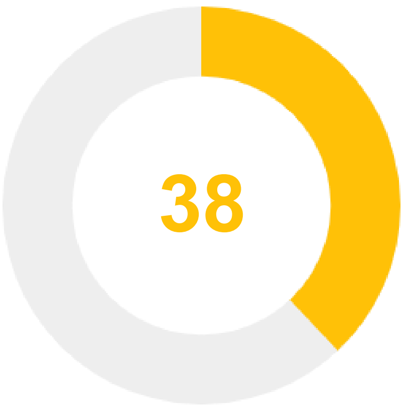
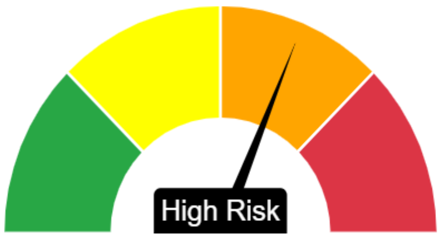
Security Score



Security Score 38/100

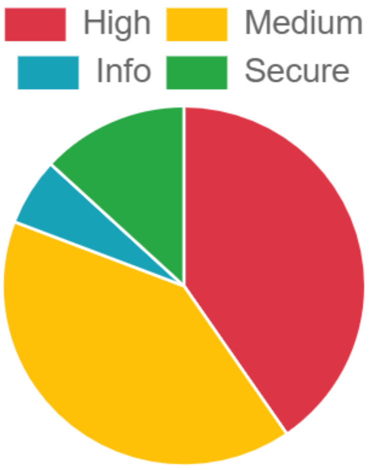
Risk Rating



Grade

A B **C** F

Severity Distribution (%)



Privacy Risk

0

User/Device Trackers

Findings

High **6**	Medium **6**	Info **1**	Secure **2**	Hotspot **1**

high Debug Enabled For App — **MANIFEST**

high Service (.handlers.VulnerableService) is not Protected. — **MANIFEST**

high Broadcast Receiver (.handlers.VulnerableReceiver) is not Protected. — **MANIFEST**

high Content Provider (.handlers.VulnerableContentProvider) is not Protected. — **MANIFEST**

high The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext. — **CODE**

high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. — **CODE**

medium Application Data can be Backed up — **MANIFEST**

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**

medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc. — **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**

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 application has no privacy trackers — **TRACKERS**

hotspot Found 10 critical permission(s) — **PERMISSIONS**

MobSF Application Security Scorecard generated for (PIVAA)

Version v3.5.2 Beta