# ANDROID STATIC ANALYSIS REPORT

## Doximity (11.3.0)

| | |
|---|---|
| File Name: | com.doximity.doximitydroid_213621.apk |
| Package Name: | com.doximity.doximitydroid |
| Scan Date: | Aug. 29, 2025, 9:46 p.m. |
| App Security Score: | 49/100 (MEDIUM RISK) |

|  |  |
|---|---|
| Grade: | B |
| Trackers Detection: | 5/432 |

## FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 6 | 23 | 6 | 4 | 2 |

## FILE INFORMATION

**File Name:** com.doximity.doximitydroid_213621.apk
**Size:** 88.75MB
**MD5:** f1ad8833f3926460003c6d00794f6440
**SHA1:** b769153207815a29f101604c32610b53234688ff
**SHA256:** 1216a5683c6a5de8a0d860a290c1d06dfb9aa8d641c8eb576073aed10f356ac0

## APP INFORMATION

**App Name:** Doximity
**Package Name:** com.doximity.doximitydroid

**Main Activity:** com.doximity.doximitydroid.NavActivity
**Target SDK:** 35
**Min SDK:** 25
**Max SDK:**
**Android Version Name:** 11.3.0
**Android Version Code:** 213621

## APP COMPONENTS

**Activities:** 12
**Services:** 21
**Receivers:** 20
**Providers:** 8
**Exported Activities:** 1
**Exported Services:** 3
**Exported Receivers:** 6
**Exported Providers:** 1

## CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Mateo, O=Doximity, OU=Doximity, CN=Shari Buck
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-02-18 07:00:25+00:00
Valid To: 2038-07-06 07:00:25+00:00
Issuer: C=US, ST=California, L=San Mateo, O=Doximity, OU=Doximity, CN=Shari Buck
Serial Number: 0x4d5e1909
Hash Algorithm: sha1
md5: 7c7373986654ad8a04d0d507f94ccb45
sha1: 7f009a3dc403faac68c93611da7144b6a526b438
sha256: f2e15c47da4ecffca7821a16dba221be2629d9803c41c4af459a76596e64752a
sha512: 52a71512a6cec17427a4858d659e02db62a6ec5cf526ba19f100546b3c0d0ec31b4f2651f4e18a7fe75c14dfa3e3b9b69e73fa9ba8e0621f906920ac55576e2f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b630affd3e153a9a8832a97cb96ab289a02f9e08d140e29ddeb00e839edaef05
Found 1 unique certificates

## APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| 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.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |
| 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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| 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.READ_PHONE_NUMBERS | dangerous | allows reading of the device's phone number(s). | Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications. |
| 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.USE_BIOMETRIC | normal | allows use of device-supported biometric modalities. | Allows an app to use device supported biometric modalities. |
| 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.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| 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.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.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| android.permission.FOREGROUND_SERVICE_CAMERA | normal | allows foreground services with camera use. | Allows a regular application to use Service.startForeground with the type "camera". |
| android.permission.FOREGROUND_SERVICE_MICROPHONE | normal | permits foreground services with microphone use. | Allows a regular application to use Service.startForeground with the type "microphone". |
| android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK | normal | enables foreground services for media playback. | Allows a regular application to use Service.startForeground with the type "mediaPlayback". |
| android.permission.FOREGROUND_SERVICE_PHONE_CALL | normal | enables foreground services during phone calls. | Allows a regular application to use Service.startForeground with the type "phoneCall". |
| android.permission.MANAGE_OWN_CALLS | normal | enables a calling app to manage its own calls. | Allows a calling application which manages it own calls through the self-managed ConnectionService APIs. |
| android.permission.DOWNLOAD_WITHOUT_NOTIFICATION | unknown | Unknown permission | Unknown permission from android reference |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.FOREGROUND_SERVICE_DATA_SYNC | normal | permits foreground services for data synchronization. | Allows a regular application to use Service.startForeground with the type "dataSync". |
| com.google.android.gms.permission.AD_ID | normal | application shows advertisements | This app uses a Google advertising ID and can possibly serve advertisements. |
| BIND_GET_INSTALL_REFERRER_SERVICE | unknown | Unknown permission | Unknown permission from android reference |
| com.android.vending.CHECK_LICENSE | unknown | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.doximity.doximitydroid.permission.C2D_MESSAGE | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications |
| android.permission.USE_FULL_SCREEN_INTENT | normal | required for full screen intents in notifications. | Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents. |
| com.doximity.doximitydroid.CROSS_APP_COMMUNICATION | 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. |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| 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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |
| android.permission.ACCESS_ADSERVICES_ATTRIBUTION | normal | allow applications to access advertising service attribution | This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns. |
| android.permission.ACCESS_ADSERVICES_AD_ID | normal | allow app to access the device's advertising ID. | This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy. |
| android.permission.CHANGE_NETWORK_STATE | normal | change network connectivity | Allows applications to change network connectivity state. |
| 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.doximity.doximitydroid.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH_CONNECT | dangerous | necessary for connecting to paired Bluetooth devices. | Required to be able to connect to paired Bluetooth devices. |

## APKID ANALYSIS

| FILE | DETAILS | |
|---|---|---|
| f1ad8833f3926460003c6d00794f6440.apk | FINDINGS | DETAILS |
| | Anti-VM Code | possible VM check |
| classes.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check<br>Build.MANUFACTURER check<br>Build.TAGS check |
| | Compiler | dexlib 1.x<br>r8 |
| classes10.dex | FINDINGS | DETAILS |
| | Compiler | r8 without marker (suspicious) |
| classes2.dex | FINDINGS | DETAILS |
| | Compiler | r8 without marker (suspicious) |
| classes3.dex | FINDINGS | DETAILS |
| | Compiler | r8 without marker (suspicious) |
| classes4.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.TAGS check |
| | Compiler | r8 without marker (suspicious) |

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.TAGS check<br>SIM operator check<br>network operator name check<br>possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes6.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes7.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes8.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check<br>possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes9.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check<br>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.doximity.doximitydroid.NavActivity | Schemes: https://, tel://, doximitydialer://, doximity://,<br>Hosts: www.doximity.com, doximity.com, doc-defender.doximity.com, dialer-api.doximity.com, dialer.doximity.com, *.doximity.services, *.doximity-staging.services, doximity.doximity.onelink.me, doximity.sng.link, v.dox.com, t.doximity.com, c-eda.doximity.com, doximity,<br>Paths: /qr, /notifications, /colleagues, /home, /api/v1/clicks,<br>Path Prefixes: /inbox, /share, /profile, /dialer, /careers/job_cards, /article, /doc_news/v2, /newsfeed, /sponsored, /collections, /show_url, /video, /voice, /care_team/members, /fax, /job-listings, /hospitals, /search, /onelink.me, /tokenized, /news, /vm1, /docs-gpt, /t,<br>Path Patterns: /.*, |

## NETWORK SECURITY

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

| NO | SCOPE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | doximity.com | secure | Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Digest: SHA-256,Pin: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E= Digest: SHA-256] |
| 2 | support.doximity.com<br>graphql-federation.doximity.services | secure | Domain config is securely configured to disallow clear text traffic to these domains in scope. |

## CERTIFICATE ANALYSIS

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

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |
| Certificate algorithm vulnerable to hash collision | high | Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. |

## MANIFEST ANALYSIS

HIGH: **1** | WARNING: **12** | INFO: **0** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | App can be installed on a vulnerable unpatched Android version<br>Android 7.1-7.1.2, [minSdk=25] | 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 | App has a Network Security Configuration<br>[android:networkSecurityConfig=@xml/network_security_config] | info | The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app. |
| 3 | TaskAffinity is set for activity<br>(com.doximity.doximitydroid.features.dialer.presentation.video.VideoCallActivity) | warning | If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 4 | Broadcast Receiver (com.doximity.doximitydroid.features.pushnotifications.channels.NotificationChannelUpdateBroadcastReceiver) is not Protected.<br>[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. |
| 5 | Broadcast Receiver (com.doximity.doximitydroid.features.dialer.presentation.ftue.setup.SmsVerificationBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.google.android.gms.auth.api.phone.permission.SEND<br>[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. |
| 6 | Broadcast Receiver (com.doximity.auth.platform.crossapplogin.DeviceApprovalBroadcastReceiver) is Protected by a permission.<br>Permission: com.doximity.doximitydroid.CROSS_APP_COMMUNICATION<br>protectionLevel: signature<br>[android:exported=true] | info | A Broadcast Receiver is found to be exported, but is protected by permission. |
| 7 | Broadcast Receiver (com.doximity.auth.platform.crossapplogin.RequestDeviceAccessTokenBroadcastReceiver) is Protected by a permission.<br>Permission: com.doximity.doximitydroid.CROSS_APP_COMMUNICATION<br>protectionLevel: signature<br>[android:exported=true] | info | A Broadcast Receiver is found to be exported, but is protected by permission. |
| 8 | Content Provider (com.doximity.auth.platform.crossapplogin.CrossAppDataContentProvider) is Protected by a permission.<br>Permission: com.doximity.doximitydroid.CROSS_APP_COMMUNICATION<br>protectionLevel: signature<br>[android:exported=true] | info | A Content Provider is found to be exported, but is protected by permission. |
| 9 | Content Provider (com.pspdfkit.document.sharing.DocumentSharingProvider) is not Protected.<br>[android:exported=true] | warning | A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 10 | Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION<br>[android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |
| 11 | Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.google.android.c2dm.permission.SEND<br>[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. |
| 12 | Service (live.hms.video.services.HMSScreenCaptureService) is not Protected.<br>[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. |
| 13 | Broadcast Receiver (live.hms.video.services.LogAlarmManager) is not Protected.<br>[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. |
| 14 | Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_JOB_SERVICE<br>[android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 15 | Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.DUMP<br>[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. |
| 16 | Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected.<br>[android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 17 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.DUMP<br>[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: **5** | SECURE: **2** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/babylon/certificatetransparency/internal/loglist/model/v2/Log.java<br>com/doximity/doximitydroid/BuildConfig.java<br>com/doximity/doximitydroid/core/presentation/BuildConfig.java<br>com/doximity/doximitydroid/core/presentation/analytics/AnalyticsViewModelDelegateKt.java<br>com/doximity/doximitydroid/core/presentation/compose/presenters/EventHandler.java<br>com/doximity/doximitydroid/core/presentation/models/dialer/DialerDeeplink.java<br>com/doximity/doximitydroid/core/presentation/pymk/PeopleYouMayKnow.java<br>com/doximity/doximitydroid/core/presentation/viewpdf/ViewPdfActivity.java<br>com/doximity/doximitydroid/core/presentation/viewpdf/ViewPdfVMState.java<br>com/doximity/doximitydroid/domain/encryption/EncryptionAlgorithm.java<br>com/doximity/doximitydroid/domain/models/AttachmentInfo.java<br>com/doximity/doximitydroid/domain/models/EncryptedUploadDataModel.java<br>com/doximity/doximitydroid/domain/models/analytics/AnalyticsKeys.java<br>com/doximity/doximitydroid/domain/models/dialer/DiscoverDialerCard.java<br>com/doximity/doximitydroid/domain/models/dialer/PatientMessageLanguage.java<br>com/doximity/doximitydroid/domain/models/dialer/PatientMessageLanguageDataModel.java<br>com/doximity/doximitydroid/domain/models/dialer/TextAttachmentCreationConfigurationDataModel.java<br>com/doximity/doximitydroid/domain/models/faxMessages/AttachmentDataModel.java<br>com/doximity/doximitydroid/domain/models/pushnotifications/PushNotification.java<br>com/doximity/doximitydroid/domain/models/resnav/ResNavCharacteristicDataModel.java<br>com/doximity/doximitydroid/domain/models/resnav/ResNavLocationDataModel.java<br>com/doximity/doximitydroid/domain/models/resnav/ResNavTrainingEnvironmentDataModel.java<br>com/doximity/doximitydroid/domain/models/serverdrivenui/ServerDrivenFTUE.java<br>com/doximity/doximitydroid/features/dialer/domain/usecase/ehr/GetEHRPatientNumbersUseCase.java<br>com/doximity/doximitydroid/features/dialer/domain/usecase/settings/patientmessagelanguage/UpdatePatientMessageLanguageUseCase.java<br>com/doximity/doximitydroid/features/dialer/domain/usecase/video/ResendVideoCallTextInviteUseCase.java<br>com/doximity/doximitydroid/features/dialer/domain/usecase/video/SendVideoCallInviteUseCase.java<br>com/doximity/doximitydroid/features/dialer/domain/usecase/video/TerminateVideoCallUseCase.java<br>com/doximity/doximitydroid/features/dialer/presentation/destinations/VideoHandOffDialogDestination.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | nation.java<br>com/doximity/doximitydroid/features/dialer/presentation/maindialer/ehr/EHRConnectVMState.java<br>com/doximity/doximitydroid/features/dialer/presentation/settings/hospitalaffiliation/HospitalAffiliationUiState.java<br>com/doximity/doximitydroid/features/dialer/presentation/settings/patientlanguage/textlink/PatientTextLinkLanguageUiState.java<br>com/doximity/doximitydroid/features/dialer/presentation/video/VideoCallUiEvent.java<br>com/doximity/doximitydroid/features/dialer/presentation/video/handoff/VideoHandOffDialogNavArgs.java<br>com/doximity/doximitydroid/features/dialer/presentation/video/handoff/VideoHandOffUiState.java<br>com/doximity/doximitydroid/features/serverdrivenui/domain/usecase/GetServerDrivenFtueUseCase.java<br>com/doximity/doximitydroid/features/serverdrivenui/domain/usecase/UpdateServerDrivenFTUEShownUseCase.java<br>com/doximity/doximitydroid/features/serverdrivenui/presentation/ftue/ServerDrivenFTUEPresenter.java<br>com/doximity/doximitydroid/features/serverdrivenui/presentation/ftue/ServerDrivenFTUEScreenNavArgs.java<br>com/doximity/doximitydroid/features/serverdrivenui/presentation/ftue/destinations/ServerDrivenFTUEScreenDestination.java<br>com/doximity/doximitydroid/features/whileyouwait/domain/usecase/GetWhileYouWaitContentUseCase.java<br>com/doximity/doximitydroid/features/whileyouwait/domain/usecase/sponsored/FetchDocPointAdUseCase.java<br>com/doximity/doximitydroid/repositories/features/pushnotifications/PushNotificationsConfigurationRepositoryImplKt.java<br>com/doximity/doximitydroid/sources/CreateOfficeLocationSourceMutation.java<br>com/doximity/doximitydroid/sources/FtueForKeyQuery.java<br>com/doximity/doximitydroid/sources/GenerateEncryptedUploadPathSourceMutation.java<br>com/doximity/doximitydroid/sources/PatientMessageLanguageOptionsSourceQuery.java<br>com/doximity/doximitydroid/sources/ResNavSearchCriteriaSourceQuery.java<br>com/doximity/doximitydroid/sources/environments/CurrentEnvironmentSourceKt.java<br>com/doximity/doximitydroid/sources/firebase/FirebaseDataSourceKt.java<br>com/doximity/doximitydroid/sources/fragment/DiscoverDialerCardFragment.java<br>com/doximity/doximitydroid/sources/fragment/ServerDrivenFtueFragment.java<br>com/doximity/doximitydroid/sources/models/dialer/Arguments.java<br>com/doximity/doximitydroid/sources/models/dialer/FromToVideoCallDataResponse.java<br>com/doximity/doximitydroid/sources/models/dialer/careteam/JoinCareTeamRequestBody.java<br>com/doximity/doximitydroid/sources/room/ResNavCharacteristicEntity.java<br>com/doximity/doximitydroid/sources/room/ResNavRegionEntity.java<br>com/doximity/doximitydroid/sources/room/ResNavTrainingEnvironmentEntity.java<br>com/doximity/doximitydroid/sources/type/Dialer_UpdateUserSettingsPatientMessageLanguageInput.java<br>com/doximity/doximitydroid/sources/type/EncryptedAttachmentInput.java<br>com/doximity/doximitydroid/sources/type/Ftue_RecordUserFtueEngagedInput.java<br>com/doximity/doximitydroid/sources/type/Ftue_RecordUserFtueViewedInput.java<br>com/doximity/doximitydroid/sources/type/Inbox_EncryptedAttachmentInput.java<br>com/doximity/doximitydroid/tracker/BuildConfig.java<br>com/effectssdk/tsvb/license/LicenseValidator.java<br>com/pspdfkit/internal/jni/NativeDocumentProvider.java<br>com/pspdfkit/internal/jni/NativeDocumentSecurityOptions.java<br>com/pspdfkit/internal/jni/NativeFormNotifications.java<br>com/pspdfkit/internal/jni/NativeSignatureBuildProperties.java<br>com/pspdfkit/ui/c.java<br>com/twilio/voice/EventKeys.java<br>com/twilio/voice/HttpsRegistrar.java<br>com/twilio/voice/VoiceURLConnection.java<br>com/twilio/voice/WarningEventConstants.java<br>io/jsonwebtoken/JwsHeader.java<br>live/hms/video/audio/HMSAudioManagerLegacy.java<br>live/hms/video/factories/HMSPeerConnectionFactory.java<br>live/hms/video/sdk/models/HMSNotifications.java<br>live/hms/video/utils/HMSConstantsKt.java<br>o/b16.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | o/lb3.java<br>o/np4.java<br>o/pi0.java<br>o/xq5.java |
| | | | | com/bugsnag/android/c.java<br>com/canhub/cropper/CropImageActivity.java<br>com/canhub/cropper/CropImageView.java<br>com/canhub/cropper/CropOverlayView.java<br>com/caverock/androidsvg/e0.java<br>com/caverock/androidsvg/h.java<br>com/caverock/androidsvg/h0.java<br>com/caverock/androidsvg/i0.java<br>com/doximity/doximitydroid/core/presentation/utils/logging/DoxDebugTree.java<br>com/doximity/doximitydroid/domain/logging/RemoteLog.java<br>com/doximity/doximitydroid/repositories/features/logging/LogRepositoryImpl.java<br>com/effectssdk/tsvb/EffectsSDK.java<br>com/effectssdk/tsvb/license/LicenseValidator.java<br>com/effectssdk/tsvb/pipeline/ImagePipelineImpl.java<br>com/effectssdk/tsvb/pipeline/PipelineCore.java<br>com/pspdfkit/annotations/c.java<br>com/pspdfkit/bookmarks/a.java<br>com/pspdfkit/document/providers/AssetDataProvider.java<br>com/pspdfkit/document/providers/ContentResolverDataProvider.java<br>com/pspdfkit/document/providers/InputStreamDataProvider.java<br>com/pspdfkit/instant/ui/InstantPdfFragment.java<br>com/pspdfkit/internal/a2.java<br>com/pspdfkit/internal/a5.java<br>com/pspdfkit/internal/ac.java<br>com/pspdfkit/internal/b9.java<br>com/pspdfkit/internal/bc.java<br>com/pspdfkit/internal/be.java<br>com/pspdfkit/internal/bg.java<br>com/pspdfkit/internal/c1.java<br>com/pspdfkit/internal/c8.java<br>com/pspdfkit/internal/c9.java<br>com/pspdfkit/internal/ca.java<br>com/pspdfkit/internal/cc.java<br>com/pspdfkit/internal/cd.java<br>com/pspdfkit/internal/cf.java<br>com/pspdfkit/internal/d8.java<br>com/pspdfkit/internal/dd.java<br>com/pspdfkit/internal/de.java<br>com/pspdfkit/internal/dh.java<br>com/pspdfkit/internal/dj.java<br>com/pspdfkit/internal/dp.java<br>com/pspdfkit/internal/e2.java<br>com/pspdfkit/internal/e5.java<br>com/pspdfkit/internal/eg.java<br>com/pspdfkit/internal/f8.java<br>com/pspdfkit/internal/g1.java<br>com/pspdfkit/internal/h8.java<br>com/pspdfkit/internal/h9.java<br>com/pspdfkit/internal/ig.java<br>com/pspdfkit/internal/ih.java<br>com/pspdfkit/internal/j.java<br>com/pspdfkit/internal/j9.java<br>com/pspdfkit/internal/jf.java<br>com/pspdfkit/internal/jj.java<br>com/pspdfkit/internal/jn.java<br>com/pspdfkit/internal/jp.java<br>com/pspdfkit/internal/k7.java<br>com/pspdfkit/internal/k8.java<br>com/pspdfkit/internal/kf.java<br>com/pspdfkit/internal/kn.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/pspdfkit/internal/l1.java<br>com/pspdfkit/internal/l9.java<br>com/pspdfkit/internal/lj.java<br>com/pspdfkit/internal/lm.java<br>com/pspdfkit/internal/lo.java<br>com/pspdfkit/internal/lp.java<br>com/pspdfkit/internal/m0.java<br>com/pspdfkit/internal/m8.java<br>com/pspdfkit/internal/md.java<br>com/pspdfkit/internal/mj.java<br>com/pspdfkit/internal/mn.java<br>com/pspdfkit/internal/mp.java<br>com/pspdfkit/internal/n1.java<br>com/pspdfkit/internal/n8.java<br>com/pspdfkit/internal/nn.java<br>com/pspdfkit/internal/no.java<br>com/pspdfkit/internal/o0.java<br>com/pspdfkit/internal/oo.java<br>com/pspdfkit/internal/p0.java<br>com/pspdfkit/internal/p1.java<br>com/pspdfkit/internal/p8.java<br>com/pspdfkit/internal/pg.java<br>com/pspdfkit/internal/qf.java<br>com/pspdfkit/internal/qk.java<br>com/pspdfkit/internal/qo.java<br>com/pspdfkit/internal/r0.java<br>com/pspdfkit/internal/r1.java<br>com/pspdfkit/internal/rc.java<br>com/pspdfkit/internal/ri.java<br>com/pspdfkit/internal/rj.java<br>com/pspdfkit/internal/rn.java<br>com/pspdfkit/internal/sf.java<br>com/pspdfkit/internal/sn.java<br>com/pspdfkit/internal/th.java<br>com/pspdfkit/internal/tj.java<br>com/pspdfkit/internal/tn.java<br>com/pspdfkit/internal/u1.java<br>com/pspdfkit/internal/uc.java<br>com/pspdfkit/internal/uh.java<br>com/pspdfkit/internal/ui/dialog/signatures/a.java<br>com/pspdfkit/internal/uj.java<br>com/pspdfkit/internal/views/document/d.java<br>com/pspdfkit/internal/views/document/editor/e.java<br>com/pspdfkit/internal/views/utils/CircleImageView.java<br>com/pspdfkit/internal/vn.java<br>com/pspdfkit/internal/vp.java<br>com/pspdfkit/internal/w8.java<br>com/pspdfkit/internal/w9.java<br>com/pspdfkit/internal/wg.java<br>com/pspdfkit/internal/wh.java<br>com/pspdfkit/internal/x.java<br>com/pspdfkit/internal/x1.java<br>com/pspdfkit/internal/x8.java<br>com/pspdfkit/internal/xb.java<br>com/pspdfkit/internal/xh.java<br>com/pspdfkit/internal/xi.java<br>com/pspdfkit/internal/y9.java<br>com/pspdfkit/internal/yf.java<br>com/pspdfkit/internal/yh.java<br>com/pspdfkit/internal/ym.java<br>com/pspdfkit/internal/z1.java<br>com/pspdfkit/internal/z3.java<br>com/pspdfkit/internal/z4.java<br>com/pspdfkit/internal/z9.java<br>com/pspdfkit/internal/zn.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/pspdfkit/ui/PdfReaderView.java<br>com/pspdfkit/ui/PdfThumbnailBar.java<br>com/pspdfkit/ui/a.java<br>com/pspdfkit/ui/c.java<br>com/pspdfkit/ui/search/b.java<br>com/pspdfkit/ui/signatures/SignaturePickerFragment.java<br>com/pspdfkit/ui/toolbar/ToolbarCoordinatorLayout.java<br>com/pspdfkit/utils/LogCatLogger.java<br>com/twilio/audioswitch/android/ProductionLogger.java<br>com/twilio/video/Logger.java<br>com/twilio/voice/EventPublisher.java<br>com/twilio/voice/Logger.java<br>com/twilio/voice/Registration.java<br>live/hms/video/audio/HMSBluetoothManager.java<br>live/hms/video/audio/manager/AudioManagerCompat.java<br>live/hms/video/audio/manager/HMSAudioManagerApi31.java<br>live/hms/video/connection/HMSConnection.java<br>live/hms/video/connection/degredation/WebRtcStatsMonitor.java<br>live/hms/video/connection/publish/HMSPublishConnection$nativeObserver$1$onIceCandidate$1.java<br>live/hms/video/connection/publish/HMSPublishConnection$nativeObserver$1$onIceConnectionChange$1.java<br>live/hms/video/connection/publish/HMSPublishConnection$nativeObserver$1$onRenegotiationNeeded$1.java<br>live/hms/video/connection/publish/HMSPublishConnection$nativeObserver$1$onSelectedCandidatePairChanged$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onAddTrack$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onDataChannel$1$1$onMessage$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onDataChannel$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onIceCandidate$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onIceConnectionChange$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onRemoveTrack$1.java<br>live/hms/video/connection/subscribe/HMSSubscribeConnection$nativeObserver$1$onSelectedCandidatePairChanged$1.java<br>live/hms/video/factories/SafeVariable.java<br>live/hms/video/factories/noisecancellation/NoiseCancellationFactoryImpl.java<br>live/hms/video/factories/noisecancellation/NoiseCancellationFake.java<br>live/hms/video/factories/noisecancellation/NoiseCancellationImpl.java<br>live/hms/video/interactivity/HmsInteractivityCenter$startWhiteboard$1.java<br>live/hms/video/interactivity/HmsInteractivityCenter.java<br>live/hms/video/polls/HMSPollResponseBuilder.java<br>live/hms/video/polls/network/HmsPollsStartManager$manage$1.java<br>live/hms/video/sdk/NoiseCancellationReportingUseCase.java<br>live/hms/video/sdk/SDKDelegate$transportObserver$1.java<br>live/hms/video/sdk/SDKDelegate.java<br>live/hms/video/sdk/managers/OnTrackRemoveManager.java<br>live/hms/video/signal/jsonrpc/JSONRpcSignal.java<br>live/hms/video/utils/ExtensionUtilsKt.java<br>live/hms/video/utils/HMSCoroutineScope$launchWithTimeout$1.java<br>live/hms/video/utils/HMSLogger.java<br>live/hms/video/utils/LogUtils.java<br>live/hms/video/virtualbackground/HMSVirtualBackground.java<br>live/hms/videoview/HMSVideoView.java<br>live/hms/videoview/textureview/HMSTextureRenderer.java<br>o/a11.java<br>o/a57.java<br>o/ab2.java<br>o/aed.java<br>o/ak3.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 2 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | o/apa.java<br>o/aw9.java<br>o/azb.java<br>o/b08.java<br>o/b1a.java<br>o/b57.java<br>o/b6b.java<br>o/b92.java<br>o/be4.java<br>o/bj2.java<br>o/bk3.java<br>o/bo.java<br>o/bpa.java<br>o/bq.java<br>o/bt3.java<br>o/bt4.java<br>o/bw9.java<br>o/c08.java<br>o/c57.java<br>o/c67.java<br>o/c8b.java<br>o/co0.java<br>o/cp3.java<br>o/cw9.java<br>o/d08.java<br>o/di2.java<br>o/dn4.java<br>o/do3.java<br>o/dp3.java<br>o/dq2.java<br>o/dr.java<br>o/dz4.java<br>o/ec3.java<br>o/ei2.java<br>o/ejd.java<br>o/erb.java<br>o/ev8.java<br>o/ewc.java<br>o/f4.java<br>o/f92.java<br>o/fd4.java<br>o/fkb.java<br>o/fqa.java<br>o/fv8.java<br>o/g22.java<br>o/g76.java<br>o/g92.java<br>o/gbb.java<br>o/ged.java<br>o/gf8.java<br>o/gg6.java<br>o/gm9.java<br>o/gqb.java<br>o/grb.java<br>o/gs.java<br>o/gv8.java<br>o/h06.java<br>o/h84.java<br>o/he0.java<br>o/ho4.java<br>o/hrb.java<br>o/hsa.java<br>o/hv8.java<br>o/i22.java<br>o/i46.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | o/i83.java<br>o/ib2.java<br>o/ij9.java<br>o/in4.java<br>o/ir5.java<br>o/it5.java<br>o/iu8.java<br>o/iv8.java<br>o/iyb.java<br>o/j7b.java<br>o/j92.java<br>o/jdb.java<br>o/joa.java<br>o/jwa.java<br>o/jzb.java<br>o/k12.java<br>o/kb0.java<br>o/kg.java<br>o/kj.java<br>o/kq.java<br>o/l4.java<br>o/l77.java<br>o/l89.java<br>o/ld5.java<br>o/loc.java<br>o/lra.java<br>o/lwa.java<br>o/lz5.java<br>o/m06.java<br>o/m12.java<br>o/m77.java<br>o/mmc.java<br>o/mqa.java<br>o/mxb.java<br>o/n2.java<br>o/nb6.java<br>o/nc0.java<br>o/ne8.java<br>o/neb.java<br>o/nl4.java<br>o/nqa.java<br>o/nwa.java<br>o/nxb.java<br>o/o12.java<br>o/oe9.java<br>o/oea.java<br>o/og.java<br>o/oh.java<br>o/oib.java<br>o/olc.java<br>o/ooa.java<br>o/op1.java<br>o/p72.java<br>o/p76.java<br>o/p7b.java<br>o/pk7.java<br>o/po3.java<br>o/pu8.java<br>o/pv2.java<br>o/pxa.java<br>o/q57.java<br>o/q76.java<br>o/qd2.java<br>o/qi0.java<br>o/qn.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | o/rf8.java<br>o/rm1.java<br>o/ro3.java<br>o/s3a.java<br>o/s4b.java<br>o/sd4.java<br>o/sg.java<br>o/sha.java<br>o/sn3.java<br>o/so3.java<br>o/sp6.java<br>o/su8.java<br>o/t16.java<br>o/t17.java<br>o/t77.java<br>o/t7a.java<br>o/t82.java<br>o/t9c.java<br>o/ta9.java<br>o/td4.java<br>o/te1.java<br>o/tx5.java<br>o/tz8.java<br>o/u1b.java<br>o/u2b.java<br>o/u4b.java<br>o/u51.java<br>o/u97.java<br>o/ua9.java<br>o/uc3.java<br>o/uh.java<br>o/uh8.java<br>o/uh9.java<br>o/uha.java<br>o/un3.java<br>o/un4.java<br>o/uo.java<br>o/up1.java<br>o/ux7.java<br>o/v7b.java<br>o/vab.java<br>o/vd.java<br>o/vd4.java<br>o/vg.java<br>o/vh8.java<br>o/vk.java<br>o/vk5.java<br>o/vm1.java<br>o/vpa.java<br>o/w12.java<br>o/w18.java<br>o/w5d.java<br>o/w74.java<br>o/w81.java<br>o/w82.java<br>o/wh.java<br>o/wj5.java<br>o/wm1.java<br>o/wn4.java<br>o/wq8.java<br>o/wu2.java<br>o/wy8.java<br>o/x01.java<br>o/x1b.java<br>o/x82.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | o/x84.java<br>o/xd4.java<br>o/xg0.java<br>o/xm3.java<br>o/xpc.java<br>o/xu8.java<br>o/xv9.java<br>o/xz8.java<br>o/y1b.java<br>o/y49.java<br>o/y82.java<br>o/ya2.java<br>o/ygd.java<br>o/yha.java<br>o/yoa.java<br>o/yw8.java<br>o/z0d.java<br>o/z1b.java<br>o/z82.java<br>o/za2.java<br>o/zb0.java<br>o/zu8.java<br>o/zz7.java<br>tvi/webrtc/DefaultVideoEncoderFactory.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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/doximity/doximitydroid/core/presentation/utils/FileExporter.java<br>com/pspdfkit/internal/d8.java<br>com/pspdfkit/internal/th.java<br>live/hms/video/utils/LogUtils.java<br>o/xg0.java |
| 4 | App creates temp file. Sensitive information should never be written into a temp file. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/canhub/cropper/CropImageActivity.java<br>com/doximity/doximitydroid/platform/file/FileHelperImpl.java<br>com/doximity/doximitydroid/repositories/MediaFileCreatorImpl.java<br>com/pspdfkit/internal/th.java<br>o/gg6.java<br>o/m89.java<br>o/m9.java<br>o/ug0.java<br>o/vx2.java<br>o/xg0.java<br>o/zs0.java |
| 5 | 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')<br>OWASP Top 10: M7: Client Code Quality | com/pspdfkit/internal/j8.java<br>o/be0.java<br>o/ce0.java<br>o/cjd.java<br>o/lob.java<br>o/mta.java<br>o/ng8.java<br>o/rg8.java<br>o/wqa.java<br>o/yx5.java<br>o/zl8.java |
| 6 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | com/twilio/voice/SidUtil.java<br>o/sp6.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 7 | Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. | warning | CWE: CWE-749: Exposed Dangerous Method or Function<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | com/doximity/doximitydroid/core/presentation/compose/videoplayer/jsvideoplayer/JsVideoPlayerContentKt.java<br>com/doximity/doximitydroid/core/presentation/compose/videoplayer/jsvideoplayer/YoutubePlayerContentKt.java<br>com/doximity/doximitydroid/features/dialer/presentation/preflight/PreFlightComposableKt.java<br>o/bv.java<br>o/ij5.java |
| 8 | This App uses SQL Cipher. Ensure that secrets are not hardcoded in code. | info | OWASP MASVS: MSTG-CRYPTO-1 | o/ai.java |
| 9 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | com/bugsnag/android/RootDetector.java<br>o/iwb.java<br>o/wm1.java |
| 10 | SHA-1 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | com/bugsnag/android/d.java<br>com/effectssdk/tsvb/ResourceProvider.java<br>com/pspdfkit/internal/ii.java<br>com/pspdfkit/internal/y9.java<br>o/di2.java<br>o/hz2.java<br>o/in4.java<br>o/j8a.java<br>o/t7a.java<br>o/wm1.java |
| 11 | Debug configuration enabled. Production builds must not be debuggable. | high | CWE: CWE-919: Weaknesses in Mobile Applications<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | com/twilio/audioswitch/BuildConfig.java |
| 12 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | com/doximity/doximitydroid/domain/extensions/ExtensionsKt.java<br>com/pspdfkit/internal/aj.java<br>com/pspdfkit/internal/d0.java<br>o/cr7.java<br>o/dr.java<br>o/ee.java<br>o/hz2.java<br>o/i22.java<br>o/jf3.java<br>o/la7.java<br>o/of2.java<br>o/pz7.java<br>o/qz7.java<br>o/s2.java<br>o/sp1.java<br>o/u12.java<br>o/u1b.java |
| 13 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | com/effectssdk/tsvb/license/PreferencesStore.java<br>com/pspdfkit/internal/oc.java |
| 14 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | com/effectssdk/tsvb/license/LicenseValidator.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 15 | 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/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/platform/ClipboardProviderImpl.java<br>com/pspdfkit/internal/j2.java<br>com/pspdfkit/internal/k2.java<br>com/pspdfkit/internal/tm.java<br>o/a87.java<br>o/io9.java<br>o/p67.java<br>o/s6.java |
| 16 | IP Address disclosure | warning | CWE: CWE-200: Information Exposure<br>OWASP MASVS: MSTG-CODE-2 | o/fr5.java<br>o/nwa.java<br>o/t31.java |
| 17 | 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<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3 | com/doximity/doximitydroid/core/presentation/webview/auth/AuthenticatedWebViewComposeKt$AuthenticatedWebViewContent$3$4$1.java |
| 18 | This app listens to Clipboard changes. Some malware also listen to Clipboard changes. | info | OWASP MASVS: MSTG-PLATFORM-4 | com/doximity/doximitydroid/core/presentation/compose/markdown/MarkdownClipboardHandlerImpl.java<br>com/pspdfkit/internal/e2.java |
| 19 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | o/d11.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 | com/twilio/video/CameraCapturer.java<br>org/webrtc/Camera1Session.java<br>tvi/webrtc/Camera1Session.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/doximity/doximitydroid/DoxAppUtilKt.java<br>com/doximity/doximitydroid/core/presentation/emailtoverify/EmailToVerifyComposablesKt$EmailToVerifyDialog$2.java<br>com/doximity/doximitydroid/core/presentation/navigation/IntentProvider.java<br>com/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/core/presentation/utils/UiExtensionsKt.java<br>com/doximity/doximitydroid/drawer/DebugDrawerViewModel.java<br>com/doximity/doximitydroid/features/login/LoginViewModel.java<br>com/doximity/doximitydroid/features/pushnotifications/action/PushNotificationIntentExtensionsKt.java<br>com/doximity/doximitydroid/features/webview/WebViewNavigatorImpl.java<br>com/doximity/doximitydroid/navigation/NavTargetsKt.java<br>com/doximity/doximitydroid/navigation/NavigatorHelperImpl.java<br>com/doximity/doximitydroid/navigation/features/IntentNavigatorImpl.java<br>com/pspdfkit/internal/hf.java<br>com/pspdfkit/internal/z1.java<br>o/bk3.java<br>o/f77.java<br>o/ig8.java<br>o/m4.java<br>o/mh7.java<br>o/on1.java<br>o/pv2.java<br>o/td4.java<br>o/uxb.java<br>o/w8c.java |
| 00022 | Open a file from given absolute path of the file | file | com/bugsnag/android/NativeInterface.java<br>com/doximity/doximitydroid/core/presentation/utils/FileExporter.java<br>com/doximity/doximitydroid/platform/file/FileHelperImpl.java<br>com/pspdfkit/document/sharing/DocumentSharingProvider.java<br>com/pspdfkit/internal/b0.java<br>com/pspdfkit/internal/d8.java<br>com/pspdfkit/internal/l9.java<br>com/pspdfkit/internal/sh.java<br>com/pspdfkit/internal/th.java<br>com/pspdfkit/internal/w8.java<br>live/hms/video/diagnostics/HMSDiagnostics.java<br>live/hms/video/media/capturers/camera/CameraControl$captureImageAtMaxSupportedResolution$1.java<br>live/hms/video/utils/LogUtils.java<br>o/bv2.java<br>o/ct4.java<br>o/g22.java<br>o/i46.java<br>o/l4.java<br>o/neb.java<br>o/rr7.java<br>o/us5.java<br>o/vx2.java<br>o/ym3.java |
| 00056 | Modify voice volume | control | org/webrtc/audio/WebRtcAudioTrack.java<br>org/webrtc/voiceengine/WebRtcAudioTrack.java<br>tvi/webrtc/audio/WebRtcAudioTrack.java<br>tvi/webrtc/voiceengine/WebRtcAudioTrack.java<br>tvo/webrtc/audio/WebRtcAudioTrack.java<br>tvo/webrtc/voiceengine/WebRtcAudioTrack.java |
| 00175 | Get notification manager and cancel notifications | notification | com/doximity/doximitydroid/core/presentation/utils/systemservice/NotificationManagerWrapperImpl.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00013 | Read file and put it into a stream | file | com/bugsnag/android/RootDetector.java<br>com/cloudinary/android/AndroidJobStrategy.java<br>com/doximity/doximitydroid/core/presentation/utils/FileExporter.java<br>com/doximity/doximitydroid/core/presentation/viewpdf/RemoteDataProvider.java<br>com/doximity/doximitydroid/domain/extensions/FileExtensionsKt.java<br>com/doximity/doximitydroid/features/aiscribe/presentation/recordvisit/filerecorder/WaveHeaderWriterImpl.java<br>com/doximity/doximitydroid/repositories/FileInfoHelperImpl.java<br>com/pspdfkit/document/providers/ContentResolverDataProvider.java<br>com/pspdfkit/document/providers/InputStreamDataProvider.java<br>com/pspdfkit/internal/b9.java<br>com/pspdfkit/internal/o.java<br>com/pspdfkit/internal/th.java<br>o/aw5.java<br>o/eka.java<br>o/erb.java<br>o/gg6.java<br>o/i46.java<br>o/jg5.java<br>o/jn3.java<br>o/kd3.java<br>o/l12.java<br>o/l55.java<br>o/lv4.java<br>o/neb.java<br>o/p53.java<br>o/qg8.java<br>o/sp6.java<br>o/t7a.java<br>o/wm1.java<br>o/za2.java |
| 00102 | Set the phone speaker on | command | live/hms/video/audio/HMSAudioManagerLegacy.java<br>live/hms/video/audio/manager/AudioManagerCompat.java<br>live/hms/video/audio/manager/HMSAudioManagerApi31.java |
| 00208 | Capture the contents of the device screen | collection screen | org/webrtc/ScreenCapturerAndroid.java<br>tvi/webrtc/ScreenCapturerAndroid.java |
| 00123 | Save the response to JSON after connecting to the remote server | network command | com/pspdfkit/internal/zi.java<br>o/j39.java<br>o/l39.java |
| 00030 | Connect to the remote server through the given URL | network | o/j39.java<br>o/l39.java |
| 00014 | Read file into a stream and put it into a JSON object | file | o/gg6.java<br>o/i46.java |
| 00005 | Get absolute path of file and put it to JSON object | file | o/i46.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | com/doximity/doximitydroid/DoxAppUtilKt.java<br>com/doximity/doximitydroid/core/presentation/emailtoverify/EmailToVerifyComposablesKt$EmailToVerifyDialog$2.java<br>com/doximity/doximitydroid/core/presentation/navigation/IntentProvider.java<br>com/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/features/pushnotifications/action/PushNotificationIntentExtensionsKt.java<br>com/doximity/doximitydroid/navigation/NavTargetsKt.java<br>com/pspdfkit/internal/hf.java<br>o/pv2.java<br>o/td4.java |
| 00195 | Set the output path of the recorded file | record file | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00199 | Stop recording and release recording resources | record | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00198 | Initialize the recorder and start recording | record | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00194 | Set the audio source (MIC) and recorded file format | record | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00197 | Set the audio encoder and initialize the recorder | record | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00007 | Use absolute path of directory for the output media file path | file | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00196 | Set the recorded file format and output path | record file | live/hms/video/diagnostics/HMSDiagnostics.java |
| 00091 | Retrieve data from broadcast | collection | com/doximity/doximitydroid/core/presentation/utils/activityresults/ViewPdfContract.java<br>com/doximity/doximitydroid/features/aiscribe/presentation/recordvisit/servicerecorder/ScribeRecordingService.java<br>com/doximity/doximitydroid/features/dialer/presentation/voice/voipservice/VoipService.java<br>com/doximity/doximitydroid/features/login/launcher/IntentMatcher.java<br>o/bk3.java<br>o/p76.java |
| 00109 | Connect to a URL and get the response code | network command | com/bugsnag/android/d.java<br>com/doximity/doximitydroid/sources/rest/NetworkFileSourceImpl.java<br>com/networknt/schema/uri/URLFetcher.java<br>com/pspdfkit/internal/aj.java<br>o/do3.java<br>o/j39.java<br>o/mqa.java<br>o/qg0.java<br>o/x01.java |
| 00202 | Make a phone call | control | com/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/navigation/NavTargetsKt.java |
| 00203 | Put a phone number into an intent | control | com/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/navigation/NavTargetsKt.java |
| 00036 | Get resource file from res/raw directory | reflection | com/doximity/doximitydroid/core/presentation/utils/ContextExtensionsKt.java<br>com/doximity/doximitydroid/core/presentation/utils/StringToUriHelper.java<br>o/ig8.java<br>o/neb.java<br>o/qlc.java<br>o/td4.java |
| 00162 | Create InetSocketAddress object and connecting to it | socket | o/tea.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00163 | Create new Socket and connecting to it | socket | o/tea.java |
| 00189 | Get the content of a SMS message | sms | com/doximity/doximitydroid/core/presentation/utils/systemservice/PhoneNumberCursorHelper.java<br>o/fc2.java |
| 00188 | Get the address of a SMS message | sms | com/doximity/doximitydroid/core/presentation/utils/systemservice/PhoneNumberCursorHelper.java<br>o/fc2.java |
| 00200 | Query data from the contact list | collection contact | com/doximity/doximitydroid/core/presentation/utils/systemservice/PhoneNumberCursorHelper.java<br>o/fc2.java |
| 00187 | Query a URI and check the result | collection sms calllog calendar | com/doximity/doximitydroid/core/presentation/utils/systemservice/PhoneNumberCursorHelper.java<br>o/fc2.java<br>o/hx7.java |
| 00201 | Query data from the call log | collection calllog | com/doximity/doximitydroid/core/presentation/utils/systemservice/PhoneNumberCursorHelper.java<br>o/fc2.java |
| 00094 | Connect to a URL and read data from it | command network | com/doximity/doximitydroid/domain/util/NetworkUtils$getNetworkRoundtrip$downloadFileJob$1.java<br>o/w82.java |
| 00096 | Connect to a URL and set request method | command network | com/doximity/doximitydroid/sources/rest/NetworkFileSourceImpl.java<br>com/singular/sdk/internal/m.java<br>o/j39.java<br>o/qfa.java<br>o/x01.java |
| 00153 | Send binary data over HTTP | http | com/doximity/doximitydroid/sources/rest/NetworkFileSourceImpl.java |
| 00108 | Read the input stream from given URL | network command | o/arb.java<br>o/bic.java<br>o/gg6.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | com/bugsnag/android/d.java<br>com/networknt/schema/uri/URLFetcher.java<br>com/pspdfkit/internal/aj.java<br>o/do3.java<br>o/qfa.java<br>o/x01.java |
| 00112 | Get the date of the calendar event | collection calendar | o/ae9.java<br>o/md9.java<br>o/ng.java |
| 00192 | Get messages in the SMS inbox | sms | com/doximity/doximitydroid/repositories/FileInfoHelperImpl.java<br>com/pspdfkit/internal/th.java |
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | com/doximity/doximitydroid/repositories/FileInfoHelperImpl.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/doximity/doximitydroid/repositories/FileInfoHelperImpl.java<br>com/pspdfkit/document/providers/ContentResolverDataProvider.java<br>o/fc2.java |
| 00026 | Method reflection | reflection | o/kw7.java<br>o/ww7.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00072 | Write HTTP input stream into a file | command network file | o/gg6.java |
| 00024 | Write file after Base64 decoding | reflection file | o/gg6.java<br>o/us5.java |
| 00004 | Get filename and put it to JSON object | file collection | o/gg6.java |
| 00125 | Check if the given file path exist | file | o/wm1.java<br>o/x01.java<br>o/zz7.java |
| 00012 | Read data and put it into a buffer stream | file | com/pspdfkit/internal/th.java |
| 00023 | Start another application from current application | reflection control | com/doximity/doximitydroid/drawer/DebugDrawerViewModel.java |

## FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| App talks to a Firebase database | info | The app talks to Firebase database at https://buoyant-valve-791.firebaseio.com |
| Firebase Remote Config enabled | warning | The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/137426936544/namespaces/firebase:fetch?key=AIzaSyAH6h6scN1-7s--a3HtueWciC85Q2wr3VQ is enabled. Ensure that the configurations are not sensitiv 'android_amion_doxanalytics_send_invalid_events': 'true', 'android_amion_whos_on_survey_link': '', 'android_compose_settings': 'true', 'android_dialer_voip_pstn_fallback_max_timeout_seconds': '10', 'android_dialer_voip_pstn_fallback_thresholc ["java.net.SocketTimeoutException","java.net.UnknownHostException","kotlinx.coroutines.JobCancellationException","com.google.firebase.remoteconfig.FirebaseRemoteConfigClientException","java.lang.Exception","com.apollographql.apollo.e 'android_minimum_required_version': '82373', 'android_newsfeed_banner_background_color': '#2c90ed', 'android_newsfeed_banner_copy': 'See COVID-19 News & Resources', 'android_newsfeed_banner_enabled': 'false', 'android_newsfeed_ba 'android_sumologic_logging_config': '{"enabled":false,"logLevel":"verbose","batchSize":5}', 'dialer_video_permission_copy': 'Enable access to your camera and microphone so you can start joining video calls. \\n\\nYour calls are never recorded.', 'ios_amion_doxanalytics_send_invalid_events': 'true', 'ios_amion_survey_enabled': '0', 'ios_amion_survey_expiration': '', 'ios_amion_survey_link': '', 'ios_amion_survey_show_again': '', 'ios_amion_update_subtitle_recommended': 'Time to update! A app.', 'ios_amion_update_title_recommended': 'App Update Available', 'ios_amion_update_title_required': 'App Update Available', 'ios_amion_update_version_recommended': '6.25.0', 'ios_amion_update_version_required': '5.14.0', 'ios_dialer_vide 'ios_dialer_voip_pstn_fallback_threshold': '600', 'ios_doxanalytics_disable_analytics_ids': 'true', 'ios_doxanalytics_send_invalid_events': 'true', 'ios_doxanalytics_suppress_analytics_ids': 'true', 'ios_monitoring_app_launch': 'true', 'ios_monitoring_en 'ios_sumologic_log_category_levels': '{}', 'ios_sumologic_log_enabled': 'true', 'ios_sumologic_log_level': 'info', 'ios_update_subtitle_recommended': 'Time to update! A new version of Doximity is available. Please update now to continue using the a 'ios_update_title_required': 'App Update Required', 'ios_update_version_recommended': '16.40.0', 'ios_update_version_required': '16.40.0'}, 'state': 'UPDATE', 'templateVersion': '406'} |

## ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 12/25 | android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED |
| Other Common Permissions | 8/44 | android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.CHANGE_NETWORK_STATE |

### 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 |
|---|---|---|
| c8y.doxcdn.com | ok | **IP:** 151.101.66.104<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| push-notification-api.doximity.com | ok | **IP:** 18.238.96.95<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| www.doximity.com | ok | **IP:** 18.238.109.100<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| ta.doximity.com | ok | **IP:** 18.238.109.26<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| pspdfkit.com | ok | **IP:** 172.66.43.77<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| prod-init.100ms.live | ok | **IP:** 34.23.87.177<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Houston<br>**Latitude:** 29.941401<br>**Longitude:** -95.344498<br>**View:** Google Map |
| analytics-webhook.doximity.com | ok | **IP:** 18.238.96.111<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| xml.org | ok | **IP:** 104.239.142.8<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Windcrest<br>**Latitude:** 29.499678<br>**Longitude:** -98.399246<br>**View:** Google Map |
| ta.dogsimity.com | ok | **IP:** 18.238.96.22<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| notify.bugsnag.com | ok | **IP:** 35.186.205.6<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| dialer-api.doximity.services2 | ok | No Geolocation information available. |
| play.google.com | ok | **IP:** 172.253.124.100<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| datatracker.ietf.org | ok | **IP:** 104.16.44.99<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |
| www.w3.org | ok | **IP:** 104.18.23.19<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| sdk-api-v1.singular.net | ok | **IP:** 23.220.73.37<br>**Country:** Colombia<br>**Region:** Antioquia<br>**City:** Medellin<br>**Latitude:** 6.251840<br>**Longitude:** -75.563591<br>**View:** Google Map |
| github.com | ok | **IP:** 140.82.112.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| firebase.google.com | ok | **IP:** 74.125.136.102<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| www.twilio.com | ok | **IP:** 18.238.96.109<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| sessions.bugsnag.com | ok | **IP:** 35.190.88.7<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.android.com | ok | **IP:** 64.233.176.100<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| s.s.dox.pub | ok | No Geolocation information available. |
| developer.android.com | ok | **IP:** 64.233.176.101<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| dox.im | ok | **IP:** 52.21.33.16<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| eventgw.twilio.com | ok | **IP:** 54.157.2.94<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| www.google.com | ok | **IP:** 142.251.15.105<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| exceptions.singular.net | ok | No Geolocation information available. |
| tools.ietf.org | ok | **IP:** 104.16.45.99<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.slf4j.org | ok | **IP:** 159.100.250.151<br>**Country:** Switzerland<br>**Region:** Vaud<br>**City:** Lausanne<br>**Latitude:** 46.515999<br>**Longitude:** 6.632820<br>**View:** Google Map |
| graphql-federation.doximity.services | ok | **IP:** 18.238.109.105<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| bugsnag.com | ok | **IP:** 18.238.96.82<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| dummy-base-url.com | ok | No Geolocation information available. |
| www.apollographql.com | ok | **IP:** 3.33.186.135<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| json-schema.org | ok | **IP:** 104.26.2.209<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| event.100ms.live | ok | **IP:** 34.23.87.177<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Houston<br>**Latitude:** 29.941401<br>**Longitude:** -95.344498<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| packageinserts.bms.com | ok | **IP:** 45.60.150.161<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.606209<br>**Longitude:** -122.332069<br>**View:** Google Map |
| maps.google.co.in | ok | **IP:** 74.125.136.101<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| app-measurement.com | ok | **IP:** 64.233.177.100<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| www.abpsus.org | ok | **IP:** 107.180.97.123<br>**Country:** United States of America<br>**Region:** Arizona<br>**City:** Scottsdale<br>**Latitude:** 33.601974<br>**Longitude:** -111.887917<br>**View:** Google Map |
| whiteboard.100ms.live | ok | **IP:** 18.238.96.4<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| 100ms.live | ok | **IP:** 76.76.21.21<br>**Country:** United States of America<br>**Region:** California<br>**City:** Walnut<br>**Latitude:** 34.015400<br>**Longitude:** -117.858223<br>**View:** Google Map |
| www.youtube.com | ok | **IP:** 142.251.15.136<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| s.dogsimity.com | ok | No Geolocation information available. |
| nasa-i.akamaihd.net | ok | **IP:** 23.206.188.215<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |
| api.segment.io | ok | **IP:** 54.214.144.241<br>**Country:** United States of America<br>**Region:** Oregon<br>**City:** Portland<br>**Latitude:** 45.523449<br>**Longitude:** -122.676208<br>**View:** Google Map |
| api.100ms.live | ok | **IP:** 34.23.87.177<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Houston<br>**Latitude:** 29.941401<br>**Longitude:** -95.344498<br>**View:** Google Map |
| firebaseremoteconfigrealtime.googleapis.com | ok | **IP:** 172.217.215.95<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| doximity.onelink.me | ok | **IP:** 18.155.173.15<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| event-nonprod.100ms.live | ok | **IP:** 20.124.167.36<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Redmond<br>**Latitude:** 47.682899<br>**Longitude:** -122.120903<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| accounts.google.com | ok | **IP:** 172.217.215.84<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| firebaseinstallations.googleapis.com | ok | **IP:** 108.177.122.95<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| www.gstatic.com | ok | **IP:** 64.233.177.94<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| cdn-settings.segment.com | ok | **IP:** 18.238.93.145<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| ns.adobe.com | ok | No Geolocation information available. |
| www.dox.im | ok | No Geolocation information available. |
| dialer-api.doximity.services | ok | **IP:** 18.238.109.100<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| docs.bugsnag.com | ok | **IP:** 18.155.173.77<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| effectssdk.ai | ok | **IP:** 172.67.73.244<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| s.doximity.com | ok | No Geolocation information available. |
| ers.twilio.com | ok | **IP:** 44.193.123.32<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| auth.100ms.live | ok | **IP:** 34.23.87.177<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Houston<br>**Latitude:** 29.941401<br>**Longitude:** -95.344498<br>**View:** Google Map |
| firebase-settings.crashlytics.com | ok | **IP:** 142.250.9.94<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| purl.org | ok | **IP:** 207.241.225.157<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.781734<br>**Longitude:** -122.459435<br>**View:** Google Map |
| dynamic.doximity.services | ok | **IP:** 18.238.96.127<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| whiteboard-qa.100ms.live | ok | **IP:** 18.238.109.107<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| google.com | ok | **IP:** 142.250.9.101<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| xmlpull.org | ok | **IP:** 185.199.109.153<br>**Country:** United States of America<br>**Region:** Pennsylvania<br>**City:** California<br>**Latitude:** 40.065632<br>**Longitude:** -79.891708<br>**View:** Google Map |
| buoyant-valve-791.firebaseio.com | ok | **IP:** 35.201.97.85<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| console.firebase.google.com | ok | **IP:** 64.233.176.139<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

## EMAILS

| EMAIL | FILE |
|---|---|
| u0013android@android.com0<br>u0013android@android.com | o/ekb.java |
| doc.simity@doximity.com | com/doximity/doximitydroid/core/presentation/compose/privateLineSaring/PrivateLineSharingKt.java |
| sales@100ms.live | live/hms/video/media/streams/HMSStreamFactory.java |

| EMAIL | FILE |
|---|---|
| dialer_directory@doximity.com<br>support@doximity.com | Android String Resource |

## TRACKERS

| TRACKER | CATEGORIES | URL |
|---|---|---|
| Bugsnag | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/207 |
| Google CrashLytics | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/27 |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |
| Segment | Profiling, Analytics | https://reports.exodus-privacy.eu.org/trackers/62 |
| Singular | Analytics | https://reports.exodus-privacy.eu.org/trackers/251 |

## HARDCODED SECRETS

| POSSIBLE SECRETS |
|---|
| "article_authors" : "Authors" |
| "com.google.firebase.crashlytics.mapping_file_id" : "be8fc2b3985e45d9b78cebce6bbd710f" |
| "edit_my_profile_credential" : "Credential" |
| "firebase_database_url" : "https://buoyant-valve-791.firebaseio.com" |
| "google_api_key" : "AIzaSyAH6h6scN1-7s--a3HtueWciC85Q2wr3VQ" |
| "google_crash_reporting_api_key" : "AIzaSyAH6h6scN1-7s--a3HtueWciC85Q2wr3VQ" |
| "pspdf__document_info_author" : "Author" |
| "pspdf__note_icon_key" : "Key" |
| "pspdf__password" : "Password" |
| "settings_private_line_name" : "%s?" |
| "support_credential" : "Credential" |
| "wpn_hospital_type_private" : "Private" |

| POSSIBLE SECRETS |
|---|
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF |
| DB7C2ABF62E35E668076BEAD2088 |
| c93d80cd2b55e95dee2bebfe396d1c1e202bb62be5911d7443a17fd3f375b159 |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF |
| a63bde1d2c293be7ad1b0780b7585ea91d8c438bda1f50703231e552eb02040d |
| 0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052 |
| 36c819f35d8527ce2b20429abe33d6d17efc420ad999a9a6888c0c42c816120d |
| 0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C |
| 7b22e1fc5365f8eaa7a6bfca260369621f72013daef854a308a41cf04d87f495 |
| 496dbbc97fb2f74cb23847c0e90b58816c65d0b20e0a825734d7048f7190d1ce |
| 3acc636c5dcbe46deefad5735e8d71b2f958582fc6ddf740e6f00df146b0b5d371d7f762691ec980e76e90843c368acbeef12d622633a1c963aa070ed08ee296 |
| E95E4A5F737059DC60DFC7AD95B3D8139515620F |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF |
| 0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01 |
| e90c53986a6f70865b947e3d68cddf05966870dc8194b7e0b6e9b72af5c888c4 |
| c16c01920f484f8ff68bb3daf9fa8d9487bf8ffcdd56da2d285b7be5714b8415 |
| f00c47021a4676e086250575e8a5ac777e1b222f229f952c83365741dc330eb8 |
| 2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B |
| 74D59FF07F6B413D0EA14B344B20A2DB049B50C3 |
| bc9c62b58d097dada75516489c77d437 |
| fdf3621f38a79df3efe170035a52be2ffcf1c6144dec8d5b76e835635e65246c |

| POSSIBLE SECRETS |
|---|
| 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6 |
| 0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92 |
| FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF |
| 64033881142927202683649881450433473985931760268884941288852745803908878638612 |
| 046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C |
| 4CSnaO6O5avXkd2Nl4k8IaJFWQ2uW15oNSUBoIt9GjThpXvqrCpkeblZLnm |
| 38a72e16ec42712967248e966222aa53ae4ba7c7e691bbb9f3a4343324804c46 |
| 04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F |
| FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF |
| 2f18814376fce4b8cc9dc3d6e03a8bd5c6188828fe46b9a945ed64b49e589846 |
| bdb2837965f81d530f0b51167dc21394cae046b6b0a2e5d6bfe8da673ca1cc72 |
| 1E589A8595423412134FAA2DBDEC95C8D8675E58 |
| 0c14416e6f6e796d6f75732053656e64657220202020 |
| 04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5 |
| A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377 |
| MQVwithSHA512KDFAndSharedInfo |
| 3babbcf080a75b94217adaa8a75688ff |
| 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F |
| bc086c6e5cc7047211d16ab4204fccc8e828681b297fbf7062a29e7888eaf1a3 |
| e265f874c6e7081d1d31aad5ade81c975fe6cbbca8f2697205bb2257fd3d31cd |
| 04B8266A46C55657AC734CE38F018F2192 |

| POSSIBLE SECRETS |
|---|
| F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03 |
| db46fda78d324ca0eb7a661c97fcc4684db7c5d0879e498a63346efaebfcdac0 |
| 883423532389192164791648750360308885314476597252960362792450860609699839 |
| a4d88b4cf1a0a0b8876bb3e736c23d51fe39e04fd274cf49075281243640451c |
| c771329ef33097af47b5c43e9f59d764650635b8f7706c69167f5c6025527fcf |
| 9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511 |
| 2866537B676752636A68F56554E12640276B649EF7526267 |
| FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A |
| FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF |
| 29818893917731240733471273240314769927240550812383695689146495261604565990247 |
| 91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20 |
| 3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96 |
| 5d1f8bd7c4da0a24cde92edbb6989ab9c04203801c2794ae63bab231f3542230 |
| e5ce1de1900323944e700fdd7a13ffef434ee4a7d5a37756a7ae9eb4d97edfed |
| bb76834158a04ea327c4cd552ee5e8e96039ad6751d530c353c81b613e412929 |
| 3045AE6FC8422F64ED579528D38120EAE12196D5 |
| AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73 |
| 04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811 |
| 64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1 |
| 04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11 |
| 0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D |
| F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00 |

| POSSIBLE SECRETS |
|---|
| 5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B |
| 19285ece1dcbc48303766d15046fb6bd58404031614d449696dfdacb7133cb76 |
| cb240fe98f10936256d282fa5cdd746acf6120cac0b952639fe8ccf80c727d3b |
| 07A526C63D3E25A256A007699F5447E32AE456B50E |
| 0565318e5b1cdf6ec6d20970a322f3c534bca219cad4ced8a684eb5f25dcc0c7 |
| ee44bcbb299dbe9a0a96032aa28bdb0f022e043eda49c11ffebb13fc60df763b |
| f9623cf64aff8ea83ed35f12ed14d26cf8f77e296540f6e01fc9ef5759e63bac |
| 71baa50cb58fc3cc0af149c07374c987d5039f26f15fe2cac967f9cd655d9db2 |
| 7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4 |
| 0307AF69989546103D79329FCC3D74880F33BBE803CB |
| 04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE |
| FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF |
| 790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16 |
| 3045AE6FC8422f64ED579528D38120EAE12196D5 |
| 10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF |
| 1e850205bf93e259463e03bef048b2283133877bf0d60d06317e8f3dd33840c3 |
| 14f6408da6c51093a59a31ba43792661978dde2c4dfae98362d3528222d25666 |
| 64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1 |
| 0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D |
| 0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7 |
| FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551 |
| fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17 |
| 0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8 |
| 3a0a4f46-cf91-4784-a874-84604828dfd6 |

| POSSIBLE SECRETS |
|---|
| 00F50B028E4D696E676875615175290472783FB1 |
| ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551 |
| 678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4 |
| 0b2d1cafdc2f5a5af63d00ee0a5312004f4ac165ac5dd6b4cfa7a4cdccd07adb |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF |
| 662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04 |
| B4E134D3FB59EB8BAB57274904664D5AF50388BA |
| 3cdfdd06b5b5975c2b7c59aa572f684c32cf3a8ef6723eaee4a675ba0eac21f2 |
| 02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7 |
| 2ad5aa1c70ccd597864e8970f7e7ecdcf7c81c13a6a51a601ada8c233764198a |
| 040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883 |
| edabbb884862fe39367be3c61317c001cde0b2ccd93b485f54a62f5dac026ec4 |
| 42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a |
| 2AA058F73A0E33AB486B0F610410C53A7F132310 |
| 4099B5A457F9D69F79213D094C4BCD4D4262210B |
| 040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150 |
| 91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28 |
| A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374 |
| 7d7374168ffe3471b60a857686a19475d3bfa2ff |
| 3826F008A8C51D7B95284D9D03FF0E00CE2CD723A |
| 3f2ffe6079f99500f1a0e1d86d1f5263cd284ba2431038aaf0d9f861f4fba95f |
| 6db14acc9e21c820ff28b1d5ef5de2b0 |
| ff47eafcd47a89e27de49805918db8ace4c8240d65f4cfe65f89a33dd9540863 |

| POSSIBLE SECRETS |
|---|
| 985BD3ADBAD4D696E676875615175A21B43A97E3 |
| 048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997 |
| 3086d221a7d46bcde86c90e49284eb15 |
| dacde541b0c7549754e70113deec4682734f719e76b158bb14eb22d810f75a19 |
| 7c5aab52321c0cea90f1b79692c834f8c131155ef67ad57fb3d61f8075a78e1e |
| b8adf1378a6eb73409fa6c9c637ba7f5 |
| 9760508f15230bccb292b982a2eb840bf0581cf5 |
| AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0 |
| 91d7539f21feb67121dac2b09ab603721115e1eec016548f1e8b11b547d14775 |
| 0c27545208546aa8c310e3255b3ed1e49aa62b4ae896ca5bd5c17c71e8994a99 |
| 010092537397ECA4F6145799D62B0A19CE06FE26AD |
| 616f0555467fbb4cfe51cc677c713e438994b8c97d68a6f6908b5f1be4403d79 |
| ba3cd32f9824dfbc953b3291715505417d8d10299cbe74d8d063fbbda56af7b8 |
| 714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129 |
| FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681 |
| E95E4A5F737059DC60DF5991D45029409E60FC09 |
| 10E723AB14D696E6768756151756FEBF8FCB49A9 |
| 37588a69073a20a711172e003e28f30c106b0973b0b9c987c638cdc8d65672ad |
| 041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315 |
| 83cc16eb9b48af93c7058404103c9894aa9a3536d1a8098ceb78ccfae7b7f2e6 |
| 044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2 |
| 020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf |
| 6b8cf07d4ca75c88957d9d670591 |
| fea40ec3a6a55439a914192efc9a7a3664c7851567d4ff2a4503b2231fbd1ad0 |
| 71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8 |
| 043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9 |

| POSSIBLE SECRETS |
|---|
| c2068de253110e715e253466774b3b00a8aaaaa6986e9f8caae51a5bdedfa872 |
| 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b |
| 78848208f163b49c9d778c9bff6eb270539cf423beccec8051d32a8e3a5850b3 |
| 216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA |
| 3086d221a7d46bcde86c90e49284eb153dab |
| 668d2b8c1129769fd2f70160347636f3fe5d3091cd4088fdfa1a1f0becb76465 |
| 0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F |
| 0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9 |
| 3b6233c45d00ea00ae500efbc6b8965117ad44209e25c9be31b46b99bafe16a5 |
| 860db861cf9a69c4425fbfa193036cfcbffb9bd8e60a842d1b59d4f2ef2aaeaf |
| 5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557 |
| C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297 |
| 249eb9519c3b39a71a3e2579d960fa216b4f7ff78a4b37c203c7d6f535997f00 |
| 4D696E676875615175985BD3ADBADA21B43A97E2 |
| A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7 |
| 0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA |
| D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311 |
| 1e7511980ad7ed93ba0faa6002b7301366c032fbf11889c5b9664b6cfce4e945 |
| 020A601907B8C953CA1481EB10512F78744A3205FD |
| c06c8400-8e06-11e0-9cb6-0002a5d5c51b |
| 1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD |
| 32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C |
| d41903ef41ddfe7c63b24b90cb05fd9f25cafa98110cbd3ca7722a8f5fde20eb |
| 19fe3300584e35ba65d1478053e083e2d105bf0501cee256f49f66b2f54bea2334c79f2a2294a0e7675cdd277fe6731558b885a274d32f50c8e197517c998b0e |
| A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085 |

| POSSIBLE SECRETS |
|---|
| 71169be7330b3038edb025f1 |
| 5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B |
| 184f9f6dcde6ee722889cd9582faf4dfeb20bd7adba42be052f3c395f479927e |
| 040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259 |
| 84f2f648f91027fa6540dfc8550dd8ed421cd4d1b62eb9db6ff7d86779e53b32 |
| 00E8BEE4D3E2260744188BE0E9C723 |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF |
| 1335318132727206734338595199483190012179423759678474868994823595993696425287347124615904033277318214103280125292538719147885989931033105677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716593764268326742697808800616315281634758 87 |
| B99B99B099B323E02709A4D696E6768756151751 |
| 90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73 |
| 03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3 |
| 7d73d21f1bd82c9e5268b6dcf9fde2cb |
| 6827be1403e23bfbcc6f08696f85a17c2aabbae097447f448972904139227f8b |
| fefa368978a279cfe92a4961571bf229a254e830 |
| AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3 |
| 043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE |
| 79885141663410976897627118935756323747307951916507639758300472692338873533959 |
| d0e8add28211d26428711a408228aa09563fd0c500a7f4362c1dcc6fa225245a |
| 28792665814854611296992347458380284135028636778229113005756334730996303888124 |
| 90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D |
| f9a398231b7ce4643fd9c8ee0c543050eb1ae709a04e049b6cf52dce0d06d815 |
| 8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f |

| POSSIBLE SECRETS |
|---|
| 00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE |
| 8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065 |
| D6031998D1B3BBFEBF59CC9BBFF9AEE1 |
| 115792089237316195423570985008687907853269984665640564039457584007913129639316 |
| b3fb3400dec5c4adceb8655d4c94 |
| 0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05 |
| 48a2aaf8a26fe98273fb560c35734e8a80f70ba4f303b2c4839d103230d439a5 |
| 24B7B137C8A14D696E6768756151756FD0DA2E5C |
| cb49d0c1c3932aefa4173d6ef220feafde08e0e6d3fe79c6d0baf0c65d4bcd86 |
| F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1 |
| 030024266E4EB5106D0A964D92C4860E2671DB9B6CC5 |
| 952ff8778b33a5b425eb6e680a45df1aaa6b06f19eb191c6ceb582cec9522ae9 |
| 10B7B4D696E676875615175137C8A16FD0DA2211 |
| 3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4 |
| 9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35 |
| D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24 |
| 03F7061798EB99E238FD6F1BF95B48FEEB4854252B |
| 6b8cf07d4ca75c88957d9d67059037a4 |
| f24eea3c48d36a26bbdb17fe553a527148d1d23 |
| AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069 |
| 962eddcc369cba8ebb260ee6b6a126d9346e38c5 |
| E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B |
| 0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB |
| E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D |
| tYKlFAyaaLTL3IVwbDS1b4epBkViHGpivrp |
| 115792089237316195423570985008687907853073762908499243225378155805079068850323 |

| POSSIBLE SECRETS |
|---|
| 78d76893f03b48d36de6fc1a862f1934e236dc1c0ae1aba2d04555698f1f3be8 |
| bb85691939b869c1d087f601554b96b80cb4f55b35f433c2 |
| 06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C |
| 636e57393a8ff41eed1ef265c5152c55f9a9f10eb0a5c9498f6cd93624b5fb48 |
| 82fbd930a1000dc824d803c4cc43d0aeba199568096e5d07807bda60f127f8f7 |
| b41849820051838d078c0625bc25a7ac04c9203fafdc4a8787f1671f66f1a768 |
| d3a6984b64e7e7d30345c4c12508e678744e98c60030afc2ace37256ebfb6582 |
| cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953 |
| 401028774D7777C7B7666D1366EA432071274F89FF01E718 |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF |
| 0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892 |
| d9f5daa96284f55cac1fc0bcad0525a34c7c8d61639c79cf66147c51547ce368 |
| 044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32 |
| 09af1f41ae0546e5006361eba7cce20e9e09e94ee6695197ba0299c0270bfe2b |
| db92371d2126e9700324977504e8c90e |
| b869c82b35d70e1b1ff91b28e37a62ecdc34409b |
| 659EF8BA043916EEDE8911702B22 |
| 0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E |
| 03E5A88919D7CAFCBF415F07C2176573B2 |
| edef8ba9-79d6-4ace-a3c8-27dcd51d21ed |
| 04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3 |
| D2C0FB15760860DEF1EEF4D696E6768756151754 |
| 255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e |
| 32010857077C5431123A46B808906756F543423E8D27877578125778AC76 |

| POSSIBLE SECRETS |
|---|
| 4D41A619BCC6EADF0448FA22FAD567A9181D37389CA |
| 53a5853476f9c4f56a867a629b49670875632ec929fa2a509e84776947a12b4c |
| 0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01 |
| MQVwithSHA256KDFAndSharedInfo |
| CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D |
| 469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9 |
| a5fcef9a4748bd16685687df2725b41ff08308c5ced32fd2d1bd77475875eeea |
| aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7 |
| c8e2dec0699e636f71f100541d915806bcebef9b3efd200ceabd63ca45d549ac |
| ecadb61aa654618eb94efa94060cff56646de9ff4e788603aa7dddce7a6fb0be |
| 01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B |
| 85E25BFE5C86226CDB12016F7553F9D0E693A268 |
| 77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE |
| wN1TXjk3ypnb6dwOwiCxUz3NUEcYMwJ0 |
| 0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9 |
| 224d7a24c588f5733c114b04b24a3422c9d3132e808e4dfa3a440ed4567d8bec |
| 77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399 |
| fb445f1df71f11d351a62bb1019461f62e47cadf0436a7f9be55587331ee3aca |
| 04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD |
| BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985 |
| D09E8800291CB85396CC6717393284AAA0DA64BA |
| CluK0RF0NP0udC4rmSCkmIIVoIENtnMi3bxn8RIm2aByGDZk1yAIfS1aA6IhVrnH0Kep73BugWz9Fq6UjkhGaCO |
| 5a13027cb01398356e5e165c8d182a4bb0ca6590fae840a34249895e062e99d1 |
| 2bc528626a50b0e00e0176b9da2c081bc939bccab7055b78e1f351fe25836e83 |
| 586f04c82fdcfaa13d60f647307d736fe783c33dfa943bb5784069a7dc6d8e9f |
| 5e768221aad5d915c20f1f0a5532ddc22a572d236f6887a5f32c44f277bb854c |

| POSSIBLE SECRETS |
|---|
| 6BA06FE51464B2BD26DC57F48819BA9954667022C7D03 |
| 8d5155894229d5e689ee01e6018a237e2cae64cd |
| 520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6 |
| e43bb460f0b80cc0c0b075798e948060f8321b7d |
| 0387d3446852fffdd778c4d229a8b5e9c36080d8fe2e657a36232a39f216be54 |
| 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9 |
| 09e1674afe7f961408292b81d4c039a0a30446166517726298ec26e4ee97d31c |
| cc54c91739f825c467cf65c470efeb7a6a8f7405d6d808c320b007474a95aab4 |
| 0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928 |
| C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83 |
| 0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1 |
| 00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814 |
| 6635a5e5470d4f0305d80d8b5973097683a970b5c313f9cb15c9df7c5f940436 |
| 00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9 |
| 45626249a8d9380499dffd753b53c11d1e232115b8bcf4f9879dea4df1a892be |
| 023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd |
| 801ae0963ea59c4d02ed0969d78788307aa164495d277426ea4537b54e29aa4c |
| 517cc1b727220a94fe13abe8fa9a6ee0 |
| 7A1F6653786A68192803910A3D30B2A2018B21CD54 |
| 31422cfdb99314e040b2501479e51e8e869589b235b9cf24ee3ed2f0e0df9874 |
| FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF |
| a4158444d48954a215718b18b155f4efbc0e1d8c18cdc8797dae39b4eb846631 |
| 70390085352083305199547718019018437840920882647164081035322601458352298396601 |

| POSSIBLE SECRETS |
|---|
| 1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10 |
| fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7 |
| f1f2f1d422952320e9acd27271b3ddc59d31ef1e93e7837b15e708c15d982eff |
| f8568cf32c3bc00b9168520b76633c216ff55ea8d03afde848ab2330bf4dd98b |
| ebfc166fcdca2b1b9af11ab413e5941214b59d45c4f7e7776efd7020bfa82f5a |
| 4d9749648484dfc5f9e426b0882bcf3059f5177694960514bb2e230758d4651b |
| 05e37b8a3d8177ec790b0691f233016cc5adca8bfe1cde48a6b8c47c230030d8 |
| 95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b |
| a6f1d83d1b0c3a816dc976e774caf15ca828caccfdff5d1dd0ec0666560c4e26 |
| 36cc47f4905176232782ffa54e27b28238354dc1ec4d1ee412ee896232e6987a |
| 0217C05610884B63B9C6C7291678F9D341 |
| b0957898901f5f222ed443c35480a48a6a487762839eac066996fc5ee7e70c63 |
| fa5855c70a47163235ca3aa8cf9031e599e36c4fd77db763420b69d656dd8d26 |
| 6C01074756099122221056911C77D77E77A777E7E7E77FCB |
| 021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F |
| 115792089210356248762697446949407573530086143415290314195533631308867097853951 |
| c85ffea02a59fd566460d2d936f0cd27c886203e2b222d39eadaff6d709bd9be |
| D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF |
| 04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB |
| 3adfdf7ff4e200a6aaad8e4e87c39bfcec3d8202dbf15303186e2e77db271e0c |
| 4A6E0856526436F2F88DD07A341E32D04184572BEB710 |
| 03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a |
| 7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE |
| 7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063 |

| POSSIBLE SECRETS |
|---|
| ea943bf5318e5ec214ef4ebf5dcb2f2cc6d71036d0e4bfdf5feaab922bbd4aa0 |
| 30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252 |
| 0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00 |
| C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E |
| 10456c4e90b3c13c13ba802653bf59ea1403181f6b504978a254ed12815a8fac |
| BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F |
| 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 |
| 0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD |
| 2eccc0880dbb5f5408cb4e8963151e3972c9f2419e358fbd784c247d5305024f |
| 295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513 |
| 0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91 |
| 5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0 |
| 040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B |
| 1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63 |
| 0095E9A9EC9B297BD4BF36E059184F |
| 1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D |
| 054aae5d4d370f00561f8f871312fdc0e75f2ec115649900e19cd38799961aec |
| 7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380 |
| 3076087afa4f50157533e888bc9da48f20607f368d82079579559d280df08dd4 |
| 28091019353058090096996979000309560759124368558014865957655842872397301267595 |
| 28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93 |
| 25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E |
| 43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136 |
| 115792089237316195423570985008687907853269984665640564039457584007913129639319 |
| 7546d31d6cb96e840a108884bb1171d3a54659a8a02ad826a57abeac67351f71 |

| POSSIBLE SECRETS |
|---|
| 5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72 |
| EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3 |
| 7c3e62b94753075f5b6f7b6969c01f3abadb9059ca7210acd0eea705ffdaa46a |
| a70a5e1e3fb851e027a15c3d15a48df9d33ffa1224df828a90bbcae29995c928 |
| 7dbc5240d413e4a782d818647d7eecf2de9bcf707b07e548f7dd484623499dac |
| 0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D |
| 91771529896554605945588149018382750217296858393520724172743325725474374979801 |
| 96341f1138933bc2f503fd44 |
| 14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224192907104613420838063639408451269182889400057152462544529576934935675272895683154177544176313938445719175509684710784659566254794231229333848392451433961472776068188060973 4239 |
| A335926AA319A27A1D00896A6773A4827ACDAC73 |
| 1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10 |
| 0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500 |
| 2100592ecc8ec8cfb56a8a06742cfbba547e476e7c90d81338ee49777a748b90 |
| 6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a |
| c469684435deb378c4b65ca9591e2a5763059a2e |
| 340E7BE2A280EB74E2BE61BADA745D97E8F7C300 |
| 70466d3d2dd8528214878f1fded79bb1845300143b36fdc3591cb71faaa69ec0 |
| 68363196144955700784444165611827252895102170888761442055095051287550314083023 |
| 7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E |
| 0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205 |
| 040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B |
| 000E0D4D696E6768756151750CC03A4473D03679 |
| 470fa2b4ae81cd56ecbcda9735803434cec591fa |
| F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F |
| 7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA |

| POSSIBLE SECRETS |
|---|
| 3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1 |
| 2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE |
| 25066fad6ee4ab10a719936146fa72932b015837c675e233e741a386e30f1ddb |
| 45fd528aea2f060977c0875851b692af15ecef1780164cdba5cbbd931a80979c |
| DUayto8uYanqsu5DkiDgk06V042KDMgWK53ll3zAweHqFv9SmTOUywDJMXyzCL64MiTnJaTIdy1Q8fEkr3tcN |
| 6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF |
| 42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341 |
| feb6a325b47db5434570971ec30ad9b2fb08a5fbeae08885870b040e805b9c93 |
| 114ca50f7a8e2f3f657c1108d9d44cfd8 |
| c1c2b4e4b5869fea095bd6bc0cd971676890a55fa1dd45c6d2a7a87fa11ba89c |
| 04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886 |
| DB7C2ABF62E35E7628DFAC6561C5 |
| 4b1c06c35b5626329d143612ee56a49d2142f8b34b1512e2fa2892944583674e |
| e5cf2a03c808d285445118e4701eb95611e657c5b8308eb4e5d3635e78ab4f89 |
| 07A11B09A76B562144418FF3FF8C2570B8 |
| 1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F |
| 13612003a82e58db22a8516b14d9ea6b22cb72bd061a83cf0847450c243fc0ba |
| MQVwithSHA384KDFAndSharedInfo |
| 072546B5435234A422E0789675F432C89435DE5242 |
| 0f46e4f15be8358f5f602b5ad5f6c32276c818aae80d14bf7a71349a7c2c0573 |
| 047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44 |
| E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148 |
| 0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0 |
| 22123dc2395a05caa7423daeccc94760a7d462256bd56916 |
| 10ba4b6d84ca343a945e77d93c69827f3f44200b1153b0b217c986c4274fec34 |

| POSSIBLE SECRETS |
|---|
| 9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB |
| 04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34 |
| 108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9 |
| 0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B |
| 03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012 |
| 57896044618658097711785492504343953927102133160255826820068844496087732066703 |
| 1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1 |
| 855ba3475756f95126b480937b9cdd4b |
| 04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332 |
| 097753bff3a99f9ada9a11eb5fd9608a6891b821ea3b07033455ed86c4a58b42 |
| 04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83 |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF |
| DB7C2ABF62E35E668076BEAD208B |
| 0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D |
| 12511cfe811d0f4e6bc688b4d |
| 002757A1114D696E6768756151755316C05E0BD4 |
| 56804144644816895d39b0074ad2227b41a03a8063738f2ea7c9d5456c90944e |
| C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294 |
| bb392ec0-8d4d-11e0-a896-0002a5d5c51b |
| 100997906755055304772081815535925224869841082572053457874823515875577147990529272777244152852699298796483356699682842027972896052747173175480590485607134746852141928680912561502802222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588322876850946740663962 |
| rJEnSQQDVG19Cf1fTnYan0GTAu0Rd67lFein5NaN3mjhjzIdIse4q0WvqGOKGNPqLRc0knP |
| 7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03 |
| bb193617a88ba8be6ba2f6c24d1f82d4441cdf853d046771fa859a0488f5f8db |
| 31a92ee2029fd10d901b113e990710f0d21ac6b6 |

| POSSIBLE SECRETS |
|---|
| 027d29778100c65a1da1783716588dce2b8b4aee8e228f1896 |
| 57896044618658097711785492504343953926634992332820282019728792003956564823190 |
| 24f3a7c3f516e2ea0c0103ee94992692ea7d620dc78bae6cd4ea8bb1530040ab |
| 7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826 |
| 7aabbe50c5bd0e2d6e5705d37de17a2f954ef0bc0ed426104309f9574e7059e5 |
| 05bff4866d59914c78a3c633ea68288fb7efcc93bb79af10222720cb170b133d |
| 04747af1821ee35534d31ee894c8c8a39232da71a45029aac80f3f9147d51816 |
| EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F |
| 010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967 |
| B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4 |
| 29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA |
| DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3 |
| 0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D |
| 127971af8721782ecffa3 |
| 036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 |
| 60142ce02815e8b73d3864f26dab84475665ee7c246891196547ae18acb3c052 |
| c4a157a24273b0c8984775dec99a95d391b1b434e6605e0888771be674b934a1 |
| 68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43 |
| 04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D |
| 5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B |
| 01762dfb38e8b58ffb134f4ab734792bda6a2b83421d10b191228924d5978fee |
| 7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864 |
| 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 |
| 13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79 |
| 51DEF1815DB5ED74FCC34C85D709 |
| b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046 |

| POSSIBLE SECRETS |
|---|
| c4545c13db0baa2479c54089fb6d06a0c23abc0eb80032d5ec72388229fcfd11 |
| 878376def7cb80c746e33bad262572bde2938d1a6e2d6caefe2353c10ca02ecd |
| 1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de |
| 5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2 |
| B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1 |
| 5FF6108462A2DC8210AB403925E638A19C1455D21 |
| 03375D4CE24FDE434489DE8746E71786015009E66E38A926DD |
| 7fe074842e381ed7d421dd999d8417bd1ddc7615cb5fc5776158f49d6c7fba22 |
| 0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A |
| 3dbc95eac62200be274e8a12cadee1f18a9d4918da134ec084df9561e5347a14 |
| 5c8150a0c78266400be395df0b43af8ea9cc2243a5dbff03419b4b4a24fa4c38 |
| D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27 |
| 7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee |
| 003088250CA6E7C7FE649CE85820F7 |
| FFFFFFFE0000000075A30D1B9038A115 |
| 040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD |
| 9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a |
| 5EEEFCA380D02919DC2C6558BB6D8A5D |
| 04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3 |
| 04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F |
| E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760 |
| 10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618 |
| 04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706 |
| dea6e847834f0a8468097e8d4d36b36b |
| 5F49EB26781C0EC6B8909156D98ED435E45FD59918 |
| C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335 |

| POSSIBLE SECRETS |
|---|
| doTtTzk989l9it5mPJjssPJRxfb6N18ktxwBqcwxp4buYzpcx9zbZyGFfrUSU7y |
| c49d360886e704936a6678e1139d26b7819f7e90 |
| 71169be7330b3038edb025f1d0f9 |
| 10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1 |
| 3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723 |
| fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768 |
| 5e5f135ca201bc1bac4012d6ca3d1e5ad10bf7cf3f312bccee90146d534e9bb6 |
| 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565 |
| 7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7 |
| 023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10 |
| 687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116 |
| 1243ae1b4d71613bc9f780a03690e |
| 02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614 |
| 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50 |
| GsYP8FsePiKha2zmDFRr4QDRgK2S1TtAQU |
| f66ae253587157fd7b9d23914b80111ed49e3c3ea1246901bdbe4038e31bcd93 |
| 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5 |
| 044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97 |
| 04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321 |
| 2b8cdefc85f33d823242d9668d8bb3f6e4e8a1b1f31f8cfe0ed5fc7855cbe542 |
| 6EE3CEEB230811759F20518A0930F1A4315A827DAC |
| 57896044618658097711785492504343953926634992332820282019728792003956564823193 |
| 9162fbe73984472a0a9d0590 |
| 1c3deb5e936ed1d5d54ca4bc0368328ea8e3f491c598f93fbfa3930af1080fb3 |
| 393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB |
| 68b989a18df1356af0d85bff07c0cf7b |

| POSSIBLE SECRETS |
|---|
| 34328f9919feb141805ed24bddf3b96854485e6288ef0c52a4690ef96ee5f3d1 |
| 324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1 |
| 02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A |
| a9c97eecae7a0f72c3af19fce53163c2251803fafbfdb810cd459bd583d2021f |
| 004D696E67687561517512D8F03431FCE63B88F4 |
| f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a |
| e8b4011604095303ca3b8099982be09fcb9ae616 |
| 93772fe5b00981eeebfd8dd779791f46 |
| 102614ac1795ea2cde56427a151654a4f17cfbffd498f320675881e4660acfc9 |
| B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF |
| 033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097 |
| 0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650 |
| 2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC |
| BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677 |
| 046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5 |
| 6127C24C05F38A0AAAF65C0EF02C |
| 0667ACEB38AF4E488C407433FFAE4F1C811638DF20 |
| 038D16C2866798B600F9F08BB4A8E860F3298CE04A5798 |
| 07B6882CAAEFA84F9554FF8428BD88E246D2782AE2 |
| BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5 |
| 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 |
| b567c03de48c828b4b5ff302f078e9bb4c7b4e8b7fd12f5b0758c9e45409d000 |
| 4E13CA542744D696E67687561517552F279A8C84 |
| f38c0d2f7ce8cecc5118c12d311fa0561e3efb90a824fa724d33ede2c905f432 |
| 2b65bdb8dfa526ba125243c612a938987ec7c9682b8cc2802644127fff35ecfd |

| POSSIBLE SECRETS |
|---|
| c5ee0a3120459d34fe7b923297d77ba99c1104847709a26cd15d3cfdfd1d9f50 |
| C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1 |
| 70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9 |
| 027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5 |
| 4435325af94e43c617a87bdf040697a96a7c08c1d07aa3af2f10ef55966e22e5 |
| 10C0FB15760860DEF1EEF4D696E676875615175D |
| 103FAEC74D696E676875615175777FC5B191EF30 |
| 356e4a21530b2975a5e43ebcfbd41316 |
| c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192 |
| 79774aacb4be40276edbf97d6d4d4126d03ad7c7891266c32150dd4a44b8f35e |
| c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 |
| 4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D |
| 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f |
| c79084e18dd0dd32f4bd996f24dbe89fddca36379afc44ca41dc22e9baa774b9 |
| 1053CDE42C14D696E67687561517533BF3F83345 |
| b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536 |
| C49D360886E704936A6678E1139D26B7819F7E90 |
| D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC |
| 0c9fdb0669af63db5e89a499c4476b2bcf964b9853d91b2fc6a15b81a8fe021c |
| D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F |
| e4437ed6010e88286f547fa90abfe4c42212 |
| 02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7 |
| 0108B39E77C4B108BED981ED0E890E117C511CF072 |
| 0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4 |
| BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE |
| 3071c8717539de5d5353f4c8cd59a032 |

| POSSIBLE SECRETS |
|---|
| 026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D |
| 7039008535208330519954771801901843784107951663004518047128434684370563350261 9 |
| 0103eb3d541dc5905bffc6434ed7fdf6b915b9197fc707f820dbd4ee267e2760 |
| b273e866f9761df3894f12e1aef4df1a373936d535dbb5424a9d212f679b336d |
| e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf |
| e4c8306707738a8a9ba160f96acdd2d711373db457bf9554679c70fd3473f9b7 |
| 0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1 |
| 0e60f70668ffc0b1ad685ea901c24dec11165eb49411abf7554abeed80e4171d |
| E87579C11079F43DD824993C2CEE5ED3 |
| dd36722d88cc219805fa27611e5cef870bafa869cad64f21ee44b3b13d017901 |
| 54d39c275bee9f6ec000c501e8e3218f78a0418191861a6125a62422ac813b6f |
| 36DF0AAFD8B8D7597CA10520D04B |
| 12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499672425412104927434935707492031276956145168922411057931124881261022967853463840169352001328899500036222606842227508135323070045173416336850045410625869714168836867788425378 20383 |
| 5e7a9cf81bb2f6ce5ec2ee3728d4324f4eda4018163d71fac3b3dd26193ed19b |
| 13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732267216074074777170091113455043205380464769490468612011308781624074018480047704715733666292624942357124882396854222175366014339148568084052033685945849480318734128858048 9525163 |
| 00689918DBEC7E5A0DD6DFC0AA55C7 |
| 036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a |
| 5a0339dc9bc980ac2acc3b18fe1119ade4d51d600b2d5d7ab47362f94e99ebb4 |
| f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773 |
| e895397b4aa2e6ac985aee8fc6015edef12fcab4c6aab7c664e5a12c66f5aef8 |
| 89057c2de58a945d50580469ecd409e4 |
| 8fbba13c088325345586a26b866377f61d910c9ccb12929c866026832182ec33 |
| d2361f0794dba1962c8c0aa9df81a946e054 |
| d1f34245ee4d36541ba7cbb6493a12be3462ec5b5db4a2a19bf3ae267725a6f9 |
| 5eac10beaa28aed8ecdd1cff14e8b87194ebae56143f38d5c3d9a6c99e25ea38 |

| POSSIBLE SECRETS |
|---|
| 6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40 |
| A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353 |
| 50dbb872111a39c5b70be245e7eafa62655039b77076b08b05fd0b295ca7ad7c |
| 04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3 |
| 60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788 |
| 1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45 |
| 0a0e9f8bf9206d5730d4bf6fc2d5deaba3e7ff3d39c1e4b7cf25b51fff91da56 |
| 2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988 |
| ef395360c645fa1c1e9a61c42fca57f254eb303c96797a3895e215275097bb00 |
| E95E4A5F737059DC60DFC7AD95B3D8139515620C |
| 617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c |
| 2bQYeCOHhmdDO4a3dIu0e20fPU6KyVzX2U1ZNHEy2jGVnWh8u4D |
| 0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521 |
| 70390085352083305199547718019018437841079516630045180471284346843705633502616 |
| FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF |
| 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53 |
| 1932c9455a5f36eaa81718b2b6b84b774fe345d77d0e2e23f1b38577cb488361 |
| 03b2f54434820b6de82c7d33c64b40c1ec3a914fab47032550b7e1431e427bfd |
| 4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F |
| c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4 |
| 040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F |

## PLAYSTORE INFORMATION

**Title:** Doximity - Medical Network

**Score:** 4.773639 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.doximity.doximitydroid

**Developer Details:** Doximity, Inc., 6583053408641093772, None, http://www.doximity.com, support@doximity.com,

**Release Date:** Feb 18, 2011 **Privacy Policy:** Privacy link

**Description:**

All healthcare professionals can use Dialer in the Doximity app. Info on how to setup: https://blog.doximity.com Doximity helps over 1 million healthcare professionals take the friction out of everyday challenges that are unique to clinicians. The tools you already use, conveniently in one place and designed to make your life a little bit easier. Features: - Free, secure and simple telemedicine tools - Call patients without using *67 - Voice call, video call or go straight to voicemail - Keep up with the latest clinical news in your specialty. - Quickly look up office info for any other physicians, NP, PA or pharmacist - Find clinicians based on specialty, location and clinical interests - Send HIPAA secure faxes from anywhere. Sign, date and annotate documents. - Reconnect with former medical school classmates, co-residents, co-fellows or colleagues

## SCAN LOGS

| Timestamp | Event | Error |
|---|---|---|
| 2025-08-29 21:46:57 | Generating Hashes | OK |
| 2025-08-29 21:46:57 | Extracting APK | OK |
| 2025-08-29 21:46:57 | Unzipping | OK |
| 2025-08-29 21:46:57 | Parsing APK with androguard | OK |
| 2025-08-29 21:46:58 | Extracting APK features using aapt/aapt2 | OK |
| 2025-08-29 21:46:58 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-08-29 21:47:00 | Parsing AndroidManifest.xml | OK |
| 2025-08-29 21:47:00 | Extracting Manifest Data | OK |
| 2025-08-29 21:47:00 | Manifest Analysis Started | OK |
| 2025-08-29 21:47:00 | Reading Network Security config from network_security_config.xml | OK |
| 2025-08-29 21:47:00 | Parsing Network Security config | OK |

| | | |
|---|---|---|
| 2025-08-29 21:47:00 | Performing Static Analysis on: Doximity (com.doximity.doximitydroid) | OK |
| 2025-08-29 21:47:01 | Fetching Details from Play Store: com.doximity.doximitydroid | OK |
| 2025-08-29 21:47:01 | Checking for Malware Permissions | OK |
| 2025-08-29 21:47:01 | Fetching icon path | OK |
| 2025-08-29 21:47:01 | Library Binary Analysis Started | OK |
| 2025-08-29 21:47:01 | Reading Code Signing Certificate | OK |
| 2025-08-29 21:47:02 | Running APKiD 2.1.5 | OK |
| 2025-08-29 21:47:13 | Detecting Trackers | OK |
| 2025-08-29 21:47:22 | Decompiling APK to Java with JADX | OK |
| 2025-08-29 21:48:01 | Converting DEX to Smali | OK |
| 2025-08-29 21:48:01 | Code Analysis Started on - java_source | OK |
| 2025-08-29 21:48:14 | Android SBOM Analysis Completed | OK |
| 2025-08-29 21:48:39 | Android SAST Completed | OK |
| 2025-08-29 21:48:39 | Android API Analysis Started | OK |
| 2025-08-29 21:49:05 | Android API Analysis Completed | OK |
| 2025-08-29 21:49:05 | Android Permission Mapping Started | OK |
| 2025-08-29 21:49:46 | Android Permission Mapping Completed | OK |

| | | |
|---|---|---|
| 2025-08-29 21:49:47 | Android Behaviour Analysis Started | OK |
| 2025-08-29 21:50:17 | Android Behaviour Analysis Completed | OK |
| 2025-08-29 21:50:17 | Extracting Emails and URLs from Source Code | OK |
| 2025-08-29 21:50:41 | Email and URL Extraction Completed | OK |
| 2025-08-29 21:50:41 | Extracting String data from APK | OK |
| 2025-08-29 21:50:41 | Extracting String data from Code | OK |
| 2025-08-29 21:50:41 | Extracting String values and entropies from Code | OK |
| 2025-08-29 21:50:58 | Performing Malware check on extracted domains | OK |
| 2025-08-29 21:51:04 | 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.