






Findings		
	High 5	
	Medium 22	
	Info 2	
	Secure 0	
	Hotspot 4	
<div><div>high</div>Base config is insecurely configured to permit clear text traffic to all domains</div>		<a href="#">NETWORK</a>
<div><div>high</div>App can be installed on a vulnerable upatched Android version</div>		<a href="#">MANIFEST</a>
<div><div>high</div>Clear text traffic is Enabled For App</div>		<a href="#">MANIFEST</a>
<div><div>high</div>Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is vulnerable to StrandHogg 2.0</div>		<a href="#">MANIFEST</a>
<div><div>high</div>The file or SharedPreferences is World Readable. Any App can read from the file</div>		<a href="#">CODE</a>
<div><div>medium</div>Application vulnerable to Janus Vulnerability</div>		<a href="#">CERTIFICATE</a>
<div><div>medium</div>Activity-Alias (com.app.pro.service) is not Protected.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Activity-Alias (com.app.pro.launcher) is not Protected.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>TaskAffinity is set for activity</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Content Provider (com.app.pro.provider.LocalHtmlProvider) is not Protected.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Broadcast Receiver (com.component.permission.service.ComponentAdminService) is Protected by a permission, but the protection level of the permission should be checked.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Service (com.component.permission.service.ComponentNotificationService) is Protected by a permission, but the protection level of the permission should be checked.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Service (com.component.permission.service.ComponentAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.</div>		<a href="#">MANIFEST</a>
<div><div>medium</div>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection</div>		<a href="#">MANIFEST</a>

level of the permission should be checked.

medium

Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium

Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium

Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium

IP Address disclosure

CODE

medium

The App uses an insecure Random Number Generator.

CODE

medium

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

CODE

medium

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

CODE

medium

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

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 creates temp file. Sensitive information should never be written into a temp file.

CODE

medium

Application contains Privacy Trackers

TRACKERS

medium

This app may contain hardcoded secrets

SECRETS

info

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

CODE

info

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

CODE

hotspot

Found 19 critical permission(s)

PERMISSIONS

hotspot

App may communicate to a server (oss.aliyuncs.com) in OFAC sanctioned country (China)

DOMAINS

hotspot

App may communicate to a server (oss-cn-hangzhou.aliyuncs.com) in OFAC sanctioned country (China)

DOMAINS

hotspot

App may communicate to a server (203.107.1.1) in OFAC sanctioned country (China)

DOMAINS