MOBSF

ANDROID STATIC ANALYSIS REPORT

My Molina (5.9.9)

File Name:	com.molina.mobile.myhealthinhand_3279.apk
Package Name:	com.molina.mobile.myhealthinhand
Scan Date:	Aug. 31, 2025, 7:01 a.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
12	27	4	2	2

FILE INFORMATION

File Name: com.molina.mobile.myhealthinhand_3279.apk
Size: 34.55MB
MD5: 016479314ef38012b268f839d274b8b1
SHA1: 881e52854ca4eb5b2bd7485106af7765b5f7ddf7
SHA256: 94a40cfd4bef7349e24d589912d1012100e8ba6bf68353b2705da9cdc8dc4448

APP INFORMATION

App Name: My Molina
Package Name: com.molina.mobile.myhealthinhand
Main Activity: com.molina.mobile.myhealthinhand.ui.launch.LaunchScreenActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 5.9.9
Android Version Code: 3279

APP COMPONENTS

Activities: 183
Services: 21
Receivers: 15
Providers: 7
Exported Activities: 8
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Long Beach, O=Molina Healthcare Inc., OU=MHI IT HSS, CN=Emerging Technology Group
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-10-19 19:04:19+00:00
Valid To: 2035-10-14 19:04:19+00:00
Issuer: C=US, ST=California, L=Long Beach, O=Molina Healthcare Inc., OU=MHI IT HSS, CN=Emerging Technology Group
Serial Number: 0x5c293085
Hash Algorithm: sha256
md5: c193f7d8a52c656f9c1e33fed90b7812
sha1: 316b168921006514ce5fa5c94fcc9f3a60e87696
sha256: 308a6f1fa344c70cabdfb5c4899dc706704840c6a0785a0dc6a919d5d6c61610
sha512: 7ec12589e44dc0beb21808ac0f105eb06ec374ee86bab75139e0952edd43b7f022ac3c5b95b035aa7a8dc9a669612d903df644bdb949d368785a38daada4ce94
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 27b2d792ecf9b89ac84843dd06fc446aecc2abdaf54cc9c7961a60eef27a3ac6
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.STORAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CALL_PRIVILEGED	SignatureOrSystem	directly call any phone numbers	Allows the application to call any phone number, including emergency numbers, without your intervention. Malicious applications may place unnecessary and illegal calls to emergency services.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.molina.mobile.myhealthinhand.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.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
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.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.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
possible ro.secure check
emulator file check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes7.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.molina.mobile.myhealthinhand.ui.login.sign_in.SignInActivity	Schemes: https://, Hosts: memberstg.molinahealthcare.com, memberu03.molinahealthcare.com, app-eprtsc0-qa-nodepxy.molina.mhc, member.molinahealthcare.com, molinahealthcare.page.link, Paths: /en,
com.molina.mobile.myhealthinhand.ui.loginCIAM.sign_in_ciam.SignInCIAMActivity	Schemes: https://, Hosts: memberstg.molinahealthcare.com, memberu03.molinahealthcare.com, app-eprtsc0-qa-nodepxy.molina.mhc, member.molinahealthcare.com, molinahealthcare.page.link, Paths: /en,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: 2 | WARNING: 1 | INFO: 1 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	info	Base config is configured to trustbundled certs @raw/root_certificate.
3	*	warning	Base config is configured to trust system certificates.
4	func-aichatbot-dev-001.azurewebsites.net api.molinahealthcare.com www.molinahealthcare.com molinahealthcare.com dc10mymolwdw01:482 dc10mymolwdw01.molina.mhc:495	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 8 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.molina.mobile.myhealthinhand.ui.login.ciam_register.CIAM_SMS_BroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.permission.SEND [android:exported=true]	warning	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.
5	Activity (com.molina.mobile.myhealthinhand.ui.login.ciam_register.CiamFlowRegistrationActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.molina.mobile.myhealthinhand.ui.dashboard_screen.home.IDCardActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (com.molina.mobile.myhealthinhand.ui.dashboard_screen.home.IDCardActivityForMP) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
8	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.login.sign_in.SignInActivity] [android:host=https://memberstg.molinahealthcare.com]	high	App Link asset verification URL (https://memberstg.molinahealthcare.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
9	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.login.sign_in.SignInActivity] [android:host=https://member.molinahealthcare.com]	high	App Link asset verification URL (https://member.molinahealthcare.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
10	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.login.sign_in.SignInActivity] [android:host=https://molinahealthcare.page.link]	high	App Link asset verification URL (https://molinahealthcare.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
11	Activity (com.molina.mobile.myhealthinhand.ui.login.sign_in.SignInActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.loginCIAM.sign_in_ciam.SignInCIAMActivity] [android:host=https://memberstg.molinahealthcare.com]	high	App Link asset verification URL (https://memberstg.molinahealthcare.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
13	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.loginCIAM.sign_in_ciam.SignInCIAMActivity] [android:host=https://member.molinahealthcare.com]	high	App Link asset verification URL (https://member.molinahealthcare.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
14	App Link assetlinks.json file not found [android:name=com.molina.mobile.myhealthinhand.ui.loginCIAM.sign_in_ciam.SignInCIAMActivity] [android:host=https://molinahealthcare.page.link]	high	App Link asset verification URL (https://molinahealthcare.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
15	Activity (com.molina.mobile.myhealthinhand.ui.loginCIAM.sign_in_ciam.SignInCIAMActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Activity (com.molina.mobile.myhealthinhand.ui.login.prelogin.PreLoginActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
18	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]	warning	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.
19	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	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]	warning	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.
23	Broadcast Receiver (com.salesforce.marketingcloud.sfmcsdk.SFMCSdkReceiver) is not Protected. [android:exported=true]	warning	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.
24	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	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.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	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

HIGH: **2** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ae/javax/accessibility/AccessibleBundle.java ae/sun/awt/FontConfiguration.java ae/sun/awt/image/PNGImageDecoder.java ae/sun/java2d/Disposer.java ae/sun/java2d/pisces/PiscesTileGenerator.java antlr/DumpASTVisitor.java antlr/build/Tool.java antlr/collections/impl/Vector.java antlr/debug/misc/JTreeASTModel.java backbone/ui/views/AssetVideoView.java backbone/utils/LogExt.java butterknife/ButterKnife.java co/touchlab/squeaky/logger/AndroidLog.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifDecoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifencoder/AnimatedGifEncoder

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/gifencoder/AnimatedGifEncoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/MediaStoreThumbFetcher.java com/bumptech/glide/load/engine/CacheLoader.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/FifoPriorityThreadPoolExecutor.java com/bumptech/glide/load/model/ImageVideoModelLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/ImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/ImageVideoBitmapDecoder.java com/bumptech/glide/load/resource/bitmap/RecyclableBufferedInputStream.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/util/ByteArrayPool.java com/bumptech/glide/util/ContentLengthInputStream.java com/fasterxml/jackson/core/util/VersionUtil.java com/fasterxml/jackson/databind/util/ISO8601Utils.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/molina/mobile/myhealthinhand/application/ApplicationLifeCycleHandler.java com/salesforce/marketingcloud/MCLogListener.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/salesforce/marketingcloud/sfmcsdk/components/encryption/KeyStoreWrapper.java com/salesforce/marketingcloud/sfmcsdk/components/logging/LogListener.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/shockwave/pdfium/PdfiumCore.java com/sun/activation/registries/LogSupport.java com/topologi/diffx/xml/sax/ReporterHandlerProxy.java com/tozny/crypto/android/AesCbcWithIntegrity.java in/co/ophio/secure/core/ObscuredPreferencesBuilder.java java/awt/font/TextJustifier.java java_cup/runtime/lr_parser.java net/engio/mbassy/bus/error/IPublicationErrorHandler.java net/sqlcipher/database/SqliteWrapper.java org/antlr/runtime/SerializedGrammar.java org/docx4j/fonts/fop/apps/FOPException.java org/docx4j/model/fields/NumberExtractor.java org/docx4j/samples/ErrorLineExtractor.java org/docx4j/slf4j/apache/commons/logging/impl/SimpleLog.java org/pptx4j/Box.java org/slf4j/helpers/Util.java
				backbone/result/StepResult.java com/molina/mobile/myhealthinhand/BuildConfig.java com/molina/mobile/myhealthinhand/dagger/api/NetworkConstants.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/AlertRequest.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/CdpAlertCloseEventRequest.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/CdpAlertDismissEventRequest.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/CdpForceCloseResponse.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/CdpIdentifyUserResponse.java com/molina/mobile/myhealthinhand/data/models/d

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ata_models/cdp/CdpPostEventResponse.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/IdentifyUsersRequest.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/molina/mobile/myhealthinhand/data/models/data_models/cdp/PostEventRequest.java com/molina/mobile/myhealthinhand/data/models/data_models/cdp/cdpResultData.java com/molina/mobile/myhealthinhand/data/models/data_models/ciam/CIAMCreateAccount.java com/molina/mobile/myhealthinhand/data/models/data_models/healthsperpa/RenewalNotification.java com/molina/mobile/myhealthinhand/data/models/data_models/login/ResetPasswordRequest.java com/molina/mobile/myhealthinhand/data/models/data_models/pregnancy/AddActivityReq.java com/molina/mobile/myhealthinhand/data/models/data_models/profile/possibleNow/CustomProperty.java com/molina/mobile/myhealthinhand/data/models/data_models/profile/possibleNow/PreferenceAttributes.java com/molina/mobile/myhealthinhand/data/models/data_models/sapphire/CDPBrowserIdResponse.java com/molina/mobile/myhealthinhand/data/models/request_models/AccountCreateRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/CarePlanRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/ChangePasswordRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/LoginRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/NewAccountCreateRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/ZyterRegisterRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/ciam/CIAMChangeEmailValidateRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/ciam/Parameters.java com/molina/mobile/myhealthinhand/data/models/request_models/cvs/CVSAccessTokenRequest.java com/molina/mobile/myhealthinhand/data/models/re

NO	ISSUE	SEVERITY	STANDARDS	FILES
				quest_models/cvs/CVSBearerTokenRequest.java com/molina/mobile/myhealthinhand/data/models/request_models/possibleNow/PreferenceAttributes.java com/molina/mobile/myhealthinhand/data/models/request_models/possibleNow/PreferenceAttributesEmail.java com/molina/mobile/myhealthinhand/engine/Constants.java com/molina/mobile/myhealthinhand/firebase/FirebaseEvent.java com/molina/mobile/myhealthinhand/language/LocaleManager.java com/molina/mobile/myhealthinhand/ui/hra/HealthRiskAssessmentActivityKt.java com/molina/mobile/myhealthinhand/ui/payment/googlepay/Constants.java com/salesforce/marketingcloud/events/Rule.java com/sun/istack/localization/Localizer.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java org/docx4j/slf4j/apache/commons/logging/LogFactory.java
3	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.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	co/touchlab/squeaky/db/SQLiteDatabase.java co/touchlab/squeaky/db/sqlite/SQLiteDatabaseImpl.java com/salesforce/marketingcloud/storage/db/b.java com/salesforce/marketingcloud/storage/db/c.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/salesforce/marketingcloud/util/l.java in/co/ophio/secure/core/ObscuredSharedPreferences.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/thedeanda/lorem/LoremIpsum.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/salesforce/marketingcloud/sfmcsdk/components/encryption/EncryptedSharedPreferences.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/pingidentity/signalssdk/root/b.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/tozny/crypto/android/AesCbcWithIntegrity.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/molina/mobile/myhealthinhand/helpers/cookie/Methods.java
10	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	in/co/ophio/secure/core/ObscuredSharedPreferences.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/docx4j/apache/http/conn/ssl/SSLContextBuilder.java org/docx4j/apache/http/ssl/SSLContextBuilder.java
12	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/github/mikephil/charting/utils/FileUtils.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/fasterxml/jackson/databind/cfg/PackageVersion.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ae/sun/awt/DebugSettings.java ae/sun/awt/FontConfiguration.java backbone/storage/file/SimpleFileAccess.java backbone/utils/FileUtils.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/resource/file/FileToStreamDecoder.java com/fasterxml/aalto/util/URLUtil.java com/molina/mobile/myhealthinhand/ui/dashboard_screen/home/PdfDocumentAdapter.java com/pingidentity/signalssdk/b.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/salesforce/marketingcloud/util/g.java com/tozny/crypto/android/AesCbcWithIntegrity.java in/co/ophio/secure/vault/Utils.java javax/activation/FileDataSource.java javax/xml/datatype/SecuritySupport.java javax/xml/parsers/SecuritySupport.java javax/xml/stream/SecuritySupport.java javax/xml/transform/SecuritySupport.java javax/xml/validation/SecuritySupport.java javax/xml/xpath/SecuritySupport.java org/antlr/runtime/ANTLRFileStream.java org/antlr/runtime/SerializedGrammar.java org/antlr/stringtemplate/PathGroupLoader.java org/codehaus/stax2/io/Stax2FileSource.java org/codehaus/stax2/io/Stax2URLSource.java org/codehaus/stax2/validation/XMLValidationSchemaFactory.java org/docx4j/apache/http/ssl/SSLContextBuilder.java org/docx4j/fonts/fop/fonts/truetype/FontFileReader.java org/docx4j/fonts/fop/fonts/type1/PFBParser.java org/docx4j/samples/ErrorLineExtractor.java org/xml/sax/helpers/SecuritySupport.java
00024	Write file after Base64 decoding	reflection file	com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/tozny/crypto/android/AesCbcWithIntegrity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	ae/sun/awt/shell/DefaultShellFolder.java com/fasterxml/aalto/util/URLUtil.java javax/xml/transform/stream/StreamResult.java javax/xml/transform/stream/StreamSource.java org/docx4j/model/images/FileConversionImageHandler.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/karumi/dexter/listener/SettingsClickListener.java
00036	Get resource file from res/raw directory	reflection	com/karumi/dexter/listener/SettingsClickListener.java
00012	Read data and put it into a buffer stream	file	org/antlr/runtime/SerializedGrammar.java org/docx4j/fonts/fop/fonts/type1/PFBParser.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00112	Get the date of the calendar event	collection calendar	com/molina/mobile/myhealthinhand/utils/HoloDatePicker.java
00091	Retrieve data from broadcast	collection	com/molina/mobile/myhealthinhand/services/GeocodeAddressIntentService.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://health-in-hand-prod.firebaseio.com

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	android.permission.BATTERY_STATS, android.permission.CALL_PHONE, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
molinaky.trizettoconnect.com	ok	**IP:** 20.59.119.27 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.bing.com	ok	**IP:** 23.62.226.49 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
visitponce.com	ok	**IP:** 170.249.236.196 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api-engage-us.sitecorecloud.io	ok	**IP:** 172.64.145.73 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 142.250.178.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
providersearch.molinahealthcare.com	ok	**IP:** 23.62.226.27 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
forms.molinahealthcare.com	ok	**IP:** 23.62.226.51 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
apidev.molinahealthcare.com	ok	**IP:** 23.62.226.26 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
memberapi.molinahealthcare.com	ok	**IP:** 23.62.226.28 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
javax.xml.transform.dom.domsource	ok	No Geolocation information available.
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
login.microsoftonline.com	ok	**IP:** 20.190.151.132 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
purl.org	ok	**IP:** 207.241.225.157 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
relaxng.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.teladoc.com	ok	**IP:** 104.17.31.172 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.211.org	ok	**IP:** 44.220.97.175 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
dc01mcwebdv01.molina.mhc	ok	No Geolocation information available.
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
opendope.org	ok	**IP:** 176.34.103.193 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
stubservice.azurewebsites.net	ok	No Geolocation information available.
javax.xml.transform.stream.streamresult	ok	No Geolocation information available.
apic.molinahealthcare.com	ok	**IP:** 23.53.145.3 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
report.molinahealth.glassboxdigital.io	ok	**IP:** 23.21.192.56 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
javax.xml.transform.dom.domresult	ok	No Geolocation information available.
javax.xml.transform.stream.streamsource	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
duckduckgo.com	ok	**IP:** 52.250.42.157 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.topologi.com	ok	No Geolocation information available.
www.docx4java.org	ok	**IP:** 176.34.103.193 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
m.providersearch.molinahealthcare.com	ok	**IP:** 23.62.226.2 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.zetetic.net	ok	**IP:** 18.238.96.30 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
schemas.openxmlformats.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
211.org	ok	**IP:** 44.220.97.175 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.municipiodejuncos.com	ok	No Geolocation information available.
www.google.com	ok	**IP:** 172.217.20.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
if.magellancompletecare.com	ok	**IP:** 199.59.243.228 **Country:** United States of America **Region:** Florida **City:** Tampa **Latitude:** 27.943518 **Longitude:** -82.510269 **View:** Google Map
www.nemours.org	ok	**IP:** 151.101.3.10 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.healthnet.com	ok	**IP:** 18.238.109.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
member.teladoc.com	ok	**IP:** 104.17.80.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
m.molinahealthcare.com	ok	**IP:** 23.62.226.49 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
api.molinahealthcare.com	ok	**IP:** 23.53.145.3 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
www.fitnesscoach.com	ok	No Geolocation information available.
app-molinachatbot-dev-001.azurewebsites.net	ok	No Geolocation information available.
dc01mcoewebdv02.molina.mhc	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.psgmolinahealthcare.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
es.bewellnm.com	ok	**IP:** 51.77.240.240 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map
search.yahoo.com	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
caguas.gov.pr	ok	**IP:** 192.124.249.111 **Country:** United States of America **Region:** California **City:** Menifee **Latitude:** 33.679798 **Longitude:** -117.189484 **View:** Google Map
wavirtualcare.molinahealthcare.com	ok	No Geolocation information available.
www.hca.wa.gov	ok	**IP:** 23.185.0.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.792030 **Longitude:** -122.406853 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.molinahealthcare.com	ok	**IP:** 23.62.226.44 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
mcfls4lwjt2rbnz0r4j4yppbq9h4.device.marketingcloudapis.com	ok	**IP:** 13.111.67.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
javax.xml.transform.sax.saxresult	ok	No Geolocation information available.
orchestrate-api.pingone.com	ok	**IP:** 18.155.173.9 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
java.sun.com	ok	**IP:** 23.62.226.28 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
qa.zyter.net	ok	**IP:** 23.23.107.56 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
member.molinahealthcare.com	ok	**IP:** 23.62.226.15 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
myhealthconnections.molinahealthcare.com	ok	**IP:** 23.62.226.28 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
health-in-hand-prod.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
molina.trizettoconnect.com	ok	**IP:** 20.59.119.27 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.thaiopensource.com	ok	**IP:** 119.81.18.13 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.bewellnm.com	ok	**IP:** 141.193.213.10 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
96.9.52.227	ok	**IP:** 96.9.52.227 **Country:** United States of America **Region:** Florida **City:** Jacksonville **Latitude:** 30.191099 **Longitude:** -81.493103 **View:** Google Map
molina.zyter.net	ok	**IP:** 54.157.149.149 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
molina.sapphirethreesixtyfive.com	ok	**IP:** 54.81.5.225 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
auth.pingone.com	ok	**IP:** 18.238.96.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
jaxb.dev.java.net	ok	**IP:** 137.254.56.48 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
svn.apache.org	ok	**IP:** 20.232.109.10 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.molinacontact.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ws-i.org	ok	**IP:** 166.78.156.91 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
youtube.com	ok	**IP:** 142.250.178.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
portalappsupport@molinahealthcare.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Salesforce Marketing Cloud		https://reports.exodus-privacy.eu.org/trackers/220

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"FIREBASE_APP_ID" : "1:144881832997:android:75c7b60b54eee786"
"credentials" : "Credentials"
"firebase_database_url" : "https://health-in-hand-prod.firebaseio.com"
"google_api_key" : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"google_crash_reporting_api_key" : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"google_maps_key" : "AIzaSyAERb1yTzwqcdUC2p-VbJ4aLZtcGBK8EEc"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"password" : "Password"
"username" : "Username"
429e8874f8c5b0ae79402cbfd0665244
45b1995bb00a4505e120b02eaae7c271

POSSIBLE SECRETS
d2b3ec81-0772-4f03-b295-c473857bfc35
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
1e47a25b64a91a187f717ef4a242513b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
08b84098-bbc5-463d-b493-722bd03cddcc
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
f27fd16986b5a1ff9515c650591737e1
F6389234-1024-481F-9173-37D9D7F5051F
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a2c169bc9f9c40e6f8bf1796d577683c
PLIvnz6vjrZYdM9hEAVFldjT36tDCWzF2Z
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
283f5881f17ead0856fce093c7d72fe6
a120ab62361c7919f3583cf8f801f34b
aefbd52de3ef3c91f3234648a3725f37
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43

POSSIBLE SECRETS
ccb159cc29e1143a4ca75bc5f0567ada
5334834d2317b42abb09a263394bbef0
c68f70c79cadc9f0df151fdacceda7bc
4dc1faf38d8e03e756445de52d282a16
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
67e138dbcebb5e2ff5c3d493216a101e
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
n73Yc2mUyjotsEoWrGO615Yx3i2eagkW
2226aeb2f8a7aee1cb3fa54c1b9710be8c84820626a91ebc7ffebff02e667efe
cd04ee3d6814aa9ccd13ba8f197d2e61
397c192ba6654e4ad192b7ee399f354f
960e7f95-4ede-4292-ab71-108c81103afb
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2dc38201e2919a6b9ab7dfc8a5b2887c
caf31557c7b46f51916392909837439c

POSSIBLE SECRETS
WrQIpbIdSHLy5m2wAyYgE2q5tlXcc6UN
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
18834fee274ce6f6005c2d3c4aae59fb
b68a41d8-875b-4c52-9c53-7bf274cdcbc2
01360240043788015936020505
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
d73a2bff-d7f3-4c67-97a7-a8ca0085e212
Tepj1pQzO6vCpRyeWOzamNLYZHJ2EK5v
9412b3ad8f1fb364e078b017e28bc77c
c8ceb755f30e66725cc1051d0886c35d
8ee44df70cac9cc836b165fb77eb617d
AIzaSyBKa2GqPXGCNOyPfDgpE7FUXPfJmicGAZM
2186f8f0-3a79-4c16-9225-b13fcef5dc36
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCMNLOuhnqM2Hjr4OM4sSLMpkDOc1mFylknbjVcxPYhYZLfcX+BBn6Vk3ENDZUIgUHKqG4k7DSp7l+GocY2GOTImc4qx7T40pzx+BAjuy1u88m5LBRV33ENEFDpxQ1xwNG95pHZawmkvrxmxXyH3VuinglutYHmIpRiAae+9n37wIDAQAB

POSSIBLE SECRETS
b785d133-750b-4104-80b1-a3884ef03282
eyJleHAiOjE1NjUxMTQyODAsInVzZXJfbmFtZSI6Im1vbGluYXVzZXIiLCJhdXRob3JpdGllcyI6WyJST0xFX0FETUlOIl0sImp0aSI6ImFjYzg1NGZmLTAzZmEtNDc1MS1hYjFhLTY4YzllNDhhZGQyOSIsImNsaWVudF9pZCI6Im1vbGluYV9jbGllbnQiLCJzY29wZSI6WyJyZWFkIiwid3JpdGUiLCJ0cnVzdCJdfQ
235998f9bbd53ff3ba8a9ef6bd6f476a
43077e78-d419-49d3-acec-358a57d2d7c2
f3e660ce558f3e93ceb4d8c641d6c1d4
705e8cbff8085a66d51d18def57707ad
e525edca45ae6111731cbb114223c038
0448641d6709747511a9e3aca9887dcb07205293827095cb1ff69a566eaa74656b5eec805f41f7ff87c17c25f4aa385936b3342581568cc6557802ed9b85872f41
f881715ad9fb75e9ad98ea8685cae8911f1906c15f47a26d437bef5323d2ad4b829011cc7b6677d26b5b065246293327b13b63b60e4aec0126240340b96b9401c923f9baf95d170e9e9eddbdc29958682463773bbe625eb405a94e00f037f27a433e1c3ed8694a5c426217717a4fc06217e8da25778d9c0ed47beac26d8e1bae
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

PLAYSTORE INFORMATION

Title: My Molina

Score: 4.284585 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.molina.mobile.myhealthinhand

Developer Details: Molina Healthcare Inc, Molina+Healthcare+Inc, None, http://www.molinahealthcare.com, MolinaPortalAppsSupport@molinahealthcare.com,

Release Date: Mar 2, 2016 **Privacy Policy:** Privacy link

Description:

Members can sign into the app using their My Molina User ID and Password to access our secure features, including: • User friendly navigation • View health coverage • View your benefits and eligibility • View/download and share ID card • Make premium payments (Marketplace only) • Manage your payment profile • Save favorite doctors • Change PCP • Access to other services When you use the My Molina app, identifiers for your mobile device are collected within Google Firebase to create a unique identifier for each application when downloaded. Please review the below link which provides a disclosure of the use of Google Analytics for Firebase and how that service processes data: www.google.com/policies/privacy/partners/

SCAN LOGS

Timestamp	Event	Error
2025-08-31 07:01:36	Generating Hashes	OK
2025-08-31 07:01:36	Extracting APK	OK
2025-08-31 07:01:36	Unzipping	OK
2025-08-31 07:01:40	Parsing APK with androguard	OK
2025-08-31 07:01:40	Extracting APK features using aapt/aapt2	OK
2025-08-31 07:01:40	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 07:01:44	Parsing AndroidManifest.xml	OK
2025-08-31 07:01:44	Extracting Manifest Data	OK

2025-08-31 07:01:44	Manifest Analysis Started	OK
2025-08-31 07:01:46	Reading Network Security config from network_security_config.xml	OK
2025-08-31 07:01:46	Parsing Network Security config	OK
2025-08-31 07:01:46	Performing Static Analysis on: My Molina (com.molina.mobile.myhealthinhand)	OK
2025-08-31 07:01:48	Fetching Details from Play Store: com.molina.mobile.myhealthinhand	OK
2025-08-31 07:01:49	Checking for Malware Permissions	OK
2025-08-31 07:01:49	Fetching icon path	OK
2025-08-31 07:01:49	Library Binary Analysis Started	OK
2025-08-31 07:01:49	Reading Code Signing Certificate	OK
2025-08-31 07:01:50	Running APKiD 2.1.5	OK
2025-08-31 07:02:00	Detecting Trackers	OK

2025-08-31 07:02:07	Decompiling APK to Java with JADX	OK
2025-08-31 07:28:58	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/016479314ef38012b268f839d274b8b1/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/016479314ef38012b268f839d274b8b1/016479314ef38012b268f839d274b8b1.apk'], 999.9999813511968)
2025-08-31 07:28:58	Converting DEX to Smali	OK
2025-08-31 07:28:58	Code Analysis Started on - java_source	OK
2025-08-31 07:29:02	Android SBOM Analysis Completed	OK
2025-08-31 07:29:15	Android SAST Completed	OK
2025-08-31 07:29:15	Android API Analysis Started	OK
2025-08-31 07:29:23	Android API Analysis Completed	OK
2025-08-31 07:29:24	Android Permission Mapping Started	OK
2025-08-31 07:29:32	Android Permission Mapping Completed	OK
2025-08-31 07:29:32	Android Behaviour Analysis Started	OK

2025-08-31 07:29:43	Android Behaviour Analysis Completed	OK
2025-08-31 07:29:43	Extracting Emails and URLs from Source Code	OK
2025-08-31 07:29:45	Email and URL Extraction Completed	OK
2025-08-31 07:29:45	Extracting String data from APK	OK
2025-08-31 07:29:45	Extracting String data from Code	OK
2025-08-31 07:29:45	Extracting String values and entropies from Code	OK
2025-08-31 07:29:49	Performing Malware check on extracted domains	OK
2025-08-31 07:29:58	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.