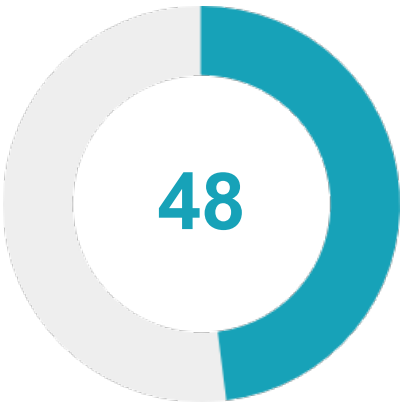


★ Security Score



Security Score 48/100

🚨 Risk Rating

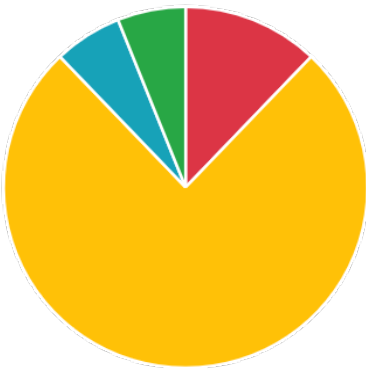


Grade



📊 Severity Distribution (%)

High Medium  
Info Secure



👤 Privacy Risk



User/Device Trackers

📄 Findings



High  
2



Medium  
12



Info  
1



Secure  
1



Hotspot  
1

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

[MANIFEST](#)

**high** Activity (com.rockman.dev.parentctrl.AppMessages) is vulnerable to Android Task Hijacking/StrandHogg.

[MANIFEST](#)

**medium** Application vulnerable to Janus Vulnerability

[CERTIFICATE](#)

**medium** Certificate algorithm might be vulnerable to hash collision

[CERTIFICATE](#)

**medium** Broadcast Receiver (com.rockman.dev.OnBootReceiver) is not Protected.

[MANIFEST](#)

**medium** Broadcast Receiver (com.rockman.dev.AlarmReceiver) is not Protected.

[MANIFEST](#)

**medium** Service (com.rockman.dev.EmptyService) is not Protected.

[MANIFEST](#)

**medium** Broadcast Receiver (com.rockman.dev.parentctrl.DeviceAdminPCReceiver) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

**medium** Broadcast Receiver (com.rockman.dev.SmsReceiver) is not Protected.

[MANIFEST](#)

**medium** Service (com.rockman.dev.parentctrl.services.PCJobService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

**medium** Service (com.rockman.dev.parentctrl.services.SLJobService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

**medium** Service (com.rockman.dev.parentctrl.services.ForegroundService) 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](#)

[CODE](#)

**medium** App can read/write to External Storage. Any App can read data written to External Storage.

**info** The App logs information. Sensitive information should never be logged.


[CODE](#)

**secure** This application has no privacy trackers

[TRACKERS](#)

**hotspot** Found 12 critical permission(s)

[PERMISSIONS](#)

MobSF Application Security Scorecard generated for  ( Parental Time Control 1.5.108) 