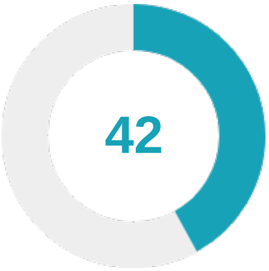
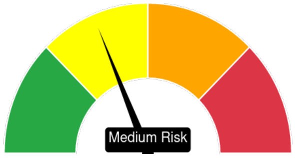
Security Score



Security Score 42/100

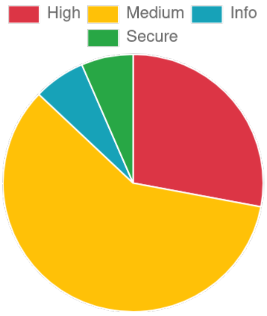
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

10

User/Device Trackers

Findings

High **9**	Medium **19**
Info **3**	Secure **3**
Hotspot **2**	

high Certificate algorithm might be vulnerable to hash collision	**CERTIFICATE**
high Clear text traffic is Enabled For App	**MANIFEST**
high Activity (com.americamovil.claroshop.detalleProducto.zip.DetalleZipActivity) is not Protected.	**MANIFEST**
high Activity (com.americamovil.claroshop.caja.zip.WebViewZipActivity) is not Protected.	**MANIFEST**
high Activity (com.americamovil.claroshop.caja.zip.ZipActivity) is not Protected.	**MANIFEST**
high Activity (com.facebook.CustomTabActivity) is not Protected.	**MANIFEST**
high Activity (com.americamovil.claroshop.login.AuthenticatedActivity) is not Protected.	**MANIFEST**
high Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	**MANIFEST**
high Application contains Privacy Trackers	**TRACKERS**
medium Application Data can be Backed up	**MANIFEST**
medium Activity (com.americamovil.claroshop.buscador.BusquedaResultadosAnteaterActivity) is not Protected.	**MANIFEST**
medium Service (com.americamovil.claroshop.myFunctions.notifications.MyFirebaseMessagingService) is not Protected.	**MANIFEST**
medium Activity (com.braintreepayments.api.BraintreeBrowserSwitchActivity) is not Protected.	**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 Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but	**MANIFEST**

the protection level of the permission should be checked.

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 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 The App uses an insecure Random Number Generator. 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 MD5 is a weak hash known to have hash collisions. CODE

medium IP Address disclosure CODE

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

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

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

medium This App may request root (Super User) privileges. CODE

medium This app may contain hardcoded secrets SECRETS

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

info This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. CODE

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

secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. CODE

secure This App may have root detection capabilities. CODE

secure This App uses SafetyNet API. CODE

hotspot Found 4 critical permission(s) PERMISSIONS

hotspot Found 4 certificate/key file(s) FILES

MobSF Application Security Scorecard generated for (Claro shop 9.7)