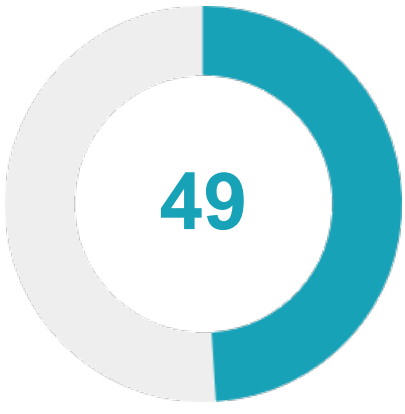



★ Security Score



49

Security Score 49/100

🚨 Risk Rating

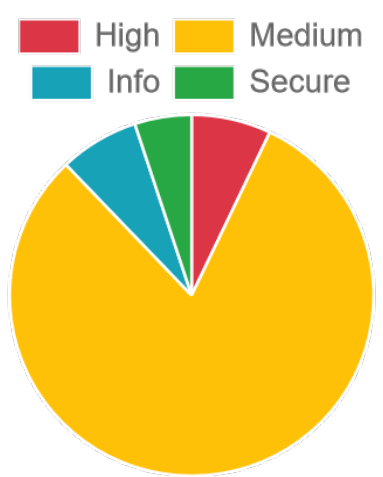


Medium Risk

Grade


A B C F

📊 Severity Distribution (%)








High Medium
Info Secure

👤 Privacy Risk



3

User/Device Trackers

Findings		
	High 3	
	Medium 32	
	Info 3	
	Secure 2	
	Hotspot 3	
<div><div>high</div>The file or SharedPreferences is World Writable. Any App can write to the file</div>		CODE
<div><div>high</div>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</div>		CODE
<div><div>high</div>Firebase DB is exposed publicly.</div>		FIREBASE
<div><div>medium</div>App can be installed on a vulnerable Android version</div>		MANIFEST
<div><div>medium</div>Activity (org.findmykids.app.presentation.screens.home.ChildHomeActivity) is not Protected.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (org.findmykids.app.presentation.receivers.RingModeBroadcastReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>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.</div>		MANIFEST
<div><div>medium</div>Service (org.findmykids.callscreening.child.ChildCallScreeningService) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (org.findmykids.callscreening.child.missedCalls.presentation.PhoneStateReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>Service (org.findmykids.pushes.google.FcmListenerService) is not Protected.</div>		MANIFEST
<div><div>medium</div>Service (pro.userx.server.job.ApiJobService) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Service (org.findmykids.logSend.presentation.services.LogSendJobService) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.SleepEventReceiver) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST

medium	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.BootReceiver) 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.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	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 (com.google.firebase.iid.FirebaseInstanceIdReceiver) 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	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 creates temp file. Sensitive information should never be written into a temp file.	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	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	Application contains Privacy Trackers	TRACKERS

<div><div>medium</div>This app may contain hardcoded secrets</div>		SECRETS
<div><div>info</div>The App logs information. Sensitive information should never be logged.</div>		CODE
<div><div>info</div>App can write to App Directory. Sensitive Information should be encrypted.</div>		CODE
<div><div>info</div>This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.</div>		CODE
<div><div>secure</div>This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</div>		CODE
<div><div>secure</div>This App may have root detection capabilities.</div>		CODE
<div><div>hotspot</div>Found 12 critical permission(s)</div>		PERMISSIONS
<div><div>hotspot</div>Found 1 certificate/key file(s)</div>		FILES
<div><div>hotspot</div>App may communicate to a server (www.baidu.com) in OFAC sanctioned country (Hong Kong)</div>		DOMAINS

MobSF Application Security Scorecard generated for

No Icon

 (Pingo 2.7.79-google) 