

★ Security Score

51

Security Score 51/100

🕒 Risk Rating

Medium Risk

Grade

A

B

C

F

📊 Severity Distribution (%)

High

Medium

Info

Secure

👤 Privacy Risk

1

User/Device Trackers

Findings		
<div><div></div><div>High</div><div>1</div></div>	<div><div></div><div>Medium</div><div>11</div></div>	<div><div></div><div>Info</div><div>2</div></div>
<div><div></div><div>Secure</div><div>1</div></div>	<div><div></div><div>Hotspot</div><div>1</div></div>	
<div><div>high</div>The file or SharedPreferences is World Readable. Any App can read from the file</div>		CODE
<div><div>medium</div>App can be installed on a vulnerable Android version</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>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.</div>		CODE
<div><div>medium</div>App creates temp file. Sensitive information should never be written into a temp file.</div>		CODE
<div><div>medium</div>The App uses an insecure Random Number Generator.</div>		CODE
<div><div>medium</div>SHA-1 is a weak hash known to have hash collisions.</div>		CODE
<div><div>medium</div>App can read/write to External Storage. Any App can read data written to External Storage.</div>		CODE
<div><div>medium</div>Application contains Privacy Trackers</div>		TRACKERS
<div><div>medium</div>This app may contain hardcoded secrets</div>		SECRETS
<div><div>info</div>The App logs information. Sensitive information should never be logged.</div>		CODE
		CODE


info App can write to App Directory. Sensitive Information should be encrypted.

secure This App may have root detection capabilities.

[CODE](#)

hotspot Found 15 critical permission(s)

[PERMISSIONS](#)

MobSF Application Security Scorecard generated for  (Security Services 31.0) 