ANDROID STATIC ANALYSIS REPORT

Harvard Health Info (5.9.9.50)

File Name:	genie.apk
Package Name:	com.geniemd.geniemd.harvard
Scan Date:	June 14, 2024, 4:16 a.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
6	20	1	0	2

FILE INFORMATION

File Name: genie.apk
Size: 37.81MB
MD5: dba8656f3c69338a38cf821d34cd25b4
SHA1: 52e80323d65f489707af3bbc76c33c782ac7fc47
SHA256: bf316e6c25fed4dec27e46b11ca1dead1a995deded5fe4d7c35cfcb3393cc96a

APP INFORMATION

App Name: Harvard Health Info
Package Name: com.geniemd.geniemd.harvard
Main Activity: com.geniemd.geniemd.banglalink.OemMain
Target SDK: 19
Min SDK: 14
Max SDK:
Android Version Name: 5.9.9.50

Android Version Code: 559050

APP COMPONENTS

Activities: 196
Services: 3
Receivers: 3
Providers: 0
Exported Activities: 5
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Ramon, O=GenieMD, OU=Engineering, CN=Abdul Warres
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-09-30 18:21:59+00:00
Valid To: 2055-09-20 18:21:59+00:00
Issuer: C=US, ST=California, L=San Ramon, O=GenieMD, OU=Engineering, CN=Abdul Warres
Serial Number: 0x549d4fd1
Hash Algorithm: sha256
md5: 6f800d8e6e7128dc0cc9513eccf136be
sha1: 38d5fc8e196a7c03802851dcfad14dbd69da662c
sha256: c0128aa716fddcc9c7560cc37a55f141f1ffa980b1a6c6c50819a79784b80223
sha512: d028707b52437e899585f7a57c23e0029847fbabe9a9958cbace4f2585c6a4311e17bfc81a1343c8f0981597abaaacf0b51ede148c6602bd1c90c66950e4ea7a
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.geniemd.geniemd.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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_GPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.SET_ALARM	normal	set alarm in alarm clock	Allows the application to set an alarm in an installed alarm clock application. Some alarm clock applications may not implement this feature.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
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.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.geniemd.geniemd.harvard.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
device ID check
subscriber ID check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	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: **2** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0-4.0.2, [minSdk=14]	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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.geniemd.geniemd.activities.loggedoff.LoggedOffGenieActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.geniemd.geniemd.activities.todolist.ToDoListActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (19) of the app to 29 or higher to fix this issue at platform level.
5	Activity (com.geniemd.geniemd.activities.todolist.ToDoListActivity) 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	Broadcast Receiver (com.google.android.gcm.GCMBroadcastReceiver) 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 (com.geniemd.geniemd.services.StartupReceiver) 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.
8	Service (com.geniemd.geniemd.services.CalendarService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity (com.geniemd.geniemd.HarvardOemActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
10	Activity (com.geniemd.geniemd.HarvardHealthInfo) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
11	Activity (com.geniemd.geniemd.OemMainAcitivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

CODE ANALYSIS

HIGH: **3** | WARNING: **9** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				br/com/rubythree/geniemd/api/controllers/UserController.java br/com/rubythree/geniemd/api/main/Main.java br/com/rubythree/geniemd/api/main/UserHandler.java br/com/rubythree/geniemd/api/models/ActionStatus.java br/com/rubythree/geniemd/api/models/Product.java br/com/rubythree/geniemd/api/models/RestfulResource.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				br/com/rubythree/geniemd/api/utils/Benchmark.java br/com/rubythree/geniemd/api/utils/XMLParser.java br/com/rubythree/test/geniemd/api/models/CareCircleRequestTest.java br/com/rubythree/test/geniemd/api/models/DailyReminderScheduleTest.java br/com/rubythree/test/geniemd/api/models/LoopTest.java br/com/rubythree/test/geniemd/api/models/MonthlyReminderScheduleTest.java br/com/rubythree/test/geniemd/api/models/SpecificDateReminderScheduleTest.java com/actionbarsherlock/internal/ActionBarSherlockCompat.java com/actionbarsherlock/internal/nineoldandroids/animation/PropertyValuesHolder.java com/actionbarsherlock/internal/view/menu/MenuItemImpl.java com/actionbarsherlock/internal/widget/ActionBarView.java com/actionbarsherlock/view/MenuInflater.java com/actionbarsherlock/widget/ActivityChooserModel.java com/actionbarsherlock/widget/SearchView.java com/actionbarsherlock/widget/SuggestionsAdapter.java com/bugsense/trace/BugProfiler.java com/bugsense/trace/BugSense.java com/bugsense/trace/BugSenseHandler.java com/bugsense/trace/CrashMechanism.java com/bugsense/trace/CryptoHttpClient.java com/bugsense/trace/DefaultExceptionHandler.java com/bugsense/trace/EventsMechanism.java com/bugsense/trace/PingsMechanism.java com/bugsense/trace/Utils.java com/fima/cardsui/objects/CardStack.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/geniemd/geniemd/GCMIntentService.java com/geniemd/geniemd/SlidePageSupportFragment.java com/geniemd/geniemd/SlidePageSupportFragment4.java com/geniemd/geniemd/activities/RecordVideoActivity.java com/geniemd/geniemd/activities/WebViewActivity.java com/geniemd/geniemd/activities/healthhistory/familyhistory/FamilyHistoryActivity.java com/geniemd/geniemd/activities/healthhistory/medicalsummary/MedicalSummaryActivity.java com/geniemd/geniemd/activities/healthhistory/procedures/AddProceduresActivity.java com/geniemd/geniemd/activities/healthhistory/vitals/AddA1CActivity.java com/geniemd/geniemd/activities/healthhistory/vitals/AddProtimeINRActivity.java com/geniemd/geniemd/activities/healthhistory/vitals/AddTemperatureActivity.java com/geniemd/geniemd/activities/healthhistory/vitals/TemperatureActivity.java com/geniemd/geniemd/activities/healthhistory/vitals/graph/GraphVitalActivity.java com/geniemd/geniemd/activities/loggedoff/LoggedOffGenieActivity.java com/geniemd/geniemd/activities/loopsocial/AddLoopBlogActivity.java com/geniemd/geniemd/activities/loopsocial/AddLoopFriendActivity.java com/geniemd/geniemd/adapters/healthhistory/vitals/BloodGlucoseAdapter.java com/geniemd/geniemd/adapters/healthhistory/vitals/EmotionAdapter.java com/geniemd/geniemd/adapters/notifications/NotificationsAdapter.java com/geniemd/geniemd/banglalink/GCMIntentService.java

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	com/geniemd/geniemd/banglalink/OemMain.java com/geniemd/geniemd/db/reminders/ScheduledSchema.java com/geniemd/geniemd/harvard/GCMIntentService.java com/geniemd/geniemd/ibm/GCMIntentService.java com/geniemd/geniemd/managers/AlarmManagerBroadcastReceiver.java com/geniemd/geniemd/managers/Downloader.java com/geniemd/geniemd/managers/Utility.java com/geniemd/geniemd/recorder/ExtAudioRecorder.java com/geniemd/geniemd/recorder/Recorder.java com/geniemd/geniemd/utils/GPSTracker.java com/geniemd/geniemd/utils/GoogleMapsApi.java com/geniemd/geniemd/utils/MGCameraActivity.java com/geniemd/geniemd/utils/VerticalScrollview.java com/geniemd/geniemd/views/BaseView.java com/geniemd/geniemd/views/findproviders/ProvidersDetailsMapView.java com/geniemd/geniemd/views/healthhistory/vitals/AddTemperatureView.java com/jjoe64/graphview/compatible/ScaleGestureDetector.java com/lowagie/text/FontFactoryImp.java com/lowagie/text/factories/GreekAlphabetFactory.java com/lowagie/text/factories/RomanAlphabetFactory.java com/lowagie/text/factories/RomanNumberFactory.java com/lowagie/text/pdf/BarcodePDF417.java com/lowagie/text/pdf/GlyphList.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/lowagie/text/pdf/PdfCopy.java com/lowagie/text/pdf/PdfLister.java com/lowagie/text/pdf/Type1Font.java com/lowagie/text/pdf/codec/Base64.java com/lowagie/text/pdf/fonts/cmaps/CMapParser.java com/lowagie/text/pdf/hyphenation/HyphenationTree.java com/lowagie/text/pdf/hyphenation/SimplePatternParser.java com/lowagie/text/pdf/hyphenation/TernaryTree.java com/lowagie/text/pdf/parser/PdfContentReaderTool.java com/lowagie/tools/ConcatPdf.java com/lowagie/tools/EncryptPdf.java com/lowagie/tools/HandoutPdf.java com/lowagie/tools/SplitPdf.java com/nineoldandroids/animation/PropertyValuesHolder.java com/testflightapp/acra/CrashReportDialog.java com/testflightapp/acra/CrashReportFinder.java com/testflightapp/acra/ErrorReporter.java com/testflightapp/acra/SendWorker.java com/testflightapp/acra/collector/ConfigurationCollector.java com/testflightapp/acra/collector/CrashReportDataFactory.java com/testflightapp/acra/collector/DeviceFeaturesCollector.java com/testflightapp/acra/collector/DropBoxCollector.java com/testflightapp/acra/collector/DumpSysCollector.java com/testflightapp/acra/collector/LogCatCollector.java com/testflightapp/acra/collector/SettingsCollector.java com/testflightapp/acra/log/AndroidLogDeleg

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/testflightapp/acra/log/AndroidLogDelegate.java com/testflightapp/acra/sender/GoogleFormSender.java com/testflightapp/acra/sender/HttpSender.java com/testflightapp/acra/util/Installation.java com/testflightapp/acra/util/PackageManagerWrapper.java com/testflightapp/acra/util/ReportUtils.java com/testflightapp/acra/util/ToastSender.java com/testflightapp/lib/BundleInfo.java com/testflightapp/lib/DeviceIDs.java com/testflightapp/lib/TestFlightProperties.java com/testflightapp/lib/core/AndroidLogger.java com/testflightapp/lib/core/Logger.java com/testflightapp/lib/core/newapi/SessionJob.java com/tjeannin/apprate/AppRate.java kankan/wheel/widget/adapters/AbstractWheelTextAdapter.java net/hockeyapp/android/Constants.java net/hockeyapp/android/CrashManager.java net/hockeyapp/android/ExceptionHandler.java net/hockeyapp/android/FeedbackActivity.java net/hockeyapp/android/FeedbackManager.java net/hockeyapp/android/PaintActivity.java net/hockeyapp/android/UpdateActivity.java net/hockeyapp/android/UpdateFragment.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/CheckUpdateTaskWithUI.java net/hockeyapp/android/views/PaintView.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/joda/time/tz/ZoneInfoCompiler.java org/kobjects/crypt/Crypt.java org/kobjects/mime/Decoder.java org/kobjects/pim/PimParser.java org/kxml2/io/KXmlParser.java org/msgpack/template/builder/beans/XMLDecoder.java org/xmlpull/v1/XmlPullParserException.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	br/com/rubythree/geniemd/api/models/Reminder.java com/actionbarsherlock/internal/view/menu/MenuBuilder.java com/lowagie/text/pdf/DefaultFontMapper.java com/testflightapp/lib/DeviceIDs.java net/hockeyapp/android/CrashManager.java net/hockeyapp/android/LoginManager.java net/hockeyapp/android/Tracking.java net/hockeyapp/android/utils/VersionCache.java
3	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/bugsense/trace/Utils.java com/geniemd/geniemd/activities/RecordVideoActivity.java com/geniemd/geniemd/activities/loopsocial/AddLoopBlogActivity.java com/geniemd/geniemd/managers/Utility.java com/lowagie/text/pdf/PdfStamper.java com/lowagie/text/pdf/parser/PdfContentReaderTool.java com/testflightapp/lib/DeviceIDs.java net/hockeyapp/android/Constants.java net/hockeyapp/android/tasks/DownloadFileTask.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/lowagie/text/pdf/PdfPKCS7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/lowagie/text/pdf/PdfEncryption.java com/lowagie/text/pdf/PdfPKCS7.java com/lowagie/text/pdf/PdfReader.java com/testflightapp/lib/core/StringUtils.java net/hockeyapp/android/Constants.java
6	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. 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/geniemd/geniemd/activities/WebViewActivity.java com/geniemd/geniemd/activities/conditions/MedlinePlusActivity.java com/geniemd/geniemd/activities/healthhistory/medicalsummary/MedicalSummaryActivity.java
7	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/commonsware/cwac/sacklist/demo/BuildConfig.java
8	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/geniemd/geniemd/activities/PrintDialogActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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/geniemd/geniemd/activities/reminders/SelectTimeActivity.java com/geniemd/geniemd/db/GenieMDDBHelper.java com/geniemd/geniemd/db/reminders/ReminderDBHelper.java com/geniemd/geniemd/db/reminders/ReminderSchema.java com/geniemd/geniemd/db/reminders/Table.java com/testflightapp/lib/core/SqliteObjectPersistor.java
10	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/bugsense/trace/Utils.java com/lowagie/text/ImgJBIG2.java com/lowagie/text/pdf/PdfEncryption.java com/lowagie/text/pdf/PdfSmartCopy.java com/testflightapp/lib/core/SqliteObjectPersistor.java net/hockeyapp/android/LoginActivity.java
11	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/bugsense/trace/CrashMechanism.java com/bugsense/trace/EventsMechanism.java com/bugsense/trace/PingsMechanism.java com/bugsense/trace/Utils.java net/hockeyapp/android/utils/SimpleMultipartEntity.java org/kobjects/crypt/Crypt.java
12	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/geniemd/geniemd/activities/healthhistory/medicalsummary/MedicalSummaryActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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/lowagie/text/pdf/PdfStamper.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/24	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.GET_TASKS, android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CONTACTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO
Other Common Permissions	4/45	android.permission.READ_CALENDAR, android.permission.CALL_PHONE, com.google.android.c2dm.permission.RECEIVE, android.permission.MODIFY_AUDIO_SETTINGS

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
ns.adobe.com	ok	No Geolocation information available.
www.nih.gov	ok	**IP:** 23.64.121.185 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
xml.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

DOMAIN	STATUS	GEOLOCATION
purl.org	ok	**IP:** 207.241.239.241 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
services-qa.walgreens.com	ok	**IP:** 27.77.82.227 **Country:** Viet Nam **Region:** Ha Noi **City:** Hanoi **Latitude:** 21.024500 **Longitude:** 105.841171 **View:** Google Map
www.cdc.gov	ok	**IP:** 104.71.145.31 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
api.goodrx.com	ok	**IP:** 44.241.13.80 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.wireless-village.org	ok	**IP:** 172.67.131.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
alt.bugsense.appspot.com	ok	**IP:** 142.250.207.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.nytimes.com	ok	**IP:** 151.101.77.164 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sites.google.com	ok	**IP:** 142.251.220.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
198.101.196.187	ok	**IP:** 198.101.196.187 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.facebook.com	ok	**IP:** 163.70.158.35 **Country:** France **Region:** Ile-de-France **City:** Nanterre **Latitude:** 48.891979 **Longitude:** 2.206750 **View:** Google Map
www.eishob.com	ok	No Geolocation information available.
ticks2.bugsense.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 172.217.27.36 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.xfa.org	ok	No Geolocation information available.
api.twitter.com	ok	**IP:** 104.244.42.2 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
www.redcross.org	ok	**IP:** 23.215.243.114 **Country:** Australia **Region:** Queensland **City:** Brisbane **Latitude:** -27.467939 **Longitude:** 153.028091 **View:** Google Map
maps.googleapis.com	ok	**IP:** 172.217.24.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
edition.cnn.com	ok	**IP:** 151.101.67.5 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.xmlsoap.org	ok	**IP:** 13.107.246.59 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.openmobilealliance.org	ok	**IP:** 104.26.9.105 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
wsearch.nlm.nih.gov	ok	**IP:** 130.14.16.207 **Country:** United States of America **Region:** Maryland **City:** Bethesda **Latitude:** 38.999641 **Longitude:** -77.155083 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.hockeyapp.net	ok	**IP:** 40.70.164.17 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
www.ncbi.nlm.nih.gov	ok	**IP:** 130.14.29.110 **Country:** United States of America **Region:** Maryland **City:** Bethesda **Latitude:** 38.999641 **Longitude:** -77.155083 **View:** Google Map
www.geniemd.com	ok	**IP:** 52.197.0.54 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.suicidepreventionlifeline.org	ok	**IP:** 172.67.73.127 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bugsense.appspot.com	ok	**IP:** 142.251.220.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.amberalert.gov	ok	**IP:** 149.101.127.86 **Country:** United States of America **Region:** Maryland **City:** Potomac **Latitude:** 39.025749 **Longitude:** -77.197731 **View:** Google Map
www.geniemd.net	ok	**IP:** 54.187.41.139 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
familywize.org	ok	**IP:** 108.157.14.10 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.pollen.com	ok	**IP:** 52.23.90.186 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.color.org	ok	**IP:** 104.26.5.216 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
m.cdc.gov	ok	No Geolocation information available.
zxing.appspot.com	ok	**IP:** 172.217.31.20 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
emergency.cdc.gov	ok	**IP:** 104.71.145.31 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.google.com	ok	**IP:** 142.251.222.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.aiim.org	ok	**IP:** 199.60.103.225 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
m.facebook.com	ok	**IP:** 163.70.158.35 **Country:** France **Region:** Ile-de-France **City:** Nanterre **Latitude:** 48.891979 **Longitude:** 2.206750 **View:** Google Map
www.mayoclinic.com	ok	**IP:** 129.176.1.88 **Country:** United States of America **Region:** Minnesota **City:** Rochester **Latitude:** 44.036819 **Longitude:** -92.491203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.thehotline.org	ok	**IP:** 104.21.7.76 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
serv.familywize.org	ok	**IP:** 18.67.216.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.fda.gov	ok	**IP:** 104.71.156.37 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.accessdata.fda.gov	ok	**IP:** 104.71.156.37 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
services.walgreens.com	ok	**IP:** 27.77.82.227 **Country:** Viet Nam **Region:** Ha Noi **City:** Hanoi **Latitude:** 21.024500 **Longitude:** 105.841171 **View:** Google Map
en.wikipedia.org	ok	**IP:** 103.102.166.224 **Country:** United States of America **Region:** Indiana **City:** Francisco **Latitude:** 38.333332 **Longitude:** -87.447220 **View:** Google Map
alt.bugsense.com	ok	No Geolocation information available.
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

✉ EMAILS

EMAIL	FILE
junit@geniemd.com	br/com/rubythree/geniemd/api/main/Main.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/ReminderTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/LoopBlogTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/UserConditionTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/SymptomTest.java
junit@geniemd.com junitfriend@geniemd.com	br/com/rubythree/test/geniemd/api/models/LoopInvitationTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/UserAllergyTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/VitalTest.java
junit@geniemd.com junitfriend@geniemd.com	br/com/rubythree/test/geniemd/api/models/LoopTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/UserProfileTest.java
junit@geniemd.com junitfriend@geniemd.com	br/com/rubythree/test/geniemd/api/models/UserTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/CareCircleRequestTest.java

EMAIL	FILE
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/MedicationTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/UserInteractionTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/TweetTest.java
junit@geniemd.com c2@geniemd.com c1@geniemd.com	br/com/rubythree/test/geniemd/api/models/EmergencyContactTest.java
junit@geniemd.com	br/com/rubythree/test/geniemd/api/models/FileUploadTest.java
customercare@geniemd.com	com/geniemd/geniemd/activities/WebViewActivity.java
customercare@geniemd.com	com/geniemd/geniemd/activities/TermsOfUseActivity.java
customercare@geniemd.com	com/geniemd/geniemd/activities/videos/VideosActivity.java
your.account@domain.com	com/testflightapp/acra/ErrorReporter.java
customercare@geniemd.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
BugSense	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/371

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
HockeyApp	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/26

HARDCODED SECRETS

POSSIBLE SECRETS
0095E9A9EC9B297BD4BF36E059184F
5EEEFCA380D02919DC2C6558BB6D8A5D
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
b892d9ebdbfc37e397256dd8a5d3123534d1f03726284743ddc6be3a709edb696fc40c7d902ed804c6eee730eee3d5b20bf6bd8d87a296813c87d3b3cc9d7947
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B
E87579C11079F43DD824993C2CEE5ED3
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
f75e80839b9b9379f1cf1128f321639757dba514642c206bbbd99f9a4846208b3e93fbbe5e0527cc59b1d4b929d9555853004c7c8b30ee6a213c3d1bb7415d03

POSSIBLE SECRETS
10C0FB15760860DEF1EEF4D696E676875615175D
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
1394548711991158256014096551076907131070417070599280317977580014543757653577229840941243685222882398330391146816480766882369212207373226721607407477717009111345504320538046476949046861201130878162407401848004770471573366629262494235712488239685422217536601433914856808405203368594584948031873412885804895251637

POSSIBLE SECRETS
115792089237316195423570985008687907853269984665640564039457584007913129639316
ef4cede573cea47f83699b814de4302edb60eefe426c52e17bd7870ec7c6b7a24fe55282ebb73775f369157726fcfb988def2b40350bdca9e5b418340288f649
E95E4A5F737059DC60DF5991D45029409E60FC09
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
9f66f6b05410cd503b2709e88115d55daced94d1a34d4e32bf824d0dde6028ae79c5f07b580f5dce240d7111f7ddb130a7945cd7d957d1920994da389f490c89
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
1335318132727206734338595199483190012179423759678474868994823595993696425287347124615904033277318214103280125292538719147885989931033105677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716593764268326742697808800616315281634758 87
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
74D59FF07F6B413D0EA14B344B20A2DB049B50C3

POSSIBLE SECRETS
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
659EF8BA043916EEDE8911702B22
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
142011741597563481196368286022318089743276138395243738762872573441927459393512718973631166078467600360848946623567625795282774719212241929071046134208380636394084512691828894000571524625445295769349356752728956831541775441763139384457191755096847107846595662547942312293338483924514339614727760681880609734239
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
91771529896554605945588149018382750217296858393520724172743325725474374979801
0217C05610884B63B9C6C7291678F9D341
92e08f83cc9920746989ca5034dcb384a094fb9c5a6288fcc4304424ab8f56388f72652d8fafc65a4b9020896f2cde297080f2a540e7b7ce5af0b3446e1258d1dd7f245cf54124b4c6e17da21b90a0ebd22605e6f45c9f136d7a13eaac1c0f7487de8bd6d924972408ebb58af71e76fd7b012a8d0e165f3ae2e5077a8648e619
31a92ee2029fd10d901b113e990710f0d21ac6b6

POSSIBLE SECRETS
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
0737aaac7d6a4b31af4e3edec6696905
002757A1114D696E6768756151755316C05E0BD4
883423532389192164791648750360308885314476597252960362792450860609699839
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
010092537397ECA4F6145799D62B0A19CE06FE26AD
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
10B7B4D696E676875615175137C8A16FD0DA2211
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

POSSIBLE SECRETS
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
4D696E676875615175985BD3ADBADA21B43A97E2
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
70b7123e8e69dfa76feb1236d0a686144b00e9232ed52b73847e74ef3af71fb45ccb24261f40d27f98101e230cf27b977a5d5f1f15f6cf48d5cb1da2a3a3b87f
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
04B8266A46C55657AC734CE38F018F2192
64033881142927202683649881450433473985931760268884941288852745803908878638612
29818893917731240733471273240314769927240550812383695689146495261604565990247
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
1E589A8595423412134FAA2DBDEC95C8D8675E58

POSSIBLE SECRETS
00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
d3d83daf2a0cecd3367ae6f8ae1aeb82e9ac2f816c6fc483533d8297dd7884cd
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
E95E4A5F737059DC60DFC7AD95B3D8139515620F
6277101735386680763835789423207666416083908700390324961279
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
DB7C2ABF62E35E7628DFAC6561C5
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
57896044618658097711785492504343953926634992332820282019728792003956564823190

POSSIBLE SECRETS
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
115792089210356248762697446949407573530086143415290314195533631308867097853951
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
0307AF69989546103D79329FCC3D74880F33BBE803CB
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
000E0D4D696E6768756151750CC03A4473D03679
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
103FAEC74D696E676875615175777FC5B191EF30
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
07A11B09A76B562144418FF3FF8C2570B8
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150

POSSIBLE SECRETS
22123dc2395a05caa7423daeccc94760a7d462256bd56916
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
b259d2d6e627a768c94be36164c2d9fc79d97aab9253140e5bf17751197731d6f7540d2509e7b9ffee0a70a6e26d56e92d2edd7f85aba85600b69089f35f6bdbf3c298e05842535d9f064e6b0391cb7d306e0a2d20c4dfb4e7b49a9640bdea26c10ad69c3f05007ce2513cee44cfe01998e62b6c3637d3fc0391079b26ee36d5
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
57896044618658097711785492504343953926634992332820282019728792003956564823193
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
B99B99B099B323E02709A4D696E6768756151751
79885141663410976897627118935756323747307951916507639758300472692338873533959
A335926AA319A27A1D00896A6773A4827ACDAC73
c49d360886e704936a6678e1139d26b7819f7e90

POSSIBLE SECRETS
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
DB7C2ABF62E35E668076BEAD208B
51DEF1815DB5ED74FCC34C85D709
E95E4A5F737059DC60DFC7AD95B3D8139515620C
12345678901234567890123456789012
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
6c641094e24d172728b8da3c2777e69adfd0839085be7e38c7c4a2dd00b1ae969f2ec9d23e7e37090fcd449a40af0ed463fe1c612d6810d6b4f58b7bfa31eb5f
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
24B7B137C8A14D696E6768756151756FD0DA2E5C
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
dae7651ee69ad1d081ec5e7188ae126f6004ff39556bde90e0b870962fa7b926d070686d8244fe5a9aa709a95686a104614834b0ada4b10f53197a5cb4c97339

POSSIBLE SECRETS
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
f01734d7960ea60070f1b06f2bb81bfac48ff192ae18451d5e56c734a5aab8a5
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
FFFFFFFE0000000075A30D1B9038A115
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
7039008535208330519954771801901843784107951663004518047128434684370563350261 6
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
00689918DBEC7E5A0DD6DFC0AA55C7
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
1270212482889324174659070427771764435257876535089165358128175072657050312609850984974231883334834011809259999951209889341306592056149967242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336850045410625869714168836867788425378203 83
4E13CA542744D696E67687561517552F279A8C84
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4

POSSIBLE SECRETS
7deb1b194a85bcfd29cf871411468adbc987650903e3bacc8338c449ca7b32efd39ffc33bc84412fcd7df18d23ce9d7c25ea910b1ae9985373e0273b4dca7f2e0db3b7314056ac67fd277f8f89cf2fd73c34c6ca69f9ba477143d2b0e2445548aa0b4a8473095182631da46844c356f5e5c7522eb54b5a33f11d730ead9c0cff
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
401028774D7777C7B7666D1366EA432071274F89FF01E718
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
2AA058F73A0E33AB486B0F610410C53A7F132310
4294182614861580414387344773795550239267234596860714306679811299408947123142002706038521669956384871995765728481489890977075946261343766945636488273037083893479108083593264797677860191534347440096103423131667257868692048219493287863336020338479709268434224762105576023501613261478065276102850944540333865234 1
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
85E25BFE5C86226CDB12016F7553F9D0E693A268
68363196144955700784444165611827252895102170888761442055095051287550314083023
3045AE6FC8422F64ED579528D38120EAE12196D5
1009979067550553047720818155359252248698410825720534578748235158755771479905292727772441528526992987964833566996828420279728960527471731754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940973554032134009725883228768509467406639 62
FB15760860DEF1EEF4D696E6768756151754

POSSIBLE SECRETS
e8b4011604095303ca3b8099982be09fcb9ae616
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
c469684435deb378c4b65ca9591e2a5763059a2e
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
4099B5A457F9D69F79213D094C4BCD4D4262210B
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
b4a7e46170574f16a97082b22be58b6a2a629798419be12872a4bdba626cfae9900f76abfb12139dce5de56564fab2b6543165a040c606887420e33d91ed7ed7
004D696E67687561517512D8F03431FCE63B88F4
985BD3ADBAD4D696E676875615175A21B43A97E3
e38f5750d97e270996a286df2e653fd26c242106436f5bab0f4c7a9e654ce02665d5a281f2c412456f2d1fa26586ef04a9adac9004ca7f913162cb28e13bf40d
6c929e4e81672fef49d9c825163fec97c4b7ba7acb26c0824638ac22605d7201c94625770984f78a56e6e25904fe7db407099cad9b14588841b94f5ab498dded
00E8BEE4D3E2260744188BE0E9C723
8de0d113c5e736969c8d2b047a243f8fe18edad64cde9e842d3669230ca486f7cfdde1f8eec54d1905fff04acc85e61093e180cadc6cea407f193d44bb0e9449b8dbb49784cd9e36260c39e06a947299978c6ed8300724e887198cfede20f3fbde658fa2bd078be946a392bd349f2b49c486e20c405588e306706c9017308e69
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

POSSIBLE SECRETS
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
412935c6b6bc770204be0c2060e75e23
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
57896044618658097711785492504343953927102133160255826820068844496087732066703
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
115792089237316195423570985008687907853073762908499243225378155805079068850323
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A
072546B5435234A422E0789675F432C89435DE5242

POSSIBLE SECRETS
1d1a2d3ca8e52068b3094d501c9a842fec37f54db16e9a67070a8b3f53cc03d4257ad252a1a640eadd603724d7bf3737914b544ae332eedf4f34436cac25ceb5
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
e43bb460f0b80cc0c0b075798e948060f8321b7d
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
6127C24C05F38A0AAAF65C0EF02C
97c7737d1b9a0088c3c7b528539247fd2a1593e7e01cef18848755be82f4a45aa093276cb0cbf118cb41117540a78f3fc471ba5d69f0042274defc9161265721
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
b8f52fc6f38593dabb661d3f50f8897f8106eee68b1bce78a95b132b4e5b5d19
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

POSSIBLE SECRETS
00F50B028E4D696E676875615175290472783FB1
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
10E723AB14D696E6768756151756FEBF8FCB49A9
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
70390085352083305199547718019018437841079516630045180471284346843705633502619
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
020A601907B8C953CA1481EB10512F78744A3205FD
28792665814854611296992347458380284135028636778229113005756334730996303888124
2866537B676752636A68F56554E12640276B649EF7526267
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b30090603550408130243413112301006035504071309506 16c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b06035504031314466163 65626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b 3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084 6616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c2 07d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de20 18ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864 886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483 998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b4 2bd928a2

POSSIBLE SECRETS
297edcbea2076962f8f252724786875b
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
D6031998D1B3BBFEBF59CC9BBFF9AEE1
C49D360886E704936A6678E1139D26B7819F7E90
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
6C01074756099122221056911C77D77E77A777E7E7E77FCB
3045AE6FC8422f64ED579528D38120EAE12196D5
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04

POSSIBLE SECRETS

B4E134D3FB59EB8BAB57274904664D5AF50388BA
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
28091019353058090096996979000309560759124368558014865957655842872397301267595
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
c0a0758cdf14256f78d4708c86becdead1b50ad4ad6c5c703e2168fbf37884cb
70390085352083305199547718019018437840920882647164081035322601458352298396601
115792089237316195423570985008687907853269984665640564039457584007913129639319

POSSIBLE SECRETS
0108B39E77C4B108BED981ED0E890E117C511CF072
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
bca6990fc3c15a8105800c0673517a4b579634a1
7d7374168ffe3471b60a857686a19475d3bfa2ff
003088250CA6E7C7FE649CE85820F7
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
DB7C2ABF62E35E668076BEAD2088
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
1053CDE42C14D696E67687561517533BF3F83345
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
36DF0AAFD8B8D7597CA10520D04B

POSSIBLE SECRETS
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
07A526C63D3E25A256A007699F5447E32AE456B50E
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
D09E8800291CB85396CC6717393284AAA0DA64BA
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
060f6de0-4986-4ce2-881c-e6ab52914a1a
03E5A88919D7CAFCBF415F07C2176573B2

POSSIBLE SECRETS
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
b54bb9edff22051d9ee60f9351a48591b6500a319429c069a3e335a1d6171391

Report Generated by - MobSF v4.0.3

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.