ANDROID STATIC ANALYSIS REPORT

app_icon

SoberTracker (1.4.4)

File Name:	SoberBuddy_ Sober Tracker_1.4.4_APKPure.apk
Package Name:	com.soberbuddy.app
Scan Date:	Nov. 27, 2024, 12:34 a.m.
App Security Score:	**49/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	15	3	2	1

FILE INFORMATION

File Name: SoberBuddy_ Sober Tracker_1.4.4_APKPure.apk
Size: 86.31MB
MD5: 4d0866dbaf9b33e4d4963e9a674697a7
SHA1: 52007bc662da1c28d55660bbe4af2754a48d9ac2
SHA256: c5bf9120185f96a675777c5604b881858de96e4762e7c9641c289fc78587c759

APP INFORMATION

App Name: SoberTracker
Package Name: com.soberbuddy.app
Main Activity: com.soberbuddy.app.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 1.4.4

Android Version Code: 73

APP COMPONENTS

Activities: 9
Services: 10
Receivers: 16
Providers: 6
Exported Activities: 1
Exported Services: 1
Exported Receivers: 3
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=CA, L=Newport Beach, O=SoberBuddy, CN=Tara Schiller
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-29 19:28:26+00:00
Valid To: 2120-06-05 19:28:26+00:00
Issuer: C=US, ST=CA, L=Newport Beach, O=SoberBuddy, CN=Tara Schiller
Serial Number: 0xd91d478
Hash Algorithm: sha256
md5: ec130b9e2046ca2e63c3bdecfd45c0d3
sha1: c0224e1f4c37f3dba70572dead1ff65b223e5600
sha256: c36ef7a25bc4ee390b8f1b88d7f6efec3a1afeda5099002234d42fe0f5f16a05
sha512: 9c8dbd5f6366fecc76a47017db409bb277de4012d9df7b8c88834dfd6746346916ba301bc04bdcb4994d510d21c47e3e23408bd055f403cbd0cfaed1f0c61631
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: da7b7c80474fb95e1a0813b047e03687ccd59a1964f4d57477ffc3c86cffd1f1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.soberbuddy.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible VM check
	Obfuscator	Kiwi encrypter
	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
	FINDINGS	DETAILS
classes3.dex	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.soberbuddy.app.MainActivity	Schemes: http://, https://, @string/deeplink_scheme://, Hosts: @string/applink_host, @string/applink_host_alternate,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.soberbuddy.app,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [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.
5	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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: **0** | WARNING: **6** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java
				com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationStorage.java com/capacitorjs/plugins/localnotifications/TimedNotificationPublisher.java com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ava com/revenuecat/purchases/capacitor/PurchasesPlugin.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/DeferredAppLinkDataHandler.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser.java io/branch/referral/validators/DeepLinkRoutingValidator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/c/b.java com/capacitor/rateApp/CapacitorRateApp.java com/capacitorjs/plugins/network/NetworkPlugin.java com/getcapacitor/Logger.java com/revenuecat/purchases/capacitor/PurchasesPlugin.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.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/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/BridgeWebChromeClient.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java
9	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	io/branch/referral/ShareLinkManager.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/amazon/a/a/b/b.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/getcapacitor/Bridge.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java io/branch/referral/Branch.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00096	Connect to a URL and set request method	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java
00089	Connect to a URL and receive input stream from the server	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java
00030	Connect to the remote server through the given URL	network	com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/getcapacitor/plugin/util/HttpRequestHandler.java com/revenuecat/purchases/common/HTTPClient.java
00094	Connect to a URL and read data from it	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java com/getcapacitor/Bridge.java io/branch/referral/Branch.java
00036	Get resource file from res/raw directory	reflection	com/amazon/a/a/i/g.java com/capacitorjs/plugins/localnotifications/LocalNotificationManager.java com/capacitorjs/plugins/localnotifications/NotificationChannelManager.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java io/branch/referral/Branch.java
00192	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/amazon/c/a/a/c.java com/getcapacitor/AndroidProtocolHandler.java com/revenuecat/purchases/common/FileHelper.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java
00078	Get the network operator name	collection telephony	io/branch/referral/SystemObserver.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://your-soberbuddy-app.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/936310992710/namespaces/firebase:fetch?key=AIzaSyAabQzqud38QIRUgsNy27blCKSeAbLVaNQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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

DOMAIN	STATUS	GEOLOCATION
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
help.branch.io	ok	**IP:** 104.16.241.118 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 34.198.224.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.branch.io	ok	**IP:** 13.225.195.28 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 3.162.3.41 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api-paywalls.revenuecat.com	ok	**IP:** 34.198.224.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
branch.app.link	ok	**IP:** 13.225.195.66 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 3.161.213.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.branch.io	ok	**IP:** 3.161.213.119 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 3.162.2.181 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
your-soberbuddy-app.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
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
play.google.com	ok	**IP:** 142.251.41.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bnc.lt	ok	**IP:** 54.192.51.38 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
api.revenuecat.com	ok	**IP:** 34.198.224.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
capacitorjs.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

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"branch_key" : "key_live_gmYsnRoHVl2dLsIKJoT0EomlrxlEdOAd"
"branch_test_key" : "key_test_af8whJeUTj7oStLKHwucpphnAydraHCC"
"firebase_database_url" : "https://your-soberbuddy-app.firebaseio.com"
"google_api_key" : "AIzaSyAabQzqud38QIRUgsNy27blCKSeAbLVaNQ"
"google_crash_reporting_api_key" : "AIzaSyAabQzqud38QIRUgsNy27blCKSeAbLVaNQ"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□□<b>facebook.com/device</b>□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□□"
UloSfoTFTeHwqhun6eFIktptgYL2IDO82d0FsFWUGkksiDJXPejv+whIfZ+2Wfan
qqkgHuCnSf99P11sSI1mmduveFqE9tgI3BiAGjoFd0Q=
yuf1nsAsFy3olrhDGup7vlloJ0uqB/pCPd1wXjadNbk08Ahzm1ms2kGIpbi3j3n0
ME2QJ5XUdJ4H7tJ/4Z12d9y6FonD1ndLFXNLtFSyv18t135hu7AHtSikKZF3zLCe
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
WlHsOh3wlV0WLQIL1K9rw/fkp4GO6NjuEiNcfL+sOy0Pjb3rqvyOdqvxRQtxMK9a

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
0sUnM0f6jlJ2HFtGqy6I2XKbpiW5H3xN4OJ+XAaaX74=
Z32lznDxcfXBlpXaiScrYTSjeY6TCwZQ4arkKKXRMmw=
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
886A7k0gCRGrgCy/c5GSpG0vYnwEUdVtxuzPfTnYprNYN9F5XuGF9g0NY4fPk5Hd
9aN5Cm+1eB8M6WEeTCyHrcP34KU7gU8jlMBy6C9bmSWwJjNodfWmCfc45rNGVCVv
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
KV7CkapOc398LrUMWLxbtIox9+Yv3R2fIy2uxXRJMPI=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
6AMFYAA1mweGFVX4poqZeQeR2M0TfYtYyjbhtBhim8Y=
vIuyJgkXAuHDOYyZs/XS63TUqVD1sO0CQ+HhaScCOnqgG3I71zSq+SxqNmjD4E1e
hyYn+RjvP2onIyOXybEZ6mkvLCHC0SlFWfJn2VBlQ1U=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
7xM/jp1ssnTHy48Ysast7LrhX+6n3G9zqz4TlIUZi1E=
EoDE6fB1YbrAX67hf86xlBvGVg8B3u9wZtbhQoEO0J04e2Wdeoe11h/TJjV6o6eA
Y36p4+OnCZGc4+WeLfFtxuI6ijQbwb2FRBUVzIb1EqM=
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e04160414 8d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
SMQ0oHMJOqiqLmGCdZSOhgiL74ZHfxFO1BXhlv2/4270PZ+nQBq2Z++21yQPgk4C
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
49f946663a8deb7054212b8adda248c6
kMXyn5TCo9Bebr+VtNQhQbsedp0AgYXwXzhxSBLRAfdMLXXtz9tGq6347jNKG6EM
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
hX9HXpz3HDJtF53Eqq7YR2TaBd+4lJGvaDWuDcJVda216lrs8zYBdPXwugzu5Gf7

POSSIBLE SECRETS
hM2f+ZpOxGYOaoXhhqTEB4E2d1ZW9gQWshCuliQN60Y=
4rwcEO1STWNFfBc3lwJoy7fjIKj0+9F5WKY6nBJgTk0=
kbdrv8tsziKs0Eek7BsM4U0iKocTYc9jJCZMuz5pfY858GShsX2u88zYbIs2mx+G
ebsUU9Ppqfz4PifIRFfiICzwWhwX2B63IgcdBHgXQC8=
115792089210356248762697446949407573529996955224135760342422259061068512044369
ZZzuwfIygL/edqNYv6TIjIHmhzUDfuWz7Uf43FouJ1g=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
9b8f518b086098de3d77736f9458a3d2f6f95a37
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3
doCqFliMrm1a/QUTbgigv63oWalof2MAZ3FbCUkhzYI=
115792089210356248762697446949407573530086143415290314195533631308867097853951
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
yAAnOyC41KY/eL6CMAojoxxQ2iiLx6vx3Hn+A3WrzJkepsJehbcbUfsfqGMngMgj
18t2+sVmBFWOR34FTgk9oqx1qcZI0NwZV8Dtcvfe5eY=
B3EEABB8EE11C2BE770B684D95219ECB

POSSIBLE SECRETS
RP5LQuE/2876zTvAb2rVm25QfjxwoRyidjQTLjf0RRc=
gwRPz8bLLKP2CNEw52CWr8qH7aLQJQgZH2Do8dWUF6DoOxZ/M4tgY0r5mQPR4CHj
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
wXdYywy2LsdIoEkljSZxSgKQk9kgrY0qof3Oat1MHRk=
4hMU+mzsUU6XYstubXUmZj16dvyex8xOMz7Jpzy9YvA=
T73PopQD1DEGYFr8uKZxHThHCY1arOonGG0ho3b7ul0=
95m8nxzquSP6UteH+ctwS+fnWW3e+ARzjY5ilI8E7MqGTZUjuLdEgCnwSuHZqZih
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
V8HYPAghzWHqrIy38Vh6p4w3eeyqyQ2rIl2LLOtw9JM=
c56fb7d591ba6704df047fd98f535372fea00211
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
4qo7ydIZUH0p5YejDx/8wjt7DkOxdD2eNzq7zPXjrFqYSIF2FJuHDk9SiXwd9Q5H
PYnCLpLLKhA0q7i2li/Zt4bu8StAsClZCXaLnFnfz+0=
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
zvpJLhHcREzFwRQlrOzsvLoNpjh/NkRx1SzlprPtOYrQsQFy5mJhifaboWh6aFyp
XcryxQHEcO2NLi7jWtJQeOEAAGF+i46DQLx722/7X2w=
Ja6aP+2sRyo5nxEaCirzMomJuTTHKAyM16vEB9WmdYo=
Hi6y3/CP3FfCDFHJzBy2rbo5w1qdyw4sxSVfaLENOd74y8BTNPMSy00WznqvaqDe
SsRJwzlVc/FD7Gcgkfy2usB8pnbNBUiAfm++VXDvOVBbBVhgo4O90KdNPi86tLTu
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: SoberBuddy: Sober Tracker

Score: 4.277228 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.soberbuddy.app

Developer Details: SoberBuddy, SoberBuddy, 4041 MacArthur BLVD STE 400, Newport Beach, CA 92660, https://yoursoberbuddy.com/, admin@yoursoberbuddy.com,

Release Date: Jun 29, 2020 **Privacy Policy:** Privacy link

Description:

Embark on a Sober Journey with Confidence Struggling to find your path to sobriety? Feel overwhelmed or unmotivated? Meet "SoberBuddy" - your personal guide to help you get and stay sober. Join over 100,000 individuals who have transformed their lives with our supportive, user-friendly app. Track Your Success with Confetti Sober Tracker • Celebrate each sober day with our vibrant Confetti Sober Tracker. Visualize your progress and feel the joy of every milestone in your sober journey. Daily Mood Check-Ins with Buddy • Start your day with a mood check-in. Receive motivating and comforting responses from "Buddy," your virtual sober companion, tailored to uplift and inspire you, no matter where you are in your journey. Bite-Size Challenges for Lasting Sobriety • Engage in daily, easy-to-follow challenges. Learn evidence-based skills proven to aid in maintaining sobriety. Our bite-size approach makes learning and applying these skills manageable and effective. Evidence-Based, User-Approved • SoberBuddy is not just an app; it's a community-tested solution backed by scientific evidence. Experience methods that have helped thousands in their sobriety journey. Stay Motivated and Supported • Whether you're just starting out or have been on this path for a while, SoberBuddy is here to support you. Our features are designed to keep you motivated and focused on your goal: a healthier, sober life. Start Feeling Empowered Today • Ready to take control of your sobriety? Download SoberBuddy now and learn skills that will boost your sobriety. Your journey to a sober, fulfilling life starts here!

SCAN LOGS

Timestamp	Event	Error
2024-11-27 00:34:39	Generating Hashes	OK
2024-11-27 00:34:39	Extracting APK	OK
2024-11-27 00:34:39	Unzipping	OK
2024-11-27 00:34:40	Getting Hardcoded Certificates/Keystores	OK
2024-11-27 00:34:40	Parsing APK with androguard	OK
2024-11-27 00:34:42	Parsing AndroidManifest.xml	OK
2024-11-27 00:34:42	Extracting Manifest Data	OK
2024-11-27 00:34:42	Manifest Analysis Started	OK
2024-11-27 00:34:42	Performing Static Analysis on: SoberTracker (com.soberbuddy.app)	OK

2024-11-27 00:34:42	Fetching Details from Play Store: com.soberbuddy.app	OK
2024-11-27 00:34:43	Checking for Malware Permissions	OK
2024-11-27 00:34:43	Fetching icon path	OK
2024-11-27 00:34:43	Library Binary Analysis Started	OK
2024-11-27 00:34:43	Reading Code Signing Certificate	OK
2024-11-27 00:34:43	Running APKiD 2.1.5	OK
2024-11-27 00:34:47	Updating Trackers Database....	OK
2024-11-27 00:34:47	Detecting Trackers	OK
2024-11-27 00:34:49	Decompiling APK to Java with JADX	OK
2024-11-27 00:35:11	Converting DEX to Smali	OK
2024-11-27 00:35:11	Code Analysis Started on - java_source	OK

2024-11-27 00:35:12	Android SBOM Analysis Completed	OK
2024-11-27 00:35:16	Android SAST Completed	OK
2024-11-27 00:35:16	Android API Analysis Started	OK
2024-11-27 00:35:18	Android API Analysis Completed	OK
2024-11-27 00:35:18	Android Permission Mapping Started	OK
2024-11-27 00:35:19	Android Permission Mapping Completed	OK
2024-11-27 00:35:19	Android Behaviour Analysis Started	OK
2024-11-27 00:35:20	Android Behaviour Analysis Completed	OK
2024-11-27 00:35:20	Extracting Emails and URLs from Source Code	OK
2024-11-27 00:35:21	Email and URL Extraction Completed	OK
2024-11-27 00:35:21	Extracting String data from APK	OK

2024-11-27 00:35:21	Extracting String data from Code	OK
2024-11-27 00:35:21	Extracting String values and entropies from Code	OK
2024-11-27 00:35:24	Performing Malware check on extracted domains	OK
2024-11-27 00:35:26	Saving to Database	OK

Report Generated by - MobSF v4.2.6

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.