ANDROID STATIC ANALYSIS REPORT

APPatient (7.8.0 (5705cb8b0))

File Name:	com.modernizingmedicine.patientportal_7616.apk

Package Name:	com.modernizingmedicine.patientportal
Scan Date:	Aug. 31, 2025, 6:19 a.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	17	3	3	3

FILE INFORMATION

File Name: com.modernizingmedicine.patientportal_7616.apk
Size: 22.41MB
MD5: 13a521df2fd1bee2f19799d32d9766c0
SHA1: 278710941176b4419e97da37d93e42e08b27ed72
SHA256: 17be59b1aa6a304a73f4bb736d823338fc9d956b8693a90d20f54b126fefd901

APP INFORMATION

App Name: APPatient
Package Name: com.modernizingmedicine.patientportal
Main Activity: com.modernizingmedicine.patientportal.features.login.activities.SplashActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 7.8.0 (5705cb8b0)
Android Version Code: 7616

APP COMPONENTS

Activities: 94

Services: 7
Receivers: 5
Providers: 4
Exported Activities: 3
Exported Services: 0
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: ST=FL, L=Boca Raton, O=Modernizing Medicine, CN=Alex Rocha
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-10-06 14:52:28+00:00
Valid To: 2039-09-30 14:52:28+00:00
Issuer: ST=FL, L=Boca Raton, O=Modernizing Medicine, CN=Alex Rocha
Serial Number: 0x51d6a05d
Hash Algorithm: sha256
md5: 6c2737e84da9806696683b4a60387c34
sha1: 220e004e1293c1dc126175e3a4cecef31c817c4a
sha256: 05127c5e1f1ee8c843166dababd39ffb22f12a80d8f5d0e8e7e5e8505a000066
sha512: 0263f5b96d6245b0d91db752df946249a6433b0545697ebc83443654516b1284565f9a55884e03d47c2cd746df0434c52a7013126a6839413cff25638cd9f9f6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9fa3985b5fb4ace6aee628f1da2dd85d806df72d7ea25ff0abaab4d9f2ac1fa6
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION

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_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_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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.modernizingmedicine.patientportal.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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.modernizingmedicine.patientportal.features.login.activities.SplashActivity	Schemes: https://, Hosts: mobileproxy.m-2.md, mobileproxy-qa.m-2.md, mobileproxy.infra.mmicse.com, mobileproxy.qa.infra.mmicse.com, Path Prefixes: /ema/pocket-patient/online-check-in, /ema/pocket-patient/video-streaming, /ema/pocket-patient/login,
com.modernizingmedicine.patientportal.features.login.activities.ResetPasswordDeeplinkActivity	Schemes: https://, Hosts: mobileproxy.m-2.md, mobileproxy-qa.m-2.md, mobileproxy.infra.mmicse.com, mobileproxy.qa.infra.mmicse.com, Path Prefixes: /ema/ForgotPasswordMobile.action,
com.adyen.checkout.dropin.ui.DropInActivity	Schemes: adyencheckout://, Hosts: com.modernizingmedicine.patientportal,
com.adyen.threeds2.internal.ui.activity.ChallengeActivity	Schemes: adyen3ds2://, Hosts: com.modernizingmedicine.patientportal,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	Activity (com.modernizingmedicine.patientportal.features.login.activities.ResetPasswordDeeplinkActivity) 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.
3	Activity (com.adyen.checkout.dropin.ui.DropInActivity) 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
4	Activity (com.adyen.threeds2.internal.ui.activity.ChallengeActivity) 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.
5	Broadcast Receiver (com.adyen.threeds2.internal.AppUpgradeBroadcastReceiver) 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.
6	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.
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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: **3** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b0/d.java be/c.java c4/j.java com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/ConsoleLog.java com/amazonaws/services/chime/sdk/meetings/utils/logger/ConsoleLogger.java com/biba/bibacommon/ProxyConfig.java com/bugsnag/android/b0.java com/bugsnag/android/x0.java com/github/amlcurran/showcaseview/n.java com/hootsuite/nachos/NachoTextView.java com/leansoft/nano/log/ALog.java com/modernizingmedicine/patientportal/EMAApplication.java com/modernizingmedicine/patientportal/HomePortalActivity.java com/modernizingmedicine/patientportal/core/RootManager.java com/modernizingmedicine/patientportal/core/SingleLiveEvent.java com/modernizingmedicine/patientportal/core/activities/p.java com/modernizingmedicine/patientportal/core/adapters/MultiViewHolderAdapter.java com/modernizingmedicine/patientportal/core/adapters/NewRecyclerViewAdapter.java com/modernizingmedicine/patientportal/core/adapters/TwoViewHolderAdapter.java com/modernizingmedicine/patientportal/core/adapters/home/viewholder/HomeToDoListViewHolder.java com/modernizingmedicine/patientportal/core/enums/mail/MessageCategoryColor.java com/modernizingmedicine/patientportal/core/enums/mail/MessageRecipientType.java com/modernizingmedicine/patientportal/core/f.java com/modernizingmedicine/patientportal/core/h.java com/modernizingmedicine/patientportal/core/json/DateTypeDeserializer.java com/modernizingmedicine/patientportal/core/model/

NO	ISSUE	SEVERITY	STANDARDS	FILES
				json/patientportal/MultiselectionRegistryForm.java com/modernizingmedicine/patientportal/core/pdf/fragments/PDFViewerFragment.java com/modernizingmedicine/patientportal/core/push/GcmService.java com/modernizingmedicine/patientportal/core/push/c.java com/modernizingmedicine/patientportal/core/push/d.java com/modernizingmedicine/patientportal/core/utils/TimeUtils.java com/modernizingmedicine/patientportal/core/utils/c.java com/modernizingmedicine/patientportal/core/utils/l.java com/modernizingmedicine/patientportal/core/utils/s.java com/modernizingmedicine/patientportal/core/utils/w.java com/modernizingmedicine/patientportal/features/appointments/upcoming/UpcomingAppointmentDetailActivity.java com/modernizingmedicine/patientportal/features/billing/ui/BillingPaymentActivity.java com/modernizingmedicine/patientportal/features/billing/ui/BillingStatementDetailFragment.java com/modernizingmedicine/patientportal/features/biometric/ui/EnableBiometricActivity.java com/modernizingmedicine/patientportal/features/home/fragments/HomeFragment.java com/modernizingmedicine/patientportal/features/login/activities/LoginActivity.java com/modernizingmedicine/patientportal/features/login/viewmodels/ResetPasswordDeeplinkViewModel.java com/modernizingmedicine/patientportal/features/newprofile/fragments/PatientProfileFragment.java com/modernizingmedicine/patientportal/features/onlinecheckin/activities/OnlineCheckInActivity.java com/modernizingmedicine/patientportal/features/payments/model/PaymentError.java com/modernizingmedicine/patientportal/features/pharmacies/fragments/PharmaciesFragment.java com/modernizingmedicine/patientportal/features/tele

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	health/activities/SignConsentActivity.java com/modernizingmedicine/patientportal/features/telehealth/activities/SignWaiverActivity.java com/modernizingmedicine/patientportal/features/telehealth/fragments/CameraWizardFragment.java com/modernizingmedicine/patientportal/features/telehealth/fragments/PhotosReviewFragment.java com/modernizingmedicine/patientportal/features/visits/presenter/VideoVisitPresenterImp.java com/radaee/pdf/Page.java com/radaee/reader/GLView.java com/radaee/reader/PDFLayoutView.java com/radaee/reader/PDFViewAct.java com/radaee/util/CommonUtil.java com/radaee/util/PDFAESStream.java com/radaee/util/PDFFileStream.java com/radaee/util/PDFHttpStream.java com/radaee/view/GLBlock.java com/tencent/mm/opensdk/channel/MMessageActV2.java com/tencent/mm/opensdk/channel/a/a.java com/tencent/mm/opensdk/diffdev/DiffDevOAuthFactory.java com/tencent/mm/opensdk/diffdev/a/a.java com/tencent/mm/opensdk/diffdev/a/b.java com/tencent/mm/opensdk/diffdev/a/d.java com/tencent/mm/opensdk/diffdev/a/e.java com/tencent/mm/opensdk/diffdev/a/f.java com/tencent/mm/opensdk/modelbiz/AddCardToWXCardPackage.java com/tencent/mm/opensdk/modelbiz/ChooseCardFromWXCardPackage.java com/tencent/mm/opensdk/modelbiz/SubscribeMessage.java com/tencent/mm/opensdk/modelbiz/SubscribeMiniProgramMsg.java com/tencent/mm/opensdk/modelbiz/WXInvoiceAuthInsert.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgram.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgramWithToken.java com/tencent/mm/opensdk/modelbiz/WXNontaxPay.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tencent/mm/opensdk/modelbiz/WXOpenBusinessView.java com/tencent/mm/opensdk/modelbiz/WXPayInsurance.java com/tencent/mm/opensdk/modelbiz/WXPreloadMiniProgram.java com/tencent/mm/opensdk/modelmsg/GetMessageFromWX.java com/tencent/mm/opensdk/modelmsg/LaunchFromWX.java com/tencent/mm/opensdk/modelmsg/SendAuth.java com/tencent/mm/opensdk/modelmsg/SendMessageToWX.java com/tencent/mm/opensdk/modelmsg/WXAppExtendObject.java com/tencent/mm/opensdk/modelmsg/WXDesignerSharedObject.java com/tencent/mm/opensdk/modelmsg/WXDynamicVideoMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiPageSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEnterpriseCardObject.java com/tencent/mm/opensdk/modelmsg/WXFileObject.java com/tencent/mm/opensdk/modelmsg/WXGameVideoFileObject.java com/tencent/mm/opensdk/modelmsg/WXImageObject.java com/tencent/mm/opensdk/modelmsg/WXMediaMessage.java com/tencent/mm/opensdk/modelmsg/WXMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXMusicObject.java com/tencent/mm/opensdk/modelmsg/WXTextObject.java com/tencent/mm/opensdk/modelmsg/WXVideoFileObject.java com/tencent/mm/opensdk/modelmsg/WXVideoObjec

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t.java com/tencent/mm/opensdk/modelmsg/WXWebpageObject.java com/tencent/mm/opensdk/modelpay/PayReq.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java com/tencent/mm/opensdk/openapi/WXAPIFactory.java com/tencent/mm/opensdk/openapi/WXApiImplComm.java com/tencent/mm/opensdk/utils/Log.java com/tencent/mm/opensdk/utils/a.java com/tencent/mm/opensdk/utils/c.java com/tencent/mm/opensdk/utils/d.java com/xodee/client/audio/audioclient/AudioClient.java d6/a.java f3/i.java g4/o.java gd/b.java h3/a.java j4/c.java j5/d.java jf/d.java k5/b.java l0/a.java m4/z.java m5/i.java m8/g.java n7/b.java nh/j.java p/c.java p/l.java p/o.java p9/b.java q4/a.java r3/a.java r3/d.java r3/e.java r3/n.java r3/o.java r3/p.java r5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rf/e.java s0/b.java s3/g.java s3/n.java s3/r.java s4/b.java s4/k.java t/a.java t/c.java t/d.java t/f.java t0/m0.java t3/w.java u3/b0.java u3/q.java u3/t.java u3/x.java u5/g.java u5/n.java uk/co/chrisjenx/calligraphy/ReflectionUtils.java uk/co/chrisjenx/calligraphy/TypefaceUtils.java v1/b.java v4/h.java y3/b.java z/f.java z3/e.java z3/m.java
2	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/radaee/util/PDFHttpStream.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/radaee/util/PDFHttpStream.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bg/a.java cg/b.java ch/e.java dg/a.java eg/a.java fg/a.java gg/b.java hg/b.java jg/j.java wf/b.java zf/a.java
5	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/amazonaws/services/sqs/MessageMD5ChecksumHandler.java com/amazonaws/util/Md5Utils.java com/radaee/util/CommonUtil.java com/tencent/mm/opensdk/utils/b.java
6	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	atd/r0/g.java bh/c.java com/amazonaws/retry/PredefinedRetryPolicies.java vg/c.java vg/d.java
				com/adyen/checkout/adyen3ds2/model/FingerprintToken.java com/adyen/checkout/card/h.java com/adyen/checkout/components/model/payments/request/CardPaymentMethod.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/services/chime/sdk/meetings/internal/video/TURNCredentials.java com/bugsnag/android/e2.java com/bugsnag/android/internal/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/bugsnag/android/t0.java com/bansoft/nano/impl/JsonWriter.java com/modernizingmedicine/patientportal/core/enums/IntervalsForHistory.java com/modernizingmedicine/patientportal/core/model/featureflag/FeatureFlag.java com/modernizingmedicine/patientportal/core/model/json/patientportal/PagingContext.java com/modernizingmedicine/patientportal/core/model/login/DeepLinkLoginData.java com/modernizingmedicine/patientportal/core/model/login/EasyLoginType.java com/modernizingmedicine/patientportal/core/model/login/newlogin/Message.java com/modernizingmedicine/patientportal/core/model/login/newlogin/SystemProperty.java com/modernizingmedicine/patientportal/core/model/onlinecheckin/NewPassword.java com/modernizingmedicine/patientportal/core/model/tasks/Physician.java com/modernizingmedicine/patientportal/core/model/tasks/ToDoTaskVisitMedicalDomain.java com/modernizingmedicine/patientportal/features/biometric/model/LoginCredentials.java com/modernizingmedicine/patientportal/features/chiefcomplaints/model/HPIAnswerOptionValue.java com/modernizingmedicine/patientportal/features/payments/model/EmaPaymentConfiguration.java com/radaee/pdf/Global.java com/tencent/mm/opensdk/constants/ConstantsAPI.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/hootsuite/nachos/NachoTextView.java com/radaee/reader/PDFGLViewAct.java com/radaee/reader/PDFViewAct.java n1/a.java
9	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/bugsnag/android/f0.java d6/a.java n7/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/modernizingmedicine/patientportal/core/print/PrintDialogActivity.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java com/modernizingmedicine/patientportal/core/RootManager.java r5/v.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/radaee/util/PDFAESStream.java n7/b.java p9/b.java
13	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	com/amazonaws/services/chime/sdk/meetings/internal/ingestion/database/SQLiteDatabaseManager.java l3/b0.java l3/f0.java l3/h0.java
14	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	atd/n/a.java com/modernizingmedicine/patientportal/core/pdf/PDFActivity.java com/modernizingmedicine/patientportal/features/ccdadocuments/ViewCCDADocumentActivity.java com/radaee/pdf/Global.java
15	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	qf/c.java qf/d.java qf/i.java qf/j.java
16	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	atd/k0/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	io/fotoapparat/hardware/CameraDevice.java org/amazon/chime/webrtc/Camera1Session.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/modernizingmedicine/patientportal/core/activities/FullScreenImageActivity.java com/modernizingmedicine/patientportal/core/utils/m.java com/modernizingmedicine/patientportal/features/appointments/upcoming/UpcomingAppointmentDetailActivity.java com/modernizingmedicine/patientportal/features/login/activities/LoginActivity.java com/modernizingmedicine/patientportal/features/pastdiagnosis/fragment/PastDiagnosisListFragment.java com/modernizingmedicine/patientportal/features/pharmacies/fragments/PharmaciesFragment.java com/modernizingmedicine/patientportal/features/visits/fragments/VideoVisitFragment.java com/radaee/reader/PDFGLViewAct.java com/radaee/reader/PDFViewAct.java com/tech/freak/wizardpager/ui/ImageFragment.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java t2/e.java u3/f0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/modernizingmedicine/patientportal/core/utils/m.java com/modernizingmedicine/patientportal/features/appointments/upcoming/UpcomingAppointmentDetailActivity.java com/modernizingmedicine/patientportal/features/login/activities/LoginActivity.java com/modernizingmedicine/patientportal/features/pastdiagnosis/fragment/PastDiagnosisListFragment.java com/modernizingmedicine/patientportal/features/pharmacies/fragments/PharmaciesFragment.java com/radaee/reader/PDFGLViewAct.java com/radaee/reader/PDFViewAct.java t2/e.java u3/f0.java
00036	Get resource file from res/raw directory	reflection	com/adyen/checkout/components/analytics/AnalyticEvent.java com/modernizingmedicine/patientportal/core/utils/m.java com/modernizingmedicine/patientportal/features/visits/fragments/VideoVisitFragment.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00096	Connect to a URL and set request method	command network	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java com/radaee/util/PDFHttpStream.java com/tencent/mm/opensdk/diffdev/a/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/amazonaws/auth/PropertiesCredentials.java com/bugsnag/android/b1.java com/bugsnag/android/ndk/NativeBridge.java com/bugsnag/android/p.java com/modernizingmedicine/patientportal/core/adapters/telehealth/viewholder/PhotoGridItemViewHolder.java com/modernizingmedicine/patientportal/core/pdf/fragments/PDFViewerFragment.java com/modernizingmedicine/patientportal/core/utils/h.java com/modernizingmedicine/patientportal/features/billing/ui/BillingStatementDetailFragment.java com/modernizingmedicine/patientportal/features/telehealth/activities/SignConsentActivity.java com/modernizingmedicine/patientportal/features/telehealth/fragments/CameraWizardFragment.java com/modernizingmedicine/patientportal/features/telehealth/fragments/PhotosReviewFragment.java com/modernizingmedicine/patientportal/features/visits/viewmodels/VirtualVisitMessagesViewModel.java com/radaee/util/CommonUtil.java com/radaee/util/PDFHttpStream.java
00089	Connect to a URL and receive input stream from the server	command network	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java com/bugsnag/android/c0.java com/radaee/util/PDFHttpStream.java com/tencent/mm/opensdk/diffdev/a/e.java
00030	Connect to the remote server through the given URL	network	com/radaee/util/PDFHttpStream.java
00094	Connect to a URL and read data from it	command network	com/amazonaws/http/UrlHttpClient.java com/radaee/util/PDFHttpStream.java com/tencent/mm/opensdk/diffdev/a/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	atd/a/a.java com/adyen/checkout/core/api/Connection.java com/amazonaws/http/UrlHttpClient.java com/radaee/util/PDFHttpStream.java com/tencent/mm/opensdk/diffdev/a/e.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	com/shawnlin/numberpicker/NumberPicker.java
00109	Connect to a URL and get the response code	network command	com/amazonaws/http/UrlHttpClient.java com/amazonaws/services/chime/sdk/meetings/internal/utils/HttpUtils$makePostRequest$2.java com/amazonaws/services/chime/sdk/meetings/internal/utils/TURNRequestUtils$doTurnRequest$2.java com/bugsnag/android/c0.java com/tencent/mm/opensdk/diffdev/a/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/modernizingmedicine/patientportal/core/activities/d.java com/modernizingmedicine/patientportal/features/allergies/addallergies/AddAllergyActivity.java com/modernizingmedicine/patientportal/features/ccdadocuments/ViewCCDADocumentActivity.java com/modernizingmedicine/patientportal/features/customclipboard/CustomClipboardActivity.java com/modernizingmedicine/patientportal/features/customclipboard/CustomClipboardSubSectionDetailActivity.java com/modernizingmedicine/patientportal/features/customclipboard/CustomClipboardSubSectionMenuActivity.java com/modernizingmedicine/patientportal/features/familyhistory/addcondition/AddFamilyConditionActivity.java com/modernizingmedicine/patientportal/features/medicalIntake/activities/MedicalIntakeSummaryActivity.java com/modernizingmedicine/patientportal/features/medications/addmedication/AddMedicationActivity.java com/modernizingmedicine/patientportal/features/obgyn/ui/AddPastPregnancyActivity.java com/modernizingmedicine/patientportal/features/obgyn/ui/EditPregnancyActivity.java com/modernizingmedicine/patientportal/features/visits/fragments/VideoVisitFragment.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00056	Modify voice volume	control	org/amazon/chime/webrtc/audio/WebRtcAudioTrack.java org/amazon/chime/webrtc/voiceengine/WebRtcAudioTrack.java
00013	Read file and put it into a stream	file	com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/internal/ReleasableInputStream.java com/amazonaws/internal/ResettableInputStream.java com/amazonaws/regions/RegionUtils.java com/bugsnag/android/RootDetector.java com/bugsnag/android/i1.java com/bugsnag/android/internal/j.java com/bugsnag/android/o2.java com/radaee/pdf/Global.java com/radaee/reader/PDFViewController.java n7/b.java uf/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00102	Set the phone speaker on	command	com/amazonaws/services/chime/sdk/meetings/device/DefaultDeviceController.java com/amazonaws/services/chime/sdk/meetings/internal/audio/DefaultAudioClientController.java
00028	Read file from assets directory	file	com/radaee/util/PDFAssetStream.java
00208	Capture the contents of the device screen	collection screen	org/amazon/chime/webrtc/ScreenCapturerAndroid.java
00130	Get the current WIFI information	wifi collection	atd/w/a.java
00012	Read data and put it into a buffer stream	file	n7/b.java
00162	Create InetSocketAddress object and connecting to it	socket	qf/b.java qf/j.java
00163	Create new Socket and connecting to it	socket	qf/b.java qf/j.java
00014	Read file into a stream and put it into a JSON object	file	com/radaee/reader/PDFViewController.java
00003	Put the compressed bitmap data into JSON object	camera	com/radaee/util/CommonUtil.java
00005	Get absolute path of file and put it to JSON object	file	com/radaee/util/CommonUtil.java
00125	Check if the given file path exist	file	com/modernizingmedicine/patientportal/core/pdf/fragments/PDFViewerFragment.java com/modernizingmedicine/patientportal/features/billing/ui/BillingStatementDetailFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/modernizingmedicine/patientportal/core/pdf/fragments/PDFViewerFragment.java com/modernizingmedicine/patientportal/features/billing/ui/BillingStatementDetailFragment.java
00189	Get the content of a SMS message	sms	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00188	Get the address of a SMS message	sms	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00200	Query data from the contact list	collection contact	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00187	Query a URI and check the result	collection sms calllog calendar	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00201	Query data from the call log	collection calllog	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00115	Get last known location of the device	collection location	atd/m/g.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	j7/b.java
00175	Get notification manager and cancel notifications	notification	com/modernizingmedicine/patientportal/core/SessionExpirationReceiver.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://patient-portal-30bd4.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1028165346701/namespaces/firebase:fetch?key=AIzaSyCVTSx7Bq9H3KBkxYioHyGbhSyTsir62bQ. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.READ_PHONE_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	4/44	android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE

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
open.weixin.qq.com	IP: 203.205.232.110 Country: China Region: Guangdong City: Shenzhen
long.open.weixin.qq.com	IP: 43.163.176.197 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.googleapis.com	ok	**IP:** 142.250.72.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.telehealthinfo.us	ok	**IP:** 104.155.177.55 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.eyefinity.com	ok	**IP:** 35.167.38.195 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
plus.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
www.surveymonkey.com	ok	**IP:** 18.155.173.82 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
checkoutshopper-live-us.adyen.com	ok	**IP:** 185.101.198.192 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **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

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
places.googleapis.com	ok	**IP:** 172.217.12.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
bugsnag.com	ok	**IP:** 18.238.96.92 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
modernizingmedicine.com	ok	**IP:** 18.238.96.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
checkoutshopper-live.adyen.com	ok	**IP:** 147.12.19.68 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
checkoutshopper-live-apse.adyen.com	ok	**IP:** 85.184.228.203 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
zxing.appspot.com	ok	**IP:** 216.58.214.180 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
checkoutshopper-test.adyen.com	ok	**IP:** 62.146.255.2 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
open.weixin.qq.com	ok	**IP:** 203.205.232.110 **Country:** China **Region:** Guangdong **City:** Shenzhen **Latitude:** 22.545540 **Longitude:** 114.068298 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.bugsnag.com	ok	**IP:** 18.155.173.95 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
long.open.weixin.qq.com	ok	**IP:** 43.163.176.197 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
patient-portal-30bd4.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
checkoutshopper-live-au.adyen.com	ok	**IP:** 85.184.231.70 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
checkoutshopper-live-in.adyen.com	ok	**IP:** 147.12.20.133 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	s3/m.java
radaee_com@yahoo.cn	com/radaee/pdf/Global.java
helpdesk@modmed.com	com/modernizingmedicine/patientportal/core/utils/l.java
legalnotices@eyefinity.com legal@modmed.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207

HARDCODED SECRETS

POSSIBLE SECRETS
"edit_username" : "USERNAME"
"firebase_database_url" : "https://patient-portal-30bd4.firebaseio.com"
"google_api_key" : "AIzaSyCVTSx7Bq9H3KBkxYioHyGbhSyTsir62bQ"
"google_crash_reporting_api_key" : "AIzaSyCVTSx7Bq9H3KBkxYioHyGbhSyTsir62bQ"
"login_password" : "Password"
"login_username" : "Username"
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
DB7C2ABF62E35E668076BEAD2088
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
020A601907B8C953CA1481EB10512F78744A3205FD
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79

POSSIBLE SECRETS
51DEF1815DB5ED74FCC34C85D709
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC
1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD
E95E4A5F737059DC60DFC7AD95B3D8139515620F
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
71169be7330b3038edb025f1
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
74D59FF07F6B413D0EA14B344B20A2DB049B50C3

POSSIBLE SECRETS
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
00E8BEE4D3E2260744188BE0E9C723
003088250CA6E7C7FE649CE85820F7
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
FFFFFFFE0000000075A30D1B9038A115
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
5EEEFCA380D02919DC2C6558BB6D8A5D
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

POSSIBLE SECRETS
0217C05610884B63B9C6C7291678F9D341
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
1E589A8595423412134FAA2DBDEC95C8D8675E58
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e74301e170d3131303131393134333933325a170d3431303131313134333933325a3081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e7430819f300d06092a864886f70d010101050003818d0030818902818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d0101050500038181009c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
6C0107475609912222105691 1C77D77E77A777E7E7E77FCB
B99B99B099B323E02709A4D696E6768756151751
9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B
115792089210356248762697446949407573530086143415290314195533631308867097853951
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618

POSSIBLE SECRETS
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
c49d360886e704936a6678e1139d26b7819f7e90
04B8266A46C55657AC734CE38F018F2192
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
71169be7330b3038edb025f1d0f9
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
883423532389192164791648750360308885314476597252960362792450860609699839
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7

POSSIBLE SECRETS
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
RVRJLVlsSUFlamt0ZFVFZUxuMXBMVzVhVUhJcEJIdFBVQ0V6TFJVQEluWnRQUjVQTzJaLU1RcEJiemtyZXpGcVlrSWJORXNRWUJFQkZDSQ
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
2866537B676752636A68F56554E12640276B649EF7526267
FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
1243ae1b4d71613bc9f780a03690e
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50

POSSIBLE SECRETS
91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
D6031998D1B3BBFEBF59CC9BBFF9AEE1
0340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
b3fb3400dec5c4adceb8655d4c94
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
24B7B137C8A14D696E6768756151756FD0DA2E5C
0095E9A9EC9B297BD4BF36E059184F
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
3045AE6FC8422F64ED579528D38120EAE12196D5

POSSIBLE SECRETS
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
10B7B4D696E676875615175137C8A16FD0DA2211
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
9162fbe73984472a0a9d0590
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
07A526C63D3E25A256A007699F5447E32AE456B50E
03F7061798EB99E238FD6F1BF95B48FEEB4854252B

POSSIBLE SECRETS
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A
6b8cf07d4ca75c88957d9d67059037a4
004D696E67687561517512D8F03431FCE63B88F4
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
e8b4011604095303ca3b8099982be09fcb9ae616
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D7598
0307AF69989546103D79329FCC3D74880F33BBE803CB
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
9B9F605F5A858107AB1EC85E6B41C8AA582CA3511EDDFB74F02F3A6598980BB9
962eddcc369cba8ebb260ee6b6a126d9346e38c5
E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
96341f1138933bc2f503fd44

POSSIBLE SECRETS
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
A335926AA319A27A1D00896A6773A4827ACDAC73
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
6127C24C05F38A0AAAF65C0EF02C
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
3045AE6FC8422f64ED579528D38120EAE12196D5
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
c469684435deb378c4b65ca9591e2a5763059a2e

POSSIBLE SECRETS
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
401028774D7777C7B7666D1366EA432071274F89FF01E718
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
4E13CA542744D696E67687561517552F279A8C84
4D696E676875615175985BD3ADBADA21B43A97E2
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32

POSSIBLE SECRETS
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
000E0D4D696E6768756151750CC03A4473D03679
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
00F50B028E4D696E676875615175290472783FB1
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
659EF8BA043916EEDE8911702B22
B4E134D3FB59EB8BAB57274904664D5AF50388BA
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

POSSIBLE SECRETS
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
10C0FB15760860DEF1EEF4D696E676875615175D
103FAEC74D696E67687561517577FC5B191EF30
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
03E5A88919D7CAFCBF415F07C2176573B2
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
D2C0FB15760860DEF1EEF4D696E6768756151754
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
2AA058F73A0E33AB486B0F610410C53A7F132310
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
4099B5A457F9D69F79213D094C4BCD4D4262210B
114ca50f7a8e2f3f657c1108d9d44cfd8

POSSIBLE SECRETS
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
DB7C2ABF62E35E7628DFAC6561C5
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
7d7374168ffe3471b60a857686a19475d3bfa2ff
07A11B09A76B562144418FF3FF8C2570B8
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
1053CDE42C14D696E67687561517533BF3F83345
C49D360886E704936A6678E1139D26B7819F7E90
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
985BD3ADBAD4D696E676875615175A21B43A97E3
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
e4437ed6010e88286f547fa90abfe4c42212
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

POSSIBLE SECRETS
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
072546B5435234A422E0789675F432C89435DE5242
3086d221a7d46bcde86c90e49284eb15
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0108B39E77C4B108BED981ED0E890E117C511CF072
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
b8adf1378a6eb73409fa6c9c637ba7f5
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
9760508f15230bccb292b982a2eb840bf0581cf5
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67
85E25BFE5C86226CDB12016F7553F9D0E693A268

POSSIBLE SECRETS
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
22123dc2395a05caa7423daeccc94760a7d462256bd56916
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
010092537397ECA4F6145799D62B0A19CE06FE26AD
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
E87579C11079F43DD824993C2CEE5ED3
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985

POSSIBLE SECRETS
D09E8800291CB85396CC6717393284AAA0DA64BA
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
E95E4A5F737059DC60DF5991D45029409E60FC09
10E723AB14D696E6768756151756FEBF8FCB49A9
DB7C2ABF62E35E668076BEAD208B
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
36DF0AAFD8B8D7597CA10520D04B
12511cfe811d0f4e6bc688b4d
002757A1114D696E6768756151755316C05E0BD4
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
00689918DBEC7E5A0DD6DFC0AA55C7
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
bb392ec0-8d4d-11e0-a896-0002a5d5c51b

POSSIBLE SECRETS
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
6b8cf07d4ca75c88957d9d670591
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
31a92ee2029fd10d901b113e990710f0d21ac6b6
8d5155894229d5e689ee01e6018a237e2cae64cd
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
e43bb460f0b80cc0c0b075798e948060f8321b7d
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45

POSSIBLE SECRETS
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
3086d221a7d46bcde86c90e49284eb153dab
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
E95E4A5F737059DC60DFC7AD95B3D8139515620C
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1

POSSIBLE SECRETS
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
127971af8721782ecffa3
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864

PLAYSTORE INFORMATION

Title: APPatient

Score: 3.5828066 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.modernizingmedicine.patientportal

Developer Details: ModMed, ModMed, None, http://www.modmed.com, ehr_apps@modmed.com,

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

Description:

Welcome to APPatient™, the end-to-end patient engagement app created for Modernizing Medicine® patients and providers. APPatient™ is a mobile, fully-functional patient engagement app that can help both patients and providers save time. Patients can access telehealth and information, and push notifications can keep them up to date on primary medical concerns. Practices with Premium Patient Connect can take advantage of 24-hour online check-in, expediting intake paperwork. It can also help providers treat patients on the go. APPatient Patient Benefits: - Chat allows you to communicate with your healthcare team. - Request prescription refills from your phone. - Access your medical records on the go. APPatient Provider Benefits: - Allows patients to access their healthcare records directly. - Communicate with patients. - Access patient information stored in EMA® from your phone. - Lab and test results can be accessed by patients. - Use your existing Patient Portal username and password to log in. For log in assistance, please contact your physician’s office.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 06:19:34	Generating Hashes	OK
2025-08-31 06:19:34	Extracting APK	OK
2025-08-31 06:19:34	Unzipping	OK
2025-08-31 06:19:35	Parsing APK with androguard	OK

2025-08-31 06:19:35	Extracting APK features using aapt/aapt2	OK
2025-08-31 06:19:35	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 06:19:37	Parsing AndroidManifest.xml	OK
2025-08-31 06:19:37	Extracting Manifest Data	OK
2025-08-31 06:19:37	Manifest Analysis Started	OK
2025-08-31 06:19:37	Performing Static Analysis on: APPatient (com.modernizingmedicine.patientportal)	OK
2025-08-31 06:19:39	Fetching Details from Play Store: com.modernizingmedicine.patientportal	OK
2025-08-31 06:19:40	Checking for Malware Permissions	OK
2025-08-31 06:19:40	Fetching icon path	OK
2025-08-31 06:19:40	Library Binary Analysis Started	OK
2025-08-31 06:19:40	Reading Code Signing Certificate	OK

2025-08-31 06:19:41	Running APKiD 2.1.5	OK
2025-08-31 06:19:45	Detecting Trackers	OK
2025-08-31 06:19:48	Decompiling APK to Java with JADX	OK
2025-08-31 06:42:17	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/13a521df2fd1bee2f19799d32d9766c0/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/13a521df2fd1bee2f19799d32d9766c0/13a521df2fd1bee2f19799d32d9766c0.apk'], 999.9999807104468)
2025-08-31 06:42:17	Converting DEX to Smali	OK
2025-08-31 06:42:17	Code Analysis Started on - java_source	OK
2025-08-31 06:42:21	Android SBOM Analysis Completed	OK
2025-08-31 06:42:31	Android SAST Completed	OK
2025-08-31 06:42:31	Android API Analysis Started	OK
2025-08-31 06:42:41	Android API Analysis Completed	OK
2025-08-31 06:42:41	Android Permission Mapping Started	OK

2025-08-31 06:42:50	Android Permission Mapping Completed	OK
2025-08-31 06:42:51	Android Behaviour Analysis Started	OK
2025-08-31 06:43:02	Android Behaviour Analysis Completed	OK
2025-08-31 06:43:02	Extracting Emails and URLs from Source Code	OK
2025-08-31 06:43:06	Email and URL Extraction Completed	OK
2025-08-31 06:43:06	Extracting String data from APK	OK
2025-08-31 06:43:06	Extracting String data from Code	OK
2025-08-31 06:43:06	Extracting String values and entropies from Code	OK
2025-08-31 06:43:09	Performing Malware check on extracted domains	OK
2025-08-31 06:43:15	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.