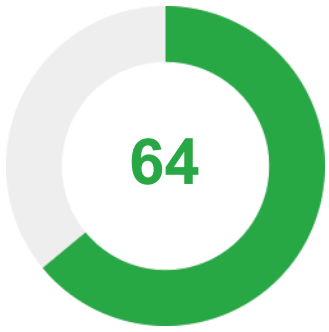
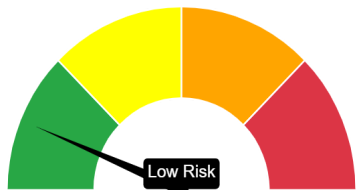
Security Score



Security Score 64/100

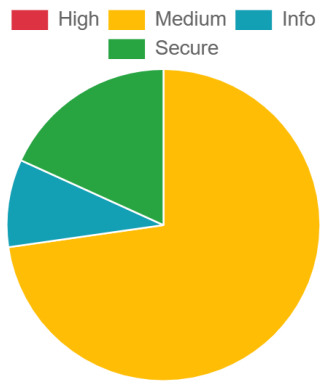
Risk Rating



Grade

A B C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High
0

Medium
8

Info
1

Secure
2

Hotspot
0

medium This App may request root (Super User) privileges.	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 MD5 is a weak hash known to have hash collisions.	CODE
medium The App uses an insecure Random Number Generator.	CODE
medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium App creates temp file. Sensitive information should never be written into a temp file.	CODE
info The App logs information. Sensitive information should never be logged.	CODE
secure This App may have root detection capabilities.	CODE
secure This application has no privacy trackers	TRACKERS

MobSF Application Security Scorecard generated for (No Icon) (ZeroSMS 1.0)

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.