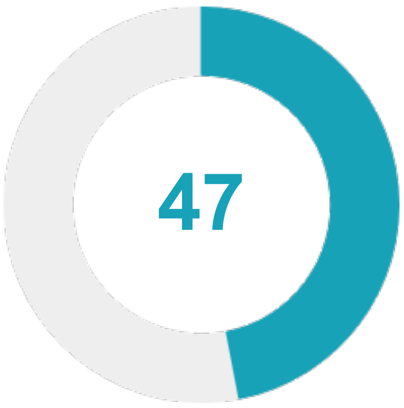
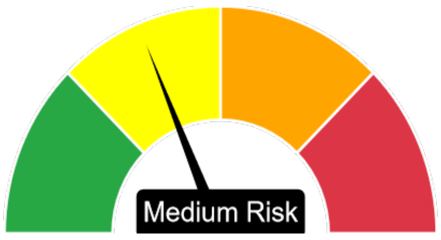
Security Score



Security Score 47/100

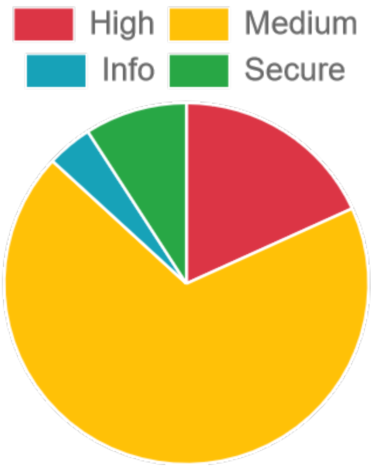
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

0

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
4	**15**	**1**	**2**	**8**

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

high Debug Enabled For App — MANIFEST

high Activity (com.example.variousdata.activity.MainActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

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

medium Application vulnerable to Janus Vulnerability — CERTIFICATE

medium Broadcast Receiver (com.example.variousdata.receiver.BootReceiver) is not Protected. — MANIFEST

medium Service (com.example.variousdata.service.UpdateService) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (com.example.variousdata.receiver.MyDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium The App uses an insecure Random Number Generator. — CODE

medium MD5 is a weak hash known to have hash collisions. — 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 can read/write to External Storage. Any App can read data written to External Storage. **CODE**

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

medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. **CODE**

medium IP Address disclosure **CODE**

medium SHA-1 is a weak hash known to have hash collisions. **CODE**

medium This app may contain hardcoded secrets **SECRETS**

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**

hotspot Found 27 critical permission(s) **PERMISSIONS**

hotspot App may communicate to a server (h.trace.qq.com) in OFAC sanctioned country (Hong Kong) **DOMAINS**

hotspot App may communicate to a server (otheve.beacon.qq.com) in OFAC sanctioned country (Hong Kong) **DOMAINS**

hotspot App may communicate to a server (test.snowflake.qq.com) in OFAC sanctioned country (Hong Kong) **DOMAINS**

hotspot App may communicate to a server (snowflake.qq.com) in OFAC sanctioned country (China) **DOMAINS**

hotspot App may communicate to a server (tun-cos-1258344701.file.myqcloud.com) in OFAC sanctioned country (China) **DOMAINS**

hotspot App may communicate to a server (htrace.wetvinfo.com) in OFAC sanctioned country (China) **DOMAINS**

hotspot App may communicate to a server (othstr.beacon.qq.com) in OFAC sanctioned country (China) **DOMAINS**

MobSF Application Security Scorecard generated for No Icon (Update service 1.3.9)

Version v4.0.6