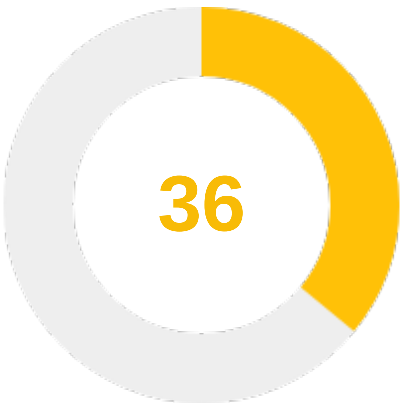
Security Score



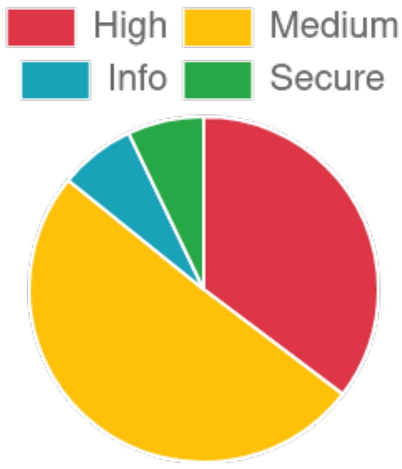
Security Score 36/100

Risk Rating

Grade

A B **C** F

Severity Distribution (%)



Privacy Risk

0

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
5	**7**	**1**	**1**	**1**

high Application vulnerable to Janus Vulnerability **CERTIFICATE**

high Application signed with debug certificate **CERTIFICATE**

high App can be installed on a vulnerable upatched Android version **MANIFEST**

high Debug Enabled For App **MANIFEST**

high Debug configuration enabled. Production builds must not be debuggable. **CODE**

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

medium Activity (jakhar.aseem.diva.APICredsActivity) is not Protected. **MANIFEST**

medium Activity (jakhar.aseem.diva.APICreds2Activity) is not Protected. **MANIFEST**

medium Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected. **MANIFEST**

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 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 application has no privacy trackers **TRACKERS**

hotspot Found 2 critical permission(s) **PERMISSIONS**

MobSF Application Security Scorecard generated for (Diva 1.0)