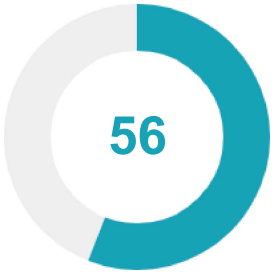
Security Score



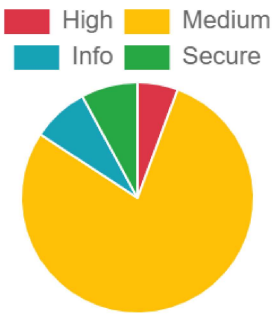
Security Score 56/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
1	12	2	2	1

high Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	MANIFEST
medium Application vulnerable to Janus Vulnerability	CERTIFICATE
medium Application Data can be Backed up	MANIFEST
medium Activity (com.amplifyframework.auth.cognito.activities.HostedUIRedirectActivity) is not Protected.	MANIFEST
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 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 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 App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium SHA-1 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 Application contains Privacy Trackers	TRACKERS
info The App logs information. Sensitive information should never be logged.	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 3 critical permission(s)	PERMISSIONS

MobSF Application Security Scorecard generated for  (ReverseHand 1.0.0)