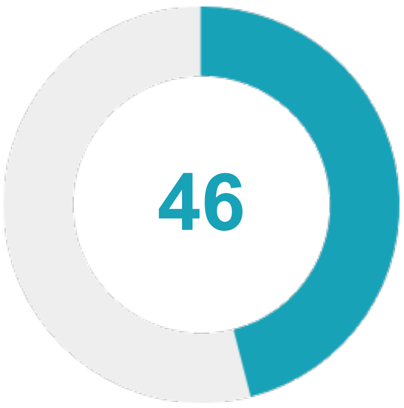
Security Score



Security Score 46/100

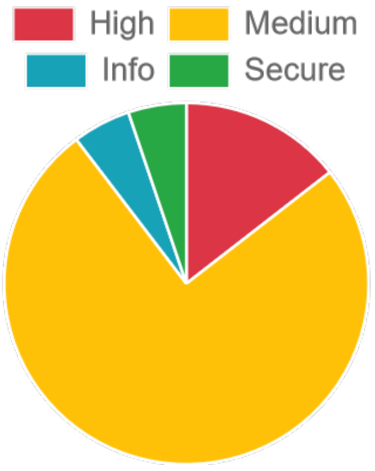
Risk Rating

Medium Risk

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

7

User/Device Trackers

Findings

High
5

Medium
25

Info
2

Secure
2

Hotspot
4

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

high App Link assetlinks.json file not found
MANIFEST

high Remote WebView debugging is enabled.
CODE

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

high Application contains Privacy Trackers
TRACKERS

medium App can be installed on a vulnerable Android version
MANIFEST

medium Activity (com.facebook.CustomTabActivity) is not Protected.
MANIFEST

medium Service (me.pushy.sdk.services.PushyJobService) is Protected by a permission, but the protection level of the permission should be checked.
MANIFEST

medium Content Provider (com.kidslox.app.providers.CommonPreferencesProvider) is not Protected.
MANIFEST

medium Broadcast Receiver (com.singular.sdk.SingularInstallReceiver) is not Protected.
MANIFEST

medium Activity (com.stripe.android.link.LinkRedirectHandlerActivity) is not Protected.
MANIFEST

medium Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) is not Protected.
MANIFEST

medium Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) is not Protected.
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 Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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 (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium High Intent Priority (9991) **MANIFEST**

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

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

medium The App uses an insecure Random Number Generator. **CODE**

medium MD5 is a weak hash known to have hash collisions. **CODE**

medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. **CODE**

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

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

info App can write to App Directory. Sensitive Information should be encrypted. **CODE**

secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. **CODE**

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

hotspot Found 16 critical permission(s) **PERMISSIONS**

hotspot Found 5 certificate/key file(s) **FILES**

hotspot App may communicate to a server (www.baidu.com) in OFAC sanctioned country (Hong Kong) DOMAINS

hotspot App may communicate to a server (www.bing.com) in OFAC sanctioned country (Sri Lanka) DOMAINS

MobSF Application Security Scorecard generated for 🔒 (Kidslox 9.6.1)