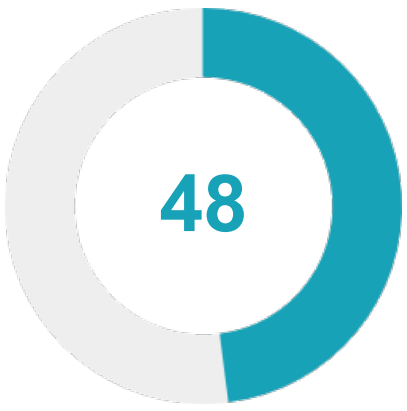
Security Score



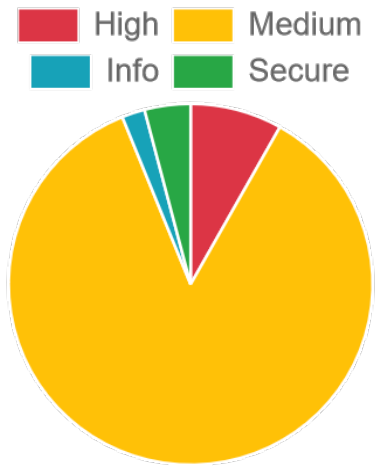
Security Score 48/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

4

User/Device Trackers

Findings

High	Medium	Info
4	38	1

Secure	Hotspot
2	2

high Base config is insecurely configured to permit clear text traffic to all domains	NETWORK
high App can be installed on a vulnerable upatched Android version	MANIFEST
high Clear text traffic is Enabled For App	MANIFEST
high App Link assetlinks.json file not found	MANIFEST
medium Certificate algorithm might be vulnerable to hash collision	CERTIFICATE
medium Activity (com.kiddoware.kidsplace.LockActivity) is not Protected.	MANIFEST
medium Activity (com.kiddoware.kidsplace.LockActivityWithGrownUpMode) is not Protected.	MANIFEST
medium Activity (com.kiddoware.kidsplace.activities.WebViewActivity) is not Protected.	MANIFEST
medium Activity (com.kiddoware.kidsplace.activities.ParseDeepLinkActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (com.kiddoware.kidsplace.admin.KPDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (com.kiddoware.kidsplace.AutoStartKpReceiver) is not Protected.	MANIFEST
medium Service (com.kiddoware.kidsplace.KidsPlaceAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Service (com.kiddoware.kidsplace.activities.RemoteLockIntentService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Activity (com.kiddoware.kidsplace.activities.FirebaseWebViewActivity) is not Protected.	MANIFEST

medium	Service (com.kiddoware.kidsplace.firebase.KPFirebaseMessagingService) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.kiddoware.kidsplace.remotecontrol.mdm.service.LocationReceiver) is not Protected.	MANIFEST
medium	Service (com.kiddoware.kidsplace.remotecontrol.geofence.GeofenceIntentService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.kiddoware.kidsplace.remotecontrol.geofence.GeofenceTransitionsService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.kiddoware.kidsplace.remotecontrol.SynchronizationReceiver) 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	Activity (com.facebook.CustomTabActivity) is not Protected.	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	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	Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected.	MANIFEST
medium	Service (com.evernote.android.job.gcm.PlatformGcmService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	MANIFEST
medium	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected.	MANIFEST
medium	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected.	MANIFEST
medium	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected.	MANIFEST
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	The App uses an insecure Random Number Generator.	CODE

medium	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	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	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	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
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 10 critical permission(s)	PERMISSIONS
hotspot	Found 1 certificate/key file(s)	FILES

MobSF Application Security Scorecard generated for (Kids Place 3.9.40)