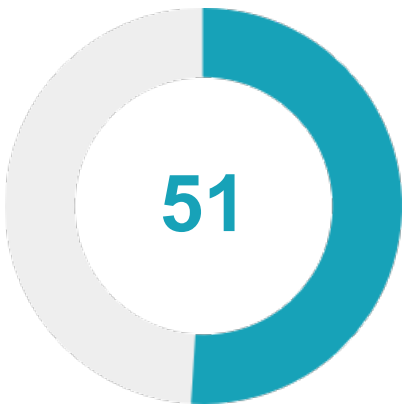
Security Score

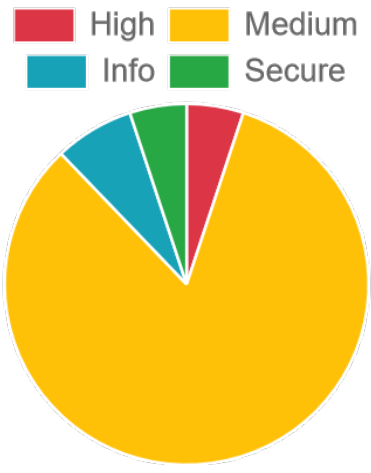


Security Score 51/100

Risk Rating

Grade

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
2	32	3	2	3

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 The file or SharedPreference is World Writable. Any App can write to the file	CODE
medium App can be installed on a vulnerable Android version	MANIFEST
medium Activity (org.findmykids.app.presentation.screens.home.ChildHomeActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (org.findmykids.app.presentation.receivers.RingModeBroadcastReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (org.findmykids.core.antiremoval.child.impl.data.ChildDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Service (org.findmykids.callscreening.child.ChildCallScreeningService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (org.findmykids.callscreening.child.missedCalls.presentation.PhoneStateReceiver) is not Protected.	MANIFEST
medium Service (org.findmykids.pushes.google.FcmListenerService) is not Protected.	MANIFEST
medium Service (pro.userx.server.job.ApiJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Service (org.findmykids.logSend.presentation.services.LogSendJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.SleepEventReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.BootReceiver) is Protected by a permission, but	MANIFEST

the protection level of the permission should be checked.

medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveFusedReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.StationReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityEventReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (org.findmykids.geo.producer.presentation.service.BootJobSchedulerService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.crowdin.platform.auth.AuthActivity) 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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	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	MD5 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	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	SHA-1 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 App can write to App Directory. Sensitive Information should be encrypted.	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 12 critical permission(s)	PERMISSIONS
hotspot Found 1 certificate/key file(s)	FILES
hotspot App may communicate to a server (www.baidu.com) in OFAC sanctioned country (Hong Kong)	DOMAINS

MobSF Application Security Scorecard generated for  (Kidsy 2.7.66-google)