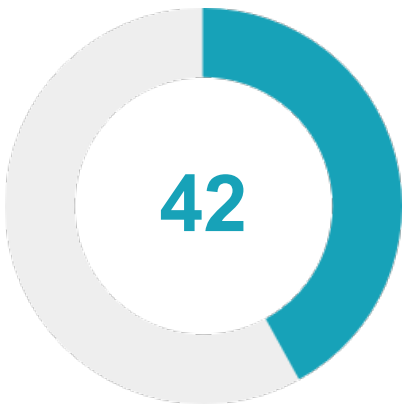
Security Score



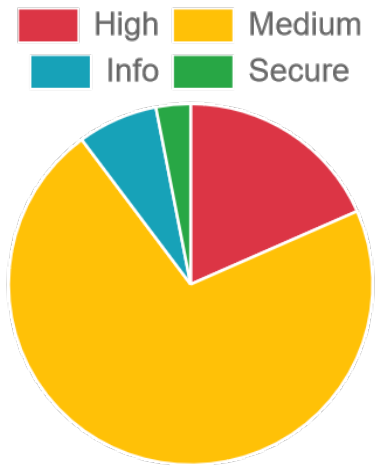
Security Score 42/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

4

User/Device Trackers

Findings

High **5** | Medium **19** | Info **2** | Secure **1** | Hotspot **2**

high Certificate algorithm vulnerable to hash collision — CERTIFICATE

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 The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. — CODE

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

medium Application Data can be Backed up — MANIFEST

medium Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. — MANIFEST

medium Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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 (com.google.android.gms.auth.api.signin.RevocationBoundService) 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 Service (com.transistorsoft.tsbackgroundfetch.FetchJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	CODE
medium IP Address disclosure	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 The App uses an insecure Random Number Generator.	CODE
medium SHA-1 is a weak hash known to have hash collisions.	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 App creates temp file. Sensitive information should never be written into a temp file.	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 copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	CODE
secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
hotspot Found 6 critical permission(s)	PERMISSIONS
hotspot Found 1 certificate/key file(s)	FILES

MobSF Application Security Scorecard generated for (KidControl Circles 6.0.19)