ANDROID STATIC ANALYSIS REPORT

COVA (1.2.2)

File Name:	COVA 1.2.2.apk
Package Name:	in.gov.punjab.cova
Average CVSS Score:	6.1
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: COVA 1.2.2.apk
Size: 6.11MB
MD5: 45f4205da0ddd4f3cbca62dd8ecb3f97
SHA1: 6bf69224fff216b52044461ed7325665ffdda5b7
SHA256: 2921f0fcb6bfab20d5669f273708e38d2a98867169a4e65c54a61515ce3f2775

APP INFORMATION

App Name: COVA
Package Name: in.gov.punjab.cova
Main Activity: in.gov.punjab.cova.MainActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: 1.2.2
Android Version Code: 14

APP COMPONENTS

Activities: 18
Services: 12
Receivers: 5
Providers: 4
Exported Activities: 0
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=91, ST=Punjab, L=Mohali, O=Govt Of Punjab, OU=Software Cell, CN=DGR Punjab
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-07 19:24:47+00:00
Valid To: 2045-03-01 19:24:47+00:00
Issuer: C=91, ST=Punjab, L=Mohali, O=Govt Of Punjab, OU=Software Cell, CN=DGR Punjab
Serial Number: 0x356ae99a
Hash Algorithm: sha256
md5: d7aa5c02a05111046f4997ff53bfc09c
sha1: c703ba872aea7f77d0d75c4ef3cbf14478b13a2a
sha256: f07feceffde4ce4f2303a2b3bb0717e1168b335dd1311409c2d1497bbe2c9cf4
sha512:
b65c1dcbfddbac03f03b6ca5a6ade9057757518e930386c168f306e5fb30388252df145c3d87655e7077ce03f724ece9a67babef90075a06d5191db70d8de9c0

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5e9f442e6d27c945603058d86910a9903112b878ec57347ed8b24ca0562ecd8c

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background. If you're requesting this permission, you must also request either
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
android.permission.BLUETOOTH_ADMIN	dangerous	bluetooth administration	Allows an application to configure the local Bluetooth phone and to discover and pair with remote devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Broadcast Receiver (in.gov.punjab.cova.Utils.AutoReadOtp.OtpARBroadcastReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

ISSUE	SEVERITY	DESCRIPTION
Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			in/gov/punjab/cova/Frames/CurfewPassFrame.java in/gov/punjab/cova/Models/Response/RNotification.java in/gov/punjab/cova/Models/Response/ROtpVerification.java in/gov/punjab/cova/Models/Response/RUserCoronaSymptom.java

ISSUE	SEVERITY	STANDARDS	FILES
			in/gov/punjab/cova/Models/Response/RPatients.java in/gov/punjab/cova/Models/Response/RDashboardCountryCitizen.java in/gov/punjab/cova/Models/Response/RSoldItemVendor.java in/gov/punjab/cova/Models/Response/RAuthenticateEmployee.java in/gov/punjab/cova/Models/Response/RDistricts.java in/gov/punjab/cova/Models/Response/RAuthenticateCitizen.java in/gov/punjab/cova/Models/Response/RChangePasswordForgot.java in/gov/punjab/cova/Models/Response/RPurposeCitizen.java in/gov/punjab/cova/Models/Response/RHotspots.java in/gov/punjab/cova/Models/Response/RHospitalList.java in/gov/punjab/cova/Models/Response/RCurfewPassType.java in/gov/punjab/cova/Models/Response/RPatientStats.java in/gov/punjab/cova/Models/Response/RServiceEssential.java in/gov/punjab/cova/Models/Response/RSendOtpForgotPwd.java in/gov/punjab/cova/Models/Response/ROtpAadhar.java in/gov/punjab/cova/Models/Response/RMapStats.java in/gov/punjab/cova/Models/Response/RInstructions.java in/gov/punjab/cova/Models/Response/RCurfewSlots.java in/gov/punjab/cova/Models/Response/RTrackingFlags.java in/gov/punjab/cova/Models/Response/RDashboardStats.java in/gov/punjab/cova/Models/Response/RUserDetail.java in/gov/punjab/cova/Models/Response/RRegisterCitizen.java in/gov/punjab/cova/Models/Response/RAppVersion.java in/gov/punjab/cova/Models/Response/RGeneratedPasses.java in/gov/punjab/cova/Models/Response/RPatientMapStats.java in/gov/punjab/cova/Models/Requests/MReportMassGathering.java in/gov/punjab/cova/Models/Requests/MBLEInsertData.java in/gov/punjab/cova/Models/Requests/MNewPasswordForgot.java in/gov/punjab/cova/Models/Requests/MHospitals.java in/gov/punjab/cova/Models/Requests/MDistricts.java in/gov/punjab/cova/Models/Requests/MAuthenticateOtpAadhar.java in/gov/punjab/cova/Models/Requests/MOtpVerify.java in/gov/punjab/cova/Models/Requests/MAppVersion.java

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	ts/MAppVersion.java in/gov/punjab/cova/Models/Requests/MTrackLocation.java in/gov/punjab/cova/Models/Requests/MCurfewPass.java in/gov/punjab/cova/Models/Requests/MNearestCovid.java in/gov/punjab/cova/Models/Requests/MPatientDistrict.java in/gov/punjab/cova/Models/Requests/MReportHomeQuarantined.java in/gov/punjab/cova/Models/Requests/MDBTrackingData.java in/gov/punjab/cova/Models/Requests/MFormHomeQuarantine.java in/gov/punjab/cova/Models/Requests/MTrackSyncDataHourly.java in/gov/punjab/cova/Models/Requests/MFeedback.java in/gov/punjab/cova/Models/Requests/MCheckoutCorona.java in/gov/punjab/cova/Models/Requests/MRegisterCitizen.java in/gov/punjab/cova/Models/Requests/MResendOtp.java in/gov/punjab/cova/Models/Requests/MAppVersionUpdate.java in/gov/punjab/cova/Models/Requests/MHourlySyncMaster.java in/gov/punjab/cova/Models/Requests/MSendOtpForgotPwd.java in/gov/punjab/cova/Models/Requests/MSendAadharOtp.java in/gov/punjab/cova/Models/Requests/MAuthenticateCitizen.java i/g0.java i/v.java i/f.java i/h0.java i/r.java i/k.java i/a.java i/t.java i/j0/h/c.java i/j0/j/a.java i/j0/l/b.java i/j0/l/a.java a/a/a/a/a/a/c.java h/d.java defpackage/b.java d/n/a.java d/g/f/b/a.java d/g/m/x.java d/g/m/y/b.java d/g/l/b.java d/s/s.java d/s/i0.java d/c/a/b/b.java d/e/c.java d/e/h.java d/e/g.java d/b/p/m0.java d/k/a/p.java e/f/a/m/b/b.java e/f/a/m/b/c.java e/d/a/u/b.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/d/a/u/i.java e/d/a/u/j.java e/d/a/t/b.java e/d/a/s/h.java e/d/a/o/h.java e/d/a/o/g.java e/d/a/o/n/o.java e/d/a/o/n/e.java e/d/a/o/n/y.java e/d/a/o/n/m.java e/d/a/o/n/c0/i.java e/d/a/o/n/c0/m.java e/d/a/o/o/j.java e/d/a/o/o/g.java e/d/a/o/o/m.java e/d/a/o/p/g/f.java e/d/a/o/p/c/o.java e/d/a/o/p/c/q.java e/d/a/o/p/c/i.java e/d/a/o/p/c/j.java e/d/a/o/p/c/r.java e/d/a/o/p/c/y.java e/e/a/a/b.java e/e/a/a/a.java e/e/a/a/i/b/h.java e/e/a/a/i/b/d.java e/e/a/a/i/b/e.java e/e/a/a/i/b/j.java e/e/a/a/i/b/f.java e/e/a/a/i/b/g.java e/e/a/a/j/b.java e/e/a/a/j/e.java e/e/a/a/j/a.java e/e/a/a/j/q/i/b.java e/e/a/a/j/q/h/c.java e/e/a/a/j/q/h/d.java e/e/a/a/j/p/b.java e/e/a/a/j/p/a.java e/e/a/c/l/h.java e/e/a/c/l/g.java e/e/a/b/g/h/d0.java e/e/a/b/g/h/u.java e/e/a/b/g/j/l5.java e/e/a/b/g/j/p2.java e/e/a/b/g/j/p3.java e/e/a/b/g/j/c6.java e/e/a/b/g/j/k5.java e/e/a/b/g/j/k6.java e/e/a/b/g/j/d2.java e/e/a/b/g/j/z5.java e/e/a/b/g/j/c5.java e/e/a/b/j/a/q9.java e/e/a/b/j/a/t9.java e/e/a/b/d/m/m/k.java e/e/a/b/b/a/e/b/b.java e/e/c/n.java e/e/c/f.java e/e/c/k.java e/e/c/l.java e/e/c/u/q.java e/e/c/u/p.java e/e/c/u/g.java e/e/c/u/a.java e/e/c/v/a.java e/e/b/c.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/e/b/r/a.java e/e/b/g/q.java e/e/b/g/r.java e/e/b/f/a/b.java e/e/b/o/a.java e/e/b/o/o/a.java e/e/b/o/p/b.java e/e/b/o/p/a.java e/e/b/m/f0.java e/e/b/m/u0.java e/e/b/q/c.java
			in/gov/punjab/cova/Utils/GPS/CustomLocationProvider.java d/i/b/e.java d/g/i/c.java d/g/g/b.java d/g/g/c.java d/g/g/d.java d/g/g/e.java d/g/g/i.java d/g/g/f.java d/g/g/j/d.java d/g/f/a.java d/g/m/b.java d/g/m/p.java d/g/m/s.java d/g/m/g.java d/g/m/a.java d/g/e/b.java d/g/e/n.java d/g/l/a.java d/t/a/a/h.java d/s/f0.java d/o/b/d.java d/m/a/a.java d/j/a/a.java d/b/o/f.java d/b/o/i/d.java d/b/o/i/g.java d/b/k/a0.java d/b/k/p.java d/b/k/x.java d/b/l/a/a.java d/b/p/z0.java d/b/p/c1.java d/b/p/v.java d/b/p/y0.java d/b/p/j0.java d/b/p/q0.java d/b/p/l0.java d/b/p/y.java d/b/p/m0.java d/k/a/e.java d/k/a/k.java com/yalantis/ucrop/UCropActivity.java com/iceteck/silicompressorr/FileUtils.java com/iceteck/silicompressorr/SiliCompressor.java com/iceteck/silicompressorr/videocompression/MediaController.java com/github/ybq/android/spinkit/ani

ISSUE	SEVERITY	STANDARDS	FILES
			mation/SpriteAnimatorBuilder.java com/github/dhaval2404/imagepicker/ImagePickerActivity.java com/github/dhaval2404/imagepicker/provider/CropProvider.java com/nabinbhandari/android/permissions/Permissions.java e/a/a/a/a.java e/h/a/r/b.java e/h/a/q/b.java e/h/a/p/b.java e/h/a/p/a.java e/d/a/b.java e/d/a/k.java e/d/a/u/k/a.java e/d/a/n/d.java e/d/a/n/e.java e/d/a/s/h.java e/d/a/s/j/i.java e/d/a/o/n/b0.java e/d/a/o/n/i.java e/d/a/o/n/j.java e/d/a/o/n/r.java e/d/a/o/n/l.java e/d/a/o/n/d0/e.java e/d/a/o/n/d0/j.java e/d/a/o/n/c0/i.java e/d/a/o/n/c0/j.java e/d/a/o/n/e0/a.java e/d/a/o/o/c.java e/d/a/o/o/d.java e/d/a/o/o/s.java e/d/a/o/o/f.java e/d/a/o/o/t.java e/d/a/o/m/b.java e/d/a/o/m/j.java e/d/a/o/m/l.java e/d/a/o/m/o/b.java e/d/a/o/m/o/d.java e/d/a/o/p/a.java e/d/a/o/p/g/d.java e/d/a/o/p/g/j.java e/d/a/o/p/g/a.java e/d/a/o/p/c/a0.java e/d/a/o/p/c/c0.java e/d/a/o/p/c/n.java e/d/a/o/p/c/c.java e/d/a/o/p/c/r.java e/d/a/o/p/c/k.java e/d/a/o/p/c/m.java e/d/a/p/o.java e/d/a/p/e.java e/d/a/p/f.java e/d/a/p/k.java e/d/a/p/l.java e/e/a/a/i/c.java e/e/a/a/j/q/h/m.java e/e/a/a/j/p/i.java e/e/a/c/c0/b.java e/e/a/c/b0/b.java e/e/a/c/l/g.java e/e/a/b/i/h/o.java e/e/a/b/g/g/i.java e/e/a/b/g/h/r.java e/e/a/b/g/j/b.java
The App logs information. Sensitive information should	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information	

ISSUE	SEVERITY	STANDARDS	FILES
Sensitive information should never be logged.	Info	into Log File OWASP Mobile Top 10 2016-M2-Insecure Data Storage MASVS-STORAGE-3	e/e/a/b/g/j/i2.java e/e/a/b/g/j/e1.java e/e/a/b/g/j/o.java e/e/a/b/g/j/d1.java e/e/a/b/g/j/tc.java e/e/a/b/g/j/r5.java e/e/a/b/g/j/m8.java e/e/a/b/g/j/u1.java e/e/a/b/g/j/l1.java e/e/a/b/g/j/s1.java e/e/a/b/g/j/t1.java e/e/a/b/g/j/o1.java e/e/a/b/g/j/p1.java e/e/a/b/g/j/r1.java e/e/a/b/a/a/b.java e/e/a/b/a/a/a.java e/e/a/b/j/a/o4.java e/e/a/b/d/w.java e/e/a/b/d/c0.java e/e/a/b/d/v.java e/e/a/b/d/e.java e/e/a/b/d/i.java e/e/a/b/d/j.java e/e/a/b/d/r/c.java e/e/a/b/d/r/h.java e/e/a/b/d/n/b.java e/e/a/b/d/n/n.java e/e/a/b/d/n/q.java e/e/a/b/d/n/e.java e/e/a/b/d/n/i.java e/e/a/b/d/n/j.java e/e/a/b/d/n/f.java e/e/a/b/d/n/l0.java e/e/a/b/d/n/k.java e/e/a/b/d/n/u0.java e/e/a/b/d/n/a.java e/e/a/b/d/s/a.java e/e/a/b/d/o/a.java e/e/a/b/d/m/m/r2.java e/e/a/b/d/m/m/z0.java e/e/a/b/d/m/m/c0.java e/e/a/b/d/m/m/k2.java e/e/a/b/d/m/m/s.java e/e/a/b/d/m/m/h1.java e/e/a/b/d/m/m/g.java e/e/a/b/d/m/m/q1.java e/e/a/b/d/m/m/r0.java e/e/a/b/d/m/m/v1.java e/e/a/b/d/m/m/k0.java e/e/a/b/d/q/c.java e/e/a/b/d/q/a.java e/e/a/b/e/g.java e/e/a/b/b/a/e/b/e.java e/e/a/b/k/b/a.java e/e/a/b/l/a.java e/e/b/c.java e/e/b/g/g.java e/e/b/o/o/b.java e/e/b/o/p/c.java e/e/b/h/d/w.java e/e/b/h/d/z.java e/e/b/h/d/i.java e/e/b/h/d/s.java e/e/b/h/d/y.java e/e/b/h/d/x.java

ISSUE	SEVERITY	STANDARDS	FILES
			e/e/b/h/e/b.java e/e/b/h/e/h.java e/e/b/h/e/e.java e/e/b/h/e/g.java e/e/b/h/e/n/d.java e/e/b/h/e/o/b.java e/e/b/h/e/o/a.java e/e/b/h/e/o/c/b.java e/e/b/h/e/o/c/d.java e/e/b/h/e/o/d/c.java e/e/b/h/e/o/d/d.java e/e/b/h/e/j/c.java e/e/b/h/e/j/h.java e/e/b/h/e/j/d.java e/e/b/h/e/j/g.java e/e/b/h/e/k/b.java e/e/b/h/e/k/d.java e/e/b/h/e/p/d.java e/e/b/h/e/p/a.java e/e/b/h/e/p/j/d.java e/e/b/h/e/p/j/a.java e/e/b/m/e1.java e/e/b/m/a0.java e/e/b/m/w.java e/e/b/m/n.java e/e/b/m/z.java e/e/b/m/g0.java e/e/b/m/e0.java e/e/b/m/c.java e/e/b/m/b0.java e/e/b/m/d.java e/e/b/m/p.java e/e/b/m/d0.java e/e/b/m/f0.java e/e/b/m/i.java e/e/b/m/h0.java e/e/b/m/g.java e/e/b/m/l0.java e/e/b/m/u0.java e/e/b/m/n0.java e/e/b/m/m.java e/e/b/m/i1.java e/e/b/m/t.java e/e/b/q/o.java e/e/b/q/q.java e/e/b/q/p.java e/e/b/q/e.java e/e/b/q/f.java e/e/b/q/g.java e/e/b/q/r.java e/b/a.java k/a/a/j/c.java k/a/a/j/a.java

ISSUE	SEVERITY	STANDARDS	FILES
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.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	in/gov/punjab/cova/Utils/Tracking/UserBLETracker.java a/a/a/a/f/c/b.java a/a/a/a/f/c/a.java a/a/a/a/f/d/f.java a/a/a/a/f/d/g.java e/e/a/a/j/q/i/n.java e/e/a/a/j/q/i/o.java e/e/a/a/j/q/i/j.java e/e/a/b/j/a/fa.java e/e/a/b/j/a/k4.java e/e/a/b/j/a/d.java e/e/a/b/j/a/t9.java e/e/a/b/j/a/ka.java e/e/a/b/d/s/a.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	in/gov/punjab/cova/Models/Requests/MNewPasswordForgot.java a/a/a/a/a/w0.java e/d/a/o/n/q.java
App creates temp file. Sensitive information should never be written into a temp file.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	d/j/a/a.java com/iceteck/silicompressorr/SiliCompressor.java e/e/b/o/o/c.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/iceteck/silicompressorr/Util.java com/iceteck/silicompressorr/PathUtil.java com/iceteck/silicompressorr/FileUtils.java com/iceteck/silicompressorr/SiliCompressor.java com/github/dhaval2404/imagepicker/util/FileUtil.java com/github/dhaval2404/imagepicker/util/FileUriUtils.java e/f/a/l/o.java e/f/a/l/g.java e/h/a/p/b.java
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	e/e/a/b/g/j/tc.java e/e/a/b/j/a/ca.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	e/e/a/b/g/j/s1.java e/e/b/h/e/j/c.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	e/e/a/b/j/a/ca.java

ISSUE	SEVERITY	STANDARDS	FILES
SHA-1 is a weak hash known to have hash collisions.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	e/e/b/h/e/j/c.java e/e/b/m/e1.java

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
msewa.punjab.gov.in	good	**IP:** 13.71.89.83 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.08784 **Longitude:** 80.278473 **View:** Google Map
api.crashlytics.com	good	**IP:** 54.225.185.12 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
plus.google.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	good	**IP:** 52.64.108.95 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
app-measurement.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
daily-needs.uen.io	good	**IP:** 15.206.6.139 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.01441 **Longitude:** 72.847939 **View:** Google Map
cova.punjab.gov.in	good	**IP:** 52.172.8.28 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.08784 **Longitude:** 80.278473 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
epasscovid19.pais.net.in	good	**IP:** 13.233.221.137 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.01441 **Longitude:** 72.847939 **View:** Google Map
www.google.com	good	**IP:** 216.58.196.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
covidhelp.punjab.gov.in	good	**IP:** 52.172.38.163 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.08784 **Longitude:** 80.278473 **View:** Google Map
www.googleadservices.com	good	**IP:** 216.58.196.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	good	IP: 172.217.167.98 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
goo.gl	good	IP: 216.58.203.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
dronamaps.com	good	IP: 54.206.19.82 Country: Australia Region: New South Wales City: Sydney Latitude: -33.867851 Longitude: 151.207321 View: Google Map
ns.adobe.com	good	No Geolocation information available.
play.google.com	good	IP: 216.58.196.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebase.google.com	good	IP: 216.58.196.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
google.com	good	IP: 216.58.200.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
reports.crashlytics.com	good	**IP:** 23.21.51.38 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
cova-275dc.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
http://covidhelp.punjab.gov.in/web-views/RegisterLabour.aspx	in/gov/punjab/cova/MainActivity.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Instructions/ https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/Get-token-list	in/gov/punjab/cova/Frames/CurfewPassListFrame.java
https://play.google.com/store/apps/details?id=in.gov.punjab.cova https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-patient-stats https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/GetValue https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-track-flag-data https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/update-ios-device https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-user-detail https://epasscovid19.pais.net.in/ http://covidhelp.punjab.gov.in/ https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-globally-stats https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/get-app-version	in/gov/punjab/cova/Frames/DashboardFrameN.java
https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-hq-user-info	in/gov/punjab/cova/Frames/FormHomeQuarantinedFrame.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Passes-Type	in/gov/punjab/cova/Frames/CurfewPassFrame.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-track-flag-data https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-Distance https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/sync-app-data	in/gov/punjab/cova/Utils/Tracking/UserTracker.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-track-flag-data https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-Distance https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-bluetooth-app-data https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/sync-app-data	in/gov/punjab/cova/Utils/Tracking/UserBLETracker.java

URL	FILE
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-app-tracking-data https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-GPS-Detail https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-Distance	in/gov/punjab/cova/Utils/Tracking/MyTracker.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-All-Notification	in/gov/punjab/cova/Activities/NotificationActivity.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-COVA_MASS_Gathering https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities	in/gov/punjab/cova/Activities/MassGatheringActivity.java
https://play.google.com/store/apps/details?id=	a/a/a/a/a/w.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/Post-feedback	a/a/a/a/a/z.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/verify-and-resend-otp	a/a/a/a/a/c.java
https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-COVA-Symptoms-list	a/a/a/a/a/h.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-COVA-Symptoms	a/a/a/a/a/d0.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/resend-otp https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/validate-otp	a/a/a/a/a/e.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-hq-user-info	a/a/a/a/a/f0.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/register-citizen	a/a/a/a/a/i.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/insert-COVA-Symptoms https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-COVA-Symptoms-list https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-track-flag-data	a/a/a/a/a/f.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/register-citizen https://play.google.com/store/apps/details?id=in.gov.punjab.cova https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/get-app-version	a/a/a/a/a/g.java
https://dronamaps.com/m.punjabcorona.html http://cova.punjab.gov.in/appforeigntravellers https://daily-needs.uen.io https://epasscovid19.pais.net.in/ http://covidhelp.punjab.gov.in/web-views/RegisterLabour.aspx?authkey= http://cova.punjab.gov.in/covaanalytics http://covidhelp.punjab.gov.in/ https://msewa.punjab.gov.in/m-sewa	a/a/a/a/a/w0.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-hospital-list	a/a/a/a/a/k.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-hospital-list	a/a/a/a/a/v0.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-hot-spot-areas	a/a/a/a/a/t.java
https://msewa.punjab.gov.in/m-sewa/api/cova/employee/auth/v1/authenticate-employee	a/a/a/a/a/a/b.java

URL	FILE
https://play.google.com/store/apps/details?id=in.gov.punjab.cova https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/auth/v1/get-app-version	a/a/a/a/a/a/a/c.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-punjab-district-wise-data	a/a/a/a/a/a/a/g.java
https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-patient-data	a/a/a/a/a/a/a/a.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/Genrate_Token https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Slot-ByPasses-Type/1 https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-user-detail https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Token-Purpose-list	a/a/a/a/a/d/b.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/Genrate_Token https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Slot-ByPasses-Type/3 https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-user-detail https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Services-Type	a/a/a/a/a/d/c.java
https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/Genrate_Token https://msewa.punjab.gov.in/m-sewa/api/common/v1/populate-entities https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Slot-ByPasses-Type/2 https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-user-detail https://msewa.punjab.gov.in/m-sewa/api/cova/citizen/services/v1/get-Sold-Item	a/a/a/a/a/d/a.java
http://ns.adobe.com/xap/1.0/	d/j/a/a.java
http://schemas.android.com/apk/res/android	d/b/k/x.java
https://github.com/florent37/InlineActivityResult	com/github/dhaval2404/imagepicker/ImagePicker.java
data:image	e/d/a/o/o/e.java
https://goo.gl/J1sWQy	e/e/a/b/g/j/tc.java
https://app-measurement.com/a	e/e/a/b/g/j/r7.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	e/e/a/b/a/a/b.java
https://firebase.google.com/support/guides/disable-analytics	e/e/a/b/j/a/h4.java
www.google.com https://www.google.com https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s https://goo.gl/NAOOOI. https://goo.gl/NAOOOI	e/e/a/b/j/a/ca.java
https://app-measurement.com/a	e/e/a/b/j/a/p.java
https://google.com/search?	e/e/a/b/j/a/p7.java

URL	FILE
https://plus.google.com/	e/e/a/b/d/n/m0.java
https://%s/%s/%s?key=%s	e/e/b/o/p/c.java
https://api.crashlytics.com/spi/v1/platforms/android/apps https://api.crashlytics.com/spi/v1/platforms/android/apps/%s https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps	e/e/b/h/e/p/h.java
https://cova-275dc.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://cova-275dc.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	e/e/a/b/d/d0.java

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: COVA Punjab

Score: 4.287287 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Health & Fitness **Play Store URL:** in.gov.punjab.cova

Developer Details: Government of Punjab, Government+of+Punjab, None, None, cova.support@punjab.gov.in,

Release Date: Mar 7, 2020 **Privacy Policy:** Privacy link

Description:

COVA Punjab (Corona Virus Alert) App has been developed by Government of Punjab to provide citizens with preventive care information and other government advisories. The app has following main sections for citizens: 1. Real time dashboard for Punjab, India and global stats 2. To check for

symptoms of Corona and have a quick self-screening 3. Corona Awareness 4. Traveling instructions 5. Prevention Products 6. Corona Hospitals, Punjab 7. FAQ 8. Call Support You will receive updates from government, advisories and instructions from time to time via PUSH notification on the App. This App will provide quick information and help to you. You should definitely visit nearest hospital / doctor in-case you develop novel corona virus symptoms.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.