permission(s) PERMISSIONS

hotspot Found 1 certificate/key file(s) FILES

MobSF Application Security Scorecard generated for (system.wifi 1.0)