MOBSF

ANDROID STATIC ANALYSIS REPORT

Lime (3.236.1)

File Name:	Lime_-_RideGreen_3.236.1_APKPure.xapk
Package Name:	com.limebike
Scan Date:	Nov. 3, 2025, 2:01 a.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	35	4	3	2

FILE INFORMATION

File Name: Lime_-_RideGreen_3.236.1_APKPure.xapk
Size: 35.28MB
MD5: c9120aa06711205e27c46687d7a41e55
SHA1: 3a904b0f259a0afb06431342d474f3b4d0ea1bb1
SHA256: c096a12ddaec0d880f47ed040ca0cf718fd37d2caf5a2488f475de2037441fb1

APP INFORMATION

App Name: Lime
Package Name: com.limebike
Main Activity: com.limebike.launcher.LauncherActivity
Target SDK: 35
Min SDK: 28
Max SDK:
Android Version Name: 3.236.1

Android Version Code: 3236001

APP COMPONENTS

Activities: 82
Services: 22
Receivers: 16
Providers: 12
Exported Activities: 14
Exported Services: 3
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Mateo, O=LimeBike, OU=Mobile Development, CN=Lime Bike
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-02-11 20:19:24+00:00
Valid To: 2042-02-05 20:19:24+00:00
Issuer: C=US, ST=California, L=San Mateo, O=LimeBike, OU=Mobile Development, CN=Lime Bike
Serial Number: 0x277fddc5
Hash Algorithm: sha256
md5: df50d600721814a052b050728c3d3ac1
sha1: 2cc457a9ba36ef04a34b479dd18593c6b57347de
sha256: 547d3283ade8e9fe50ab804d48a9289871baadba912ff422dec0492d8567be48
sha512: 771a13ae508b553d96a8b2d028b6578fc8dc9fe382bcdcdd2b92cf06578e3ce04d9283dbc92eaa538c3a67cb6145fa2489804d253cc25f555bd4e3a0b2610d12
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a5411954ba944c5b45ef11f0dbe26bf205f1d80a7df95ab2f82802797dd44b28
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.limebike.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
subscriber ID check
emulator file check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check device ID check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes5.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes6.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes7.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check</td></tr><tr><td>Obfuscator</td><td>Allatori demo</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.limebike.rider.RiderActivity	Schemes: adyencheckout://, elements://, Hosts: com.limebike,

ACTIVITY	INTENT
com.limebike.launcher.LauncherActivity	Schemes: http://, https://, limebike://, Hosts: lime.bike, limebike.app.link, limebike-alternate.app.link, limebike.page.link, limebikealternate.page.link,
com.limebike.payment.paypal.PayPalWrapperActivity	Schemes: com.limebike.braintree://,
io.primer.android.ui.deeplink.async.AsyncPaymentMethodDeeplinkActivity	Schemes: primer://, Hosts: requestor.com.limebike, Path Prefixes: /async,
io.primer.android.components.ui.activity.HeadlessActivity	Schemes: primer://, Hosts: requestor.com.limebike, Path Prefixes: /paypal,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.limebike,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.limebike,
com.stripe.android.financialconnections.lite.FinancialConnectionsSheetLiteRedirectActivity	Schemes: stripe://, Hosts: financial-connections-lite, Path Prefixes: /com.limebike/auth_redirect,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 25 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.limebike.rider.RiderActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	App Link assetlinks.json file not found [android:name=com.limebike.launcher.LauncherActivity] [android:host=https://limebike.page.link]	high	App Link asset verification URL (https://limebike.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
5	App Link assetlinks.json file not found [android:name=com.limebike.launcher.LauncherActivity] [android:host=https://limebikealternate.page.link]	high	App Link asset verification URL (https://limebikealternate.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (com.limebike.util.backgroundservice.LimeBikeFirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.braze.BrazeBootReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.limebike.util.CustomBrazeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.limebike.util.backgroundservice.LoginSmsBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Activity (com.limebike.personaidscan.PersonaWrapperActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Activity (com.limebike.payment.paypal.PayPalWrapperActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (io.primer.android.CheckoutSheetActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (io.primer.android.ui.deeplink.async.AsyncPaymentMethodDeeplinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (io.primer.android.threeds.ui.ThreeDsActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Activity (io.primer.android.components.ui.activity.HeadlessActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
18	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	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.
19	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
20	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
22	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
23	Activity (com.stripe.android.financialconnections.lite.FinancialConnectionsSheetLiteRedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
24	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
25	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
26	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
27	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
28	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				adyen/com/adyencse/pojo/Card.java com/adyen/checkout/core/log/Logger.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/api/AmplitudeLog.java com/amplitude/api/DatabaseHelper.java com/amplitude/api/Identify.java com/amplitude/api/IngestionMetadata.java com/amplitude/api/Plan.java com/amplitude/api/Revenue.java com/amplitude/api/TrackingOptions.java com/amplitude/api/Utils.java com/braintreepayments/api/BrowserSwitchPersistentStore.java com/braze/support/BrazeLogger.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_rec

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	ycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTar

NO	ISSUE	SEVERITY	STANDARDS	FILES
	information should never be logged.	info	into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/datadog/android/ndk/internal/NdkCrashLog.java com/datadog/android/rum/DdRumContentProvider.java com/jakewharton/disklrucache/DiskLruCache.java com/kount/api/CollectorTaskBase.java com/kount/api/DataCollector.java com/limebike/endtriparcore/common/rendering/ShaderUtil.java com/polidea/rxandroidble3/ClientComponent.java com/polidea/rxandroidble3/internal/QueueOperation.java com/polidea/rxandroidble3/internal/serialization/ClientOperationQueueImpl.java com/polidea/rxandroidble3/internal/util/CharacteristicPropertiesParser.java com/polidea/rxandroidble3/internal/util/ScanRecordParser.java com/snowballtech/logan/Logan.java com/snowballtech/transit/rta/api/ErrorLog.java com/stripe/android/camera/DefaultCameraErrorListener.java com/stripe/android/camera/framework/image/ImageKt.java com/stripe/android/camera/framework/imag

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e/NV21ImageKt.java com/stripe/android/camera/scanui/ScanErrorListener.java com/stripe/android/core/Logger.java com/stripe/android/core/storage/SharedPreferencesStorage.java com/stripe/android/core/utils/PluginDetector.java com/stripe/android/stripe3ds2/transaction/Logger.java com/stripe/android/stripecardscan/framework/time/LoggingTimer.java com/stripe/hcaptcha/webview/HCaptchaWebView.java dagger/android/AndroidInjection.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.java io/noties/markwon/LinkResolverDef.java io/noties/markwon/PrecomputedTextSetterCompat.java io/primer/android/internal/zp.java lib/android/paypal/com/magnessdk/o/a.java org/koin/android/logger/AndroidLogger.java org/tensorflow/lite/support/image/TensorBufferContainer.java org/tensorflow/lite/support/model/GpuDelegateProxy.java org/tensorflow/lite/task/core/BaseTaskApi.java org/tensorflow/lite/task/core/TaskJniUtils.java timber/log/Timber.java
				coil/memory/MemoryCache.java coil/request/Parameters.java com/adyen/checkout/base/analytics/AnalyticEvent.java com/adyen/checkout/base/model/paymentmethods/InputDetail.java com/braintreepayments/api/BraintreeError.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va com/braintreepayments/api/ErrorWithResponse.java com/braintreepayments/api/PayPalAccountNonce.java com/braintreepayments/api/PayPalCreditFinancing.java com/braintreepayments/api/PayPalCreditFinancingAmount.java com/braintreepayments/api/PayPalLineItem.java com/braintreepayments/api/PayPalRequest.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/android/rum/internal/domain/scope/RumViewInfo.java com/datadog/legacy/trace/api/Config.java com/datadog/trace/api/ConfigSetting.java com/limebike/network/model/request/LoginRequest.java com/limebike/network/model/request/SignupRequest.java com/limebike/network/model/request/UnlockRequest.java com/limebike/network/model/request/UserInteractionsRequest.java com/limebike/network/model/request/v2/reserve/ReserveRequest.java com/limebike/network/model/response/AddBalanceResponse.java com/limebike/network/model/response/Cont

NO	ISSUE	SEVERITY	STANDARDS	FILES
				actAvailabilityResponse.java com/limebike/network/model/response/OrderReceiptResponse.java com/limebike/network/model/response/SetupIntentFromPaymentMethodResponse.java com/limebike/network/model/response/inner/PaymentMethod.java com/limebike/network/model/response/inner/Trip.java com/limebike/network/model/response/inner/TripReceiptItem.java com/limebike/network/model/response/juicer/servey/JuicerCancelTaskReason.java com/limebike/network/model/response/stepsdata/start/AuthNextActionStepData.java com/limebike/network/model/response/v2/rider/map/ParkingPinsMetaResponse.java com/limebike/rider/summary/adapter/LineItem.java com/limebike/rider/summary/common/OrderLineItem.java com/limebike/supreme/ui/widgets/lazy/list/SupremeListItem.java com/statsig/androidsdk/Marker.java com/statsig/androidsdk/StatsigClientKt.java com/statsig/androidsdk/StatsigOptionsKt.java com/statsig/androidsdk/StoreKt.java com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java com/stripe/android/common/model/CommonConfiguration.java com/stripe/android/core/injection/InjectorKt.java com/stripe/android/core/injection/NamedConstantsKt.java com/stripe/android/core/networking/AnalyticsFields.java com/stripe/android/core/networking/NetworkConstantsKt.java com/stripe/android/core/networking/SendAn
2	Files may contain hardcoded sensitive information like usernames,	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering	

NO	ISSUE	SEVERITY	STANDARDS	FILES
	passwords, keys etc.		OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	alyticsRequestV2WorkerKt.java com/stripe/android/customersheet/CustomerSheetContractKt.java com/stripe/android/customersheet/data/CustomerSessionElementsSession.java com/stripe/android/financialconnections/FinancialConnectionsSheetConfiguration.java com/stripe/android/link/LinkConfiguration.java com/stripe/android/link/model/LinkAccount.java com/stripe/android/model/AttachConsumerToLinkAccountSession.java com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/LinkAccountSession.java com/stripe/android/model/PassiveCaptchaParams.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/RadarSessionWithHCaptcha.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/parsers/EphemeralKeyJsonParser.java com/stripe/android/model/parsers/FinancialConnectionsSessionJsonParser.java com/stripe/android/model/parsers/LinkAccountSessionJsonParser.java com/stripe/android/model/parsers/RadarSessionWithHCaptchaJsonParser.java com/stripe/android/paymentelement/confirmation/cpms/CustomPaymentMethodProxyA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ctivity.java com/stripe/android/paymentelement/embedded/content/SheetStateHolder.java com/stripe/android/payments/bankaccount/ui/CollectBankAccountViewEffect.java com/stripe/android/paymentsheet/ExternalPaymentMethodProxyActivity.java com/stripe/android/paymentsheet/addresselement/AddressDetails.java com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract.java com/stripe/android/paymentsheet/addresselement/AddressElementNavigator.java com/stripe/android/paymentsheet/repositories/CustomerRepository.java com/stripe/android/polling/IntentStatusPoller.java com/stripe/android/shoppay/ShopPayActivityContract.java com/stripe/android/shoppay/bridge/ShopPayInitParamsResponse.java com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/transaction/IntentData.java com/stripe/android/stripecardscan/cardscan/CardScanFragmentKt.java com/stripe/android/uicore/elements/AddressInputMode.java com/withpersona/sdk2/inquiry/governmentid/GovernmentId.java com/withpersona/sdk2/inquiry/governmentid/IdConfig.java com/withpersona/sdk2/inquiry/nfc/PassportNfcReaderConfig.java io/primer/android/internal/cg1.java io/primer/android/internal/ip.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/primer/android/internal/nn1.java io/primer/android/internal/qm1.java io/primer/android/internal/qn1.java io/primer/android/internal/zk1.java io/primer/android/internal/zm0.java org/jctools/maps/NonBlockingHashMap.java org/jctools/maps/NonBlockingIdentityHashMap.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/d60.java bo/app/i80.java bo/app/mq.java bo/app/mt.java bo/app/q.java com/skydoves/balloon/BalloonPersistence.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/limebike/util/DiskBitmapCache.java com/limebike/util/OpenFileHelper.java lib/android/paypal/com/magnessdk/n/a.java
5	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/amplitude/eventexplorer/EventExplorerInfoActivity.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/Curve.java com/stripe/android/stripecardscan/payment/ml/SSDOcrModelManager.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/braintreepayments/api/DeviceInspector.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/braintreepayments/api/TLSSocketFactory.java com/snowballtech/charles/http/connect/HttpClient.java lib/android/paypal/com/magnessdk/network/base/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	bo/app/r20.java com/datadog/opentracing/StringCachingBigInteger.java org/junit/runner/manipulation/Ordering.java
10	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/amplitude/api/DatabaseHelper.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	defpackage/s.java
12	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/stripe/android/shoppay/webview/EceWebView.java
13	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/braze/support/StringUtils.java
14	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	lib/android/paypal/com/magnessdk/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/junit/rules/TemporaryFolder.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	adyen/com/adyencse/encrypter/PRNGFixes.java bo/app/pa0.java bo/app/sq.java com/airbnb/lottie/network/NetworkCache.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/jakewharton/disklrucache/DiskLruCache.java com/withpersona/sdk2/inquiry/shared/image/RealImageHelper.java junit/runner/BaseTestRunner.java lib/android/paypal/com/magnessdk/n/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	bo/app/ea.java bo/app/fa.java bo/app/ko.java bo/app/rb0.java bo/app/ug0.java bo/app/xc.java com/airbnb/lottie/network/NetworkCache.java com/braze/d0.java com/datadog/android/core/internal/persistence/BatchId.java com/withpersona/sdk2/inquiry/document/DocumentCameraWorker.java com/withpersona/sdk2/inquiry/governmentid/CountdownCameraWorker.java com/withpersona/sdk2/inquiry/governmentid/DocumentSelectWorker.java com/withpersona/sdk2/inquiry/shared/image/RealImageHelper.java id/zelory/compressor/ImageUtil.java org/tensorflow/lite/Interpreter.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/limebike/rider/util/extensions/ImageProxyExtensionsKt.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/kount/api/FingerprintCollector.java
00130	Get the current WIFI information	wifi collection	com/kount/api/FingerprintCollector.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	com/kount/api/FingerprintCollector.java
00076	Get the current WiFi information and put it into JSON	collection wifi	com/kount/api/FingerprintCollector.java
00082	Get the current WiFi MAC address	collection wifi	com/kount/api/FingerprintCollector.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ai/forethought/ForethoughtActivity.java com/braintreepayments/api/BrowserSwitchInspector.java com/withpersona/sdk2/inquiry/launchers/CustomTabsLauncherModuleKt.java io/noties/markwon/LinkResolverDef.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/braintreepayments/api/BrowserSwitchInspector.java com/withpersona/sdk2/inquiry/launchers/CustomTabsLauncherModuleKt.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/braintreepayments/api/SynchronousHttpClient.java com/stripe/android/core/networking/ConnectionFactory.java
00109	Connect to a URL and get the response code	network command	com/amplitude/api/ConfigManager.java com/braintreepayments/api/SynchronousHttpClient.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00078	Get the network operator name	collection telephony	io/branch/referral/SystemObserver.java
00108	Read the input stream from given URL	network command	com/adyen/checkout/core/api/Connection.java com/braintreepayments/api/BaseHttpResponseParser.java
00075	Get location of the device	collection location	com/kount/api/LocationCollector.java com/withpersona/sdk2/inquiry/shared/inquiry_session/GpsUtilsKt.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/adyen/checkout/base/analytics/AnalyticEvent.java com/braintreepayments/api/BraintreeClient.java io/noties/markwon/LinkResolverDef.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java
00089	Connect to a URL and receive input stream from the server	command network	com/amplitude/api/ConfigManager.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java
00112	Get the date of the calendar event	collection calendar	com/kount/api/SystemCollector.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/DatabaseHelper.java
00147	Get the time of current location	collection location	com/kount/api/LocationCollector.java
00137	Get last known location of the device	location collection	com/kount/api/LocationCollector.java
00115	Get last known location of the device	collection location	com/kount/api/LocationCollector.java
00091	Retrieve data from broadcast	collection	com/datadog/android/rum/_RumInternalProxy.java
00094	Connect to a URL and read data from it	command network	com/adyen/checkout/base/analytics/AnalyticsDispatcher.java

FIREBASE DATABASES ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/299973870560/namespaces/firebase:fetch?key=AIzaSyCA_Y9mQJHfUurjT0u62tCwW-zr_2Vu1u0. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_CONTACTS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE
Other Common Permissions	7/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
c.paypal.com	ok	**IP:** 151.101.137.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 3.161.213.50 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ssl.kaptcha.com	ok	**IP:** 35.81.31.24 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
c.sandbox.paypal.com	ok	**IP:** 151.101.139.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
web-latest.lime.bike	ok	No Geolocation information available.
api.paypal.com	ok	**IP:** 66.211.168.123 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.sandbox.paypal.com	ok	**IP:** 173.0.93.181 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map
localhost.mock	ok	No Geolocation information available.
braintreepayments.com	ok	**IP:** 151.101.67.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
tst.kaptcha.com	ok	**IP:** 35.81.36.228 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
m.stripe.com	ok	**IP:** 35.83.84.96 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 34.211.66.221 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
q.stripe.com	ok	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
dashboard.primer.io	ok	**IP:** 76.76.21.93 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 54.192.51.123 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	ok	**IP:** 3.161.213.81 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
android.asset	ok	No Geolocation information available.
unproxied2.limecloudflare.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
stripe.com	ok	**IP:** 54.162.8.126 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
support.stripe.com	ok	**IP:** 198.202.176.41 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
help.branch.io	ok	**IP:** 104.18.20.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
checkoutshopper-test.adyen.com	ok	**IP:** 62.146.255.4 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 52.28.17.14 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
juicer.lime.bike	ok	**IP:** 172.64.148.190 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
checkoutshopper-live-au.adyen.com	ok	**IP:** 62.146.255.13 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
www.stage2du13.stage.paypal.com	ok	**IP:** 66.211.168.121 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
branch.app.link	ok	**IP:** 3.161.213.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.paypalobjects.com	ok	**IP:** 151.101.139.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
link.com	ok	**IP:** 3.229.145.172 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
js.hcaptcha.com	ok	**IP:** 104.19.229.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
proxied2.limecloudflare.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
primer.io	ok	**IP:** 3.162.3.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mqa.kaptcha.com	ok	No Geolocation information available.
checkoutshopper-live-us.adyen.com	ok	**IP:** 62.146.255.13 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
api.msmaster.qa.paypal.com	ok	No Geolocation information available.
api.sandbox.braintreegateway.com	ok	**IP:** 159.242.242.128 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
solve-widget.forethought.ai	ok	**IP:** 172.66.47.81 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
b.stats.paypal.com	ok	**IP:** 34.106.92.18 **Country:** United States of America **Region:** Utah **City:** Salt Lake City **Latitude:** 40.760780 **Longitude:** -111.891052 **View:** Google Map
web-production.lime.bike	ok	**IP:** 172.64.148.190 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
limebike-prod.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cs.android.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
lime.bike	ok	**IP:** 104.18.39.66 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
api2.branch.io	ok	**IP:** 3.161.213.39 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
help.li.me	ok	**IP:** 216.198.54.11 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.statsig.com	ok	**IP:** 34.128.128.0 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
api.braintreegateway.com	ok	**IP:** 159.242.242.192 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **View:** Google Map
docs.stripe.com	ok	**IP:** 3.229.145.172 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
checkoutshopper-live.adyen.com	ok	**IP:** 147.12.18.68 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 3.162.3.19 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/frauddetection/FraudDetectionDataRequest.java
support@stripe.com name@example.com test@mail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Instabug	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/206

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"_tag_login_password" : "Password"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "028c6b9caf394e9e8ae30e5cf4374acd"
"com_appboy_firebase_cloud_messaging_sender_id" : "299973870560"
"com_braze_api_key" : "5858fa6b-910b-402b-acb8-4cbe4a18dccc"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"

POSSIBLE SECRETS
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"firebase_database_url" : "https://limebike-prod.firebaseio.com"
"google_api_key" : "AIzaSyCA_Y9mQJHfUurjT0u62tCwW-zr_2Vu1u0"
"google_crash_reporting_api_key" : "AIzaSyCA_Y9mQJHfUurjT0u62tCwW-zr_2Vu1u0"
"google_pay_authenticate_button" : "Authenticate"
"google_places_api_key_debug" : "AIzaSyDsAdxF35g1qcn7ZYiRK156LjCVbXPbfjA"
"google_places_api_key_production" : "AIzaSyBF9XE02lC5ot-bso97HJa_Y0xzjPvDjSQ"
42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
145188775577763990151158743208307020242261438098488931355057091965931517706595657435907891265414916764399268423699130577757433083166651158914570105971074227669275788291575622090199821297575654322355049043101306108213104080801056529374892690144291505781966373045481835947239164288532817130229924555666307371985 5
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
deca87e736574c5c83c07314051fd93a

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13 56D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361 C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
FFFFFFFE0000000075A30D1B9038A115
1340780792994259709957402499820584612747936582059239337772356144372176403007354697680187429816690342769003185818648605085375388281194656994643364900608409 5
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
1157920892373161954235709850086879078528375642790749043826051631415181614943 37
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
1270212482889324174659070427771764435257876535089165358128175072657050312609850984974231883334834011809259999951209889341306592056149967242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336850045410625869714168836867788425378203 83

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1
ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B3
24FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583
FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B
46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC
522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D6
9F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D714000
3C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63
BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00E
F092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB584
7A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B
80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC
5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD825154
1FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE307
5A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A
8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF

6db14acc9e21c820ff28b1d5ef5de2b0

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13
56D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361
C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86
039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64EC
FB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B
18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186
AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2
D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF

1157920892103562487626974469494075735299969552241357603424222590610685120443 69

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13
56D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66D3F8152AD6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A317091883681286130BC8985DB1602E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60E69CC928B2B9C52172E413042E9B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F
9760508f15230bccb292b982a2eb840bf0581cf5
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FFF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F62901228F8C28CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045AF2767164E1DFC967C1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353BBB64E0EC377FD028370DF92B52C7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331056774413619636480306472137782665689868646846327771015080940118260877020161532499046833293129492091277624113787803022435574660628397165937642683267426978088006163152816347588 7
db92371d2126e9700324977504e8c90e
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C209E0C6497517ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63ACAE1CAA6B7902D52526735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857F689962856DED4010ABD0BE621C3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597

POSSIBLE SECRETS
1340780792994259709957402499820584612747936582059239337772356144372176403007354697680187429816690342769003185818648605085375388281194656994643364900608409 6
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
1157920892373161954235709850086879078532699846656405640394575840079131296399 35
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898 5984

POSSIBLE SECRETS
5c4ece41241a1bb513f6e3e5df74ab7d5183dfffbd71bfd43127920d880569fd
1009979067550553047720818155359252248698410825720534578748235158755771479905292727772441528526992987964833566996828420279728960527471731754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940973554032134009725883228768509467406639 62
B4E134D3FB59EB8BAB57274904664D5AF50388BA
F518AA8781A8DF278ABA4E7D64B7CB9D49462353
b1995f7b-f6bb-4dad-b64d-96672d9dfc48
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13 56D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361 C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86 039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64EC FB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B 18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
1394548711991158256014096551076907131070417070599280317977580014543757653577229840941243685222882398330391146816480766882369212207373226 721607407477717009111345504320538046476949046861201130878162407401848004770471573366629262494235712488239685422217536601433914856808405203368594584948031873412885804895251 63
37a6259cc0c1dae299a7866489dff0bd
8d8e3f79aa0783ab0cfa5c8d65d663a9da6ba99401efb2298aaaee387c3b00d6
6836319614495570078444416561182725289510217088876144205509505128755031408302 3
3613425095674979579858512791958788195661110667298501507187719825356841440510 9

POSSIBLE SECRETS
0c14416e6f6e796d6f75732053656e64657220202020
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13 56D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361 C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86 039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64EC FB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B 18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186 AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2 D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37 BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426 FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45 B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2 EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD 300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C734 73FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31 CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475 677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFF
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
340282366920938463463374607431768211456
7988514166341097689762711893575632374730795191650763975830047269233887353395 9
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1 ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B3 24FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583 FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
1157920892373161954235709850086879078532699846656405640394575840079131296399 36
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13 56D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E80 83969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43 A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE 53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
dcb428fea25c40e7b99f81ae5981ee6a
E87579C11079F43DD824993C2CEE5ED3
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
55066263022277343669578718895168534326250603453777594175500187360389116729240
517cc1b727220a94fe13abe8fa9a6ee0
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC 7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF
bb00bf547b29e9cf1676cf036a3deee11
90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
484395612939064517590525852527979142027629495260417479958440807171082404635286
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

POSSIBLE SECRETS
e3f1f98c9da02a93bb547f448b472d727e14b22455235796fe49863856252508
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
1420117415975634811963682860223180897432761383952437387628725734419274593935127189736311660784676003608489466235676257952827747192122419290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122933384839245143396147277606818806097342 39
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
41058363725152142129326129780047268409114441015993725554835256314039467401291
5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
917715298965546059455881490183827502172968583935207241727433257254743749798 01
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
340282366920938463463374607431768211455
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE5E9001A8D66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D119529A45D6F834566E3025E316A330EFBB77A86F0C1AB15B051AE3D428C8F8ACB70A8137150B8EEB10E183EDD19963DDD9E263E4770589EF6AA21E7F5F2FF381B539CCE3409D13CD566AFBB48D6C019181E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA
32670510020758816978083085130507043184471273380659243275938904335757337482424
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFACCBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371
A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7FBD7D3B9A92EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5

POSSIBLE SECRETS

308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f6964301e170d313730383034313635333375a170d343730383034313635333375a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f6964301e170d313730383034313635333375a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f6964308201220d06092a864886f70d01010105000382010f003082010a0282010100899864 6f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f6f207764842e5677e35a281a422659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f288e2a26f99eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350304e300c0603551d130405300301 01ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d2304183016801419a864c0f2618c67c803a23da909bc70521f269b300d06092a864886f70d01010b05000382010100 5403fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd386775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb3416cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3b99774f4b8f3d09262e7

PLAYSTORE INFORMATION

Title: Lime - #RideGreen

Score: 4.8625593 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Travel & Local **Play Store URL:** com.limebike

Developer Details: Neutron Holdings, Inc., 5130091855041680247, None, https://www.li.me/, support@li.me,

Release Date: May 10, 2017 **Privacy Policy:** Privacy link

Description:

You have places to be and people to see. Get there easily and on time with an emissions-free Lime e-bike or e-scooter! START YOUR RIDE IN 3 STEPS Step 1 Download the app, create an account and accept our terms and conditions https://www.li.me/user-agreement Privacy Notice https://www.li.me/legal/privacy-policy/ Step 2 Find a nearby Lime vehicle on the map (vehicle availability depends on your city and supply) Step 3 Unlock your vehicle by scanning the QR code, entering the plate number, or by tapping a button on the app. RIDE RESPONSIBLY A safe community starts with riding responsibly. It’s important to remember the rules of the road before every ride. You should always: - Ride in bike lanes, never on sidewalks - Wear a helmet when you ride - Park clear of walkways, driveways and access ramps - Visit https://safety.li.me/ to learn more #RIDEGREEN Lime is on a mission to build a future where transportation is shared, affordable and carbon-free. You can read more about Lime’s products and services, including how we calculate our prices in our terms and conditions https://www.li.me/user-agreement.

SCAN LOGS

Timestamp	Event	Error
2025-11-03 02:01:59	Generating Hashes	OK
2025-11-03 02:01:59	Extracting APK	OK
2025-11-03 02:01:59	Unzipping	OK
2025-11-03 02:02:00	Parsing APK with androguard	OK
2025-11-03 02:02:01	Extracting APK features using aapt/aapt2	OK
2025-11-03 02:02:02	Getting Hardcoded Certificates/Keystores	OK
2025-11-03 02:02:10	Parsing AndroidManifest.xml	OK
2025-11-03 02:02:11	Extracting Manifest Data	OK
2025-11-03 02:02:11	Manifest Analysis Started	OK

2025-11-03 02:02:11	Reading Network Security config from network_security_config.xml	OK
2025-11-03 02:02:11	Parsing Network Security config	OK
2025-11-03 02:02:11	Performing Static Analysis on: Lime (com.limebike)	OK
2025-11-03 02:02:12	Fetching Details from Play Store: com.limebike	OK
2025-11-03 02:02:12	Checking for Malware Permissions	OK
2025-11-03 02:02:12	Fetching icon path	OK
2025-11-03 02:02:12	Library Binary Analysis Started	OK
2025-11-03 02:02:12	Reading Code Signing Certificate	OK
2025-11-03 02:02:13	Running APKiD 3.0.0	OK
2025-11-03 02:02:16	Detecting Trackers	OK
2025-11-03 02:02:24	Decompiling APK to Java with JADX	OK

2025-11-03 02:19:07	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/c9120aa06711205e27c46687d7a41e55/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/c9120aa06711205e27c46687d7a41e55/c9120aa06711205e27c46687d7a41e55.apk'], 999.9999000839889)
2025-11-03 02:19:07	Converting DEX to Smali	OK
2025-11-03 02:19:10	Code Analysis Started on - java_source	OK
2025-11-03 02:21:37	Android SBOM Analysis Completed	OK
2025-11-03 02:22:07	Android SAST Completed	OK
2025-11-03 02:22:07	Android API Analysis Started	OK
2025-11-03 02:22:37	Android API Analysis Completed	OK
2025-11-03 02:22:37	Android Permission Mapping Started	OK
2025-11-03 02:23:45	Android Permission Mapping Completed	OK
2025-11-03 02:23:46	Android Behaviour Analysis Started	OK

2025-11-03 02:24:17	Android Behaviour Analysis Completed	OK
2025-11-03 02:24:17	Extracting Emails and URLs from Source Code	OK
2025-11-03 02:24:22	Email and URL Extraction Completed	OK
2025-11-03 02:24:22	Extracting String data from APK	OK
2025-11-03 02:24:23	Extracting String data from Code	OK
2025-11-03 02:24:23	Extracting String values and entropies from Code	OK
2025-11-03 02:24:30	Performing Malware check on extracted domains	OK
2025-11-03 02:24:36	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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