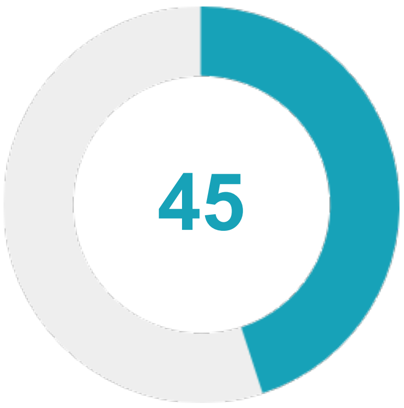
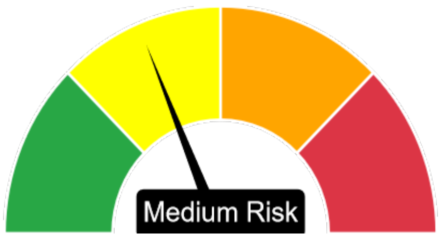
### Security Score



Security Score 45/100

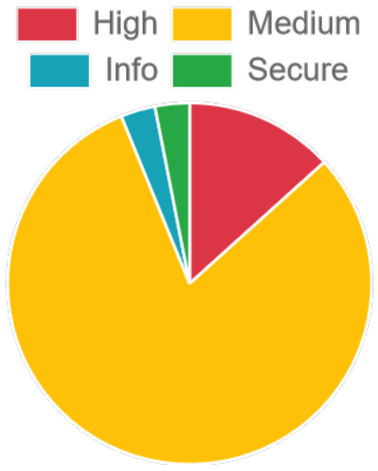
### Risk Rating



Grade

A **B** C F

### Severity Distribution (%)



### Privacy Risk

7

User/Device Trackers

### Findings

| High | Medium | Info | Secure | Hotspot |
|---|---|---|---|---|
| **4** | **23** | **1** | **1** | **1** |

**high** Certificate algorithm vulnerable to hash collision — CERTIFICATE

**high** The file or SharedPreference is World Readable. Any App can read from the file — CODE

**high** The file or SharedPreference is World Writable. Any App can write to the file — CODE

**high** Application contains Privacy Trackers — TRACKERS

**medium** App can be installed on a vulnerable Android version — MANIFEST

**medium** Activity (com.mmguardian.activity.initial_setup.MessagingAppEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppYellowEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppRedEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppPurpleEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppOrangeEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppGreenEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppBlueEntryPointActivity) is not Protected. — MANIFEST

**medium** Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppBlackEntryPointActivity) is not Protected. — MANIFEST

**medium** TaskAffinity is set for activity — MANIFEST

**medium** Activity (com.mmguardian.safebrowser.SafeBrowserActivity) is not Protected. MANIFEST

**medium** Activity (com.mmguardian.activity.LockActivityNew) is not Protected. MANIFEST

**medium** Activity (com.mmguardian.activity.LockActivityNewAndroidS) 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** 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** 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** The App uses an insecure Random Number Generator. 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** App can read/write to External Storage. Any App can read data written to External Storage. CODE

**medium** This app may contain hardcoded secrets SECRETS

**info** The App logs information. Sensitive information should never be logged. CODE

**secure** This App may have root detection capabilities. CODE

**hotspot** Found 17 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for ( MMGuardian 4.0.14)