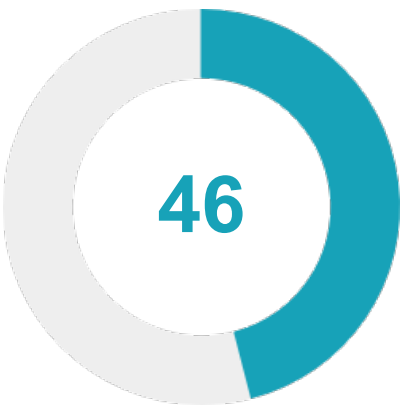
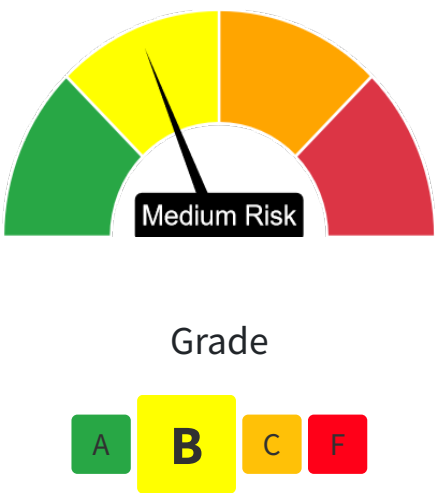


★ Security Score

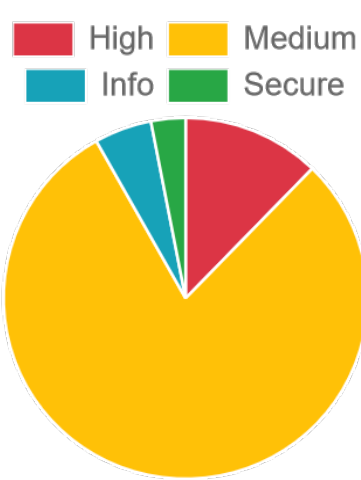


Security Score 46/100

🚨 Risk Rating



📊 Severity Distribution (%)



👤 Privacy Risk



User/Device Trackers

📄 Findings



High
7



Medium
45



Info
3



Secure
2



Hotspot
1

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 Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks

[CODE](#)

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

[CODE](#)

high Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks

[CODE](#)

high Application contains Privacy Trackers

[TRACKERS](#)

medium Application Data can be Backed up

[MANIFEST](#)

medium Activity (com.isharing.isharing.ui.MainActivity) is not Protected.

[MANIFEST](#)

medium Activity (com.isharing.isharing.ui.ShareExtActivity) is not Protected.

[MANIFEST](#)

medium Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected.

[MANIFEST](#)

medium Broadcast Receiver (com.isharing.isharing.receiver.InstallTrackerReceiver) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

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

[MANIFEST](#)

medium TaskAffinity is set for activity

[MANIFEST](#)


medium	Broadcast Receiver (com.umlaut.crowd.receiver.InsightReceiver) is not Protected.	MANIFEST
medium	Service (io.huq.sourcekit.service.HIVisitSubmissionJob) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (io.huq.sourcekit.service.HIDeviceInformationSubmissionJob) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (io.huq.sourcekit.wifi.HIWifiJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (io.huq.sourcekit.wifi.HICellularJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (io.huq.sourcekit.wifi.HIRepeatingNetworkJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (io.huq.sourcekit.service.HIPeriodicListeningJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (io.huq.sourcekit.location.HIGeofenceReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (io.huq.sourcekit.location.HILocationReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (io.huq.sourcekit.service.HIBootReceiver) is not Protected.	MANIFEST
medium	TaskAffinity is set for activity	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	Activity (com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.cumberland.sdk.core.broadcast.receiver.BootReceiver) is not Protected.	MANIFEST
medium	Service (com.cumberland.sdk.core.provider.HeartbeatProvider\$HeartbeatJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.cumberland.sdk.core.service.StartSdkJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.cumberland.sdk.core.service.SyncJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.cumberland.sdk.core.domain.controller.sampling.SdkSamplingController\$SdkSampleJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.cumberland.sdk.core.repository.kpi.web.WebAnalysisJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.applozic.mobicomkit.uiwidgets.KmFirebaseMessagingService) 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.applozic.mobicomkit.broadcast.TimeChangeBroadcastReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.applozic.mobicomkit.broadcast.ConnectivityReceiver) 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	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	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	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	IP Address disclosure	CODE
medium	MD5 is a weak hash known to have hash collisions.	CODE
medium	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	CODE
medium	This app may contain hardcoded secrets	SECRETS
info	The App logs information. Sensitive information should never be logged.	CODE
info	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	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
secure	This App may have root detection capabilities.	CODE

hotspot

Found 16 critical permission(s)

[PERMISSIONS](#)

MobSF Application Security Scorecard generated for  (iSharing 11.19.2.2) 