

ANDROID STATIC ANALYSIS REPORT



BetterHelp (2.85)

File Name:	com.betterhelp_285.apk
Package Name:	com.betterhelp
Scan Date:	Aug. 29, 2025, 8:09 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

≟ HIGH	▲ MEDIUM	i INFO	✓ SECURE	◎ HOTSPOT
3	28	3	3	2

FILE INFORMATION

File Name: com.betterhelp_285.apk

Size: 21.4MB

MD5: 5cdc39cdc85763bb0aa2dcd7d40231ce

SHA1: 1dc42018d7dac0e9a1c09778ed9fdf6527d9534c

SHA256: 9010c4cd054c6c89d8c9034ebebcd90c8314992fc42b1aac096b46d96b91d4b2

i APP INFORMATION

App Name: BetterHelp

Package Name: com.betterhelp

Main Activity: com.betterhelp.MainActivity

Target SDK: 34 Min SDK: 24 Max SDK:

Android Version Name: 2.85

EE APP COMPONENTS

Activities: 37 Services: 12 Receivers: 5 Providers: 3

Exported Activities: 11
Exported Services: 3
Exported Receivers: 2
Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=US, O=BetterHelp Signature Algorithm: rsassa_pkcs1v15 Valid From: 2014-11-13 02:21:07+00:00 Valid To: 2039-11-07 02:21:07+00:00

Issuer: C=US, O=BetterHelp Serial Number: 0x482b256f Hash Algorithm: sha256

md5: 142a5c7ce279b1f00c3c6d256eb39ce6

sha1: c84490032430574c6b4ed4e8ac6ef35490435bd8

sha256: df202ee78036d8345b03aa1dbe6f4deeede96518c6f43906f8ae92359405ce8d

sha512: a4f9850735a3ab833f2cb8f0dccb92c9456fa6ab6c7c44acc9d3c8522acab9e39a66406df732486edc681b77abe1db5e66c45f6c11db7f10b2c25cca46fd5f5b

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 9142bfc193aff4d43061d758fc25801ff9b3980aff54f8147dd39252f719bd97

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.betterhelp.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system- alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.betterhelp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

MAPKID ANALYSIS

FILE	DETAILS	
5cdc39cdc85763bb0aa2dcd7d40231ce.apk	FINDINGS	DETAILS
Scacs scaces / 05 bb out 2 act a / a + 02 s rec. apr	Anti-VM Code	possible VM check

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.TAGS check SIM operator check network operator name check ro.kernel.qemu check	
Classes.uex	Compiler	r8	

FILE	DETAILS		
	FINDINGS	DETAILS	
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check possible VM check	
	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
	FINDINGS	DETAILS	
classes3.dex	Anti-VM Code	Build.HARDWARE check	
	Compiler	r8 without marker (suspicious)	

BROWSABLE ACTIVITIES

ACTIVITY		INTENT
----------	--	--------

ACTIVITY	INTENT
com.betterhelp.MainActivity	Schemes: https://, betterhelpapp://, Hosts: www.betterhelp.com, betterhelp.com, Path Patterns: .*,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.betterhelp,
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.betterhelp/success, /com.betterhelp/cancel, Path Prefixes: /com.betterhelp/authentication_return, /com.betterhelp,

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 17 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Service (com.betterhelp.BHFirebaseMessaging) 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.
4	Activity (com.betterhelp.videoroom.VideoRoom) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.betterhelp.zoomvideoroom.ZoomVideoRoom) 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	Activity (com.betterhelp.videosession.VideoSession) 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
7	Activity (com.betterhelp.VideoTest) 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.
8	Activity (com.betterhelp.audioroom.AudioRoom) 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.
9	Activity (com.betterhelp.AudioTest) 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.
10	Activity (com.betterhelp.GooglePayActivity) 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.
11	Activity (com.betterhelp.NetworkTest) 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 (com.betterhelp.Troubleshooting) 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 (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
14	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.
15	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.
16	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.
17	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) 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	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: 2 | WARNING: 9 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A1/c.java A2/b.java A4/B.java A4/B.java A4/C.java A4/G.java A4/k.java A4/x.java B1/C1224a.java B2/g.java C3/i.java C4/c.java C4/f.java C8/d.java C9/j.java

NO	ISSUE	SEVERITY	STANDARDS	E0/J.java F1/cEjS va H7/b.java
				L/AbstractC1474b.java
				L8/e.java
				M3/e.java
				M4/e.java
				M4/j.java
				M4/k.java
				O0/d.java
				O2/w.java
				O4/a.java
				P1/b.java
				P1/e.java
				P3/f.java
				R0/f.java
				R1/c.java
				R4/a.java
				S3/C1628f.java
				S3/n.java
				T2/a.java
				T5/c.java
				U2/a.java
				V3/g.java
				W2/AbstractC1652b.java
				W2/J.java
				Y/i.java
				Y0/d.java
				Y3/C1692s.java
				b1/C2047x.java
				b2/C2060k.java
				b3/C2069g.java
				com/appsflyer/AFLogger.java
				com/appsflyer/internal/AFa1dSDK.java
				com/appsflyer/internal/AFa1jSDK.java
				com/appsflyer/internal/AFb1sSDK.java
				com/appsflyer/internal/AFb1tSDK.java
				com/appsflyer/internal/AFd1bSDK.java
				com/appsflyer/internal/AFd1eSDK.java
				com/appsflyer/internal/AFd1gSDK.java
				com/appsflyer/internal/AFd1mSDK.java

NO	ISSUE	SEVERITY	STANDARDS	com/appsflyer/internal/AFd1sSDK.java For Fappsflyer/internal/AFd1wSDK.java com/appsflyer/internal/AFd1xSDK.java
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/appsflyer/internal/AFe1pSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/share/CrossPromotionHel per.java com/appsflyer/share/LinkGenerator.java com/betterhelp/AudioTest.java com/betterhelp/VideoTest.java com/betterhelp/a.java com/betterhelp/audioroom/AudioRoom.j
				ava com/betterhelp/c.java com/betterhelp/iterable/Iterable.java com/betterhelp/videoroom/VideoRoom.j ava com/betterhelp/zoomvideoroom/ZoomVi deoRoom.java com/iterable/iterableapi/w.java com/opentok/android/BaseVideoCapture r.java com/opentok/android/OtLog.java com/opentok/android/PublisherKit.java com/twilio/audioswitch/android/Producti onLogger.java com/twilio/voice/EventPublisher.java com/twilio/voice/Logger.java com/twilio/voice/Registration.java com/vonage/mltransformers/CameraXVi deoCapturer.java com/vonage/mltransformers/MediapipeV
				ideoFrameProcessor.java com/zipow/cmmlib/Logger.java e1/e.java e2/AbstractC2911a.java i1/C3067c.java m3/AbstractC3334a.java n2/d.java n7/AbstractC3402E.java o5/InterfaceC3464d.java

NO	ISSUE	SEVERITY	STANDARDS	q3/AbstractC3537b.java
				s3/C3700g.java s4/C3709b.java t1/C3743c.java t2/AbstractC3747A.java t2/C3750D.java t2/C3751E.java t2/C3757c.java t2/x.java t2/x.java t2/y.java t4/C3773c.java u7/C3863l0.java v1/AbstractC3935a.java v2/BinderC3941F.java w2/AbstractBinderC4050a.java w2/AbstractC4025A.java w2/AbstractC4052c.java w2/AbstractDialogInterfaceOnClickListene rC4028D.java w2/C4032H.java w2/d0.java w2/d0.java w2/d0.java w2/f0.java w2/f0.java w2/n0.java w2/r0.java y3/C4267H.java z2/C4401a.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	K8/c.java K8/d.java K8/i.java K8/j.java us/zoom/video_sdk/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zipow/cmmlib/AppUtil.java us/zoom/video_sdk/i.java
				D0/C1266h.java D0/U.java D6/a.java D7/AbstractC1296h.java H/S.java K6/o.java K6/o.java K6/p.java L/C1479d0.java L6/g.java R5/a.java Z3/b.java a4/C1722e.java a4/C1740w.java com/opentok/android/DefaultAudioDevic e.java com/stripe/android/financialconnections/ a.java com/stripe/android/financialconnections/ model/FinancialConnectionsSession.java com/stripe/android/googlepaylauncher/h .java com/stripe/android/googlepaylauncher/i .java com/stripe/android/googlepaylauncher/ m.java com/stripe/android/googlepaylauncher/ m.java com/stripe/android/link/c.java com/stripe/android/link/c.java com/stripe/android/link/c.java com/stripe/android/link/c.java com/stripe/android/link/c.java com/stripe/android/payments/bankaccou nt/ui/a.java com/stripe/android/payments/core/auth entication/threeds2/c.java

NO	ISSUE	SEVERITY	STANDARDS	com/stripe/android/payments/core/auth httis: com/stripe/android/payments/paymentla
4	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	uncher/a.java com/stripe/android/payments/paymentla uncher/b.java com/stripe/android/paymentsheet/addre sselement/a.java com/stripe/android/paymentsheet/b.java com/stripe/android/paymentsheet/g.java com/stripe/android/paymentsheet/paym entdatacollection/ach/c.java
				com/stripe/android/paymentsheet/paym entdatacollection/polling/b.java com/stripe/android/paymentsheet/paym entdatacollection/polling/d.java com/twilio/voice/EventKeys.java com/twilio/voice/HttpsRegistrar.java com/twilio/voice/VoiceURLConnection.jav a
				com/twilio/voice/WarningEventConstants .java d7/InterfaceC2878c.java I5/w.java m5/C3348a.java n7/C3400C.java n7/C3408c.java
				us/zoom/libtools/storage/PreferenceUtil.j ava us/zoom/libtools/storage/ZmSharePrefer enceHelper.java v5/h.java v6/C.java v6/C3995k.java
				v6/C3996l.java v6/C4001q.java v6/C4003t.java v6/E.java v6/L.java

NO	ISSUE	SEVERITY	STANDARDS	v6/N.java F&LES va v6/U.java
				v6/Z.java v6/b0.java v6/c0.java z6/C4409c.java z6/C4410d.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	S8/a.java T8/a.java U8/a.java V8/a.java Z4/a.java j9/e.java us/zoom/net/dns/DnsServersDetector.jav a us/zoom/video_sdk/z.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	C3/w.java Y3/AbstractC1683i.java y3/AbstractC4286h.java
7	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/iterable/iterableapi/C2641m.java com/iterable/iterableapi/J.java i2/M.java i2/U.java
8	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/appsflyer/internal/AFa1wSDK.java com/appsflyer/internal/AFb1mSDK.java e8/C2926a.java
9	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/betterhelp/MainActivity.java com/betterhelp/audioroom/AudioRoom.j ava

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/betterhelp/MainActivity.java com/betterhelp/audioroom/AudioRoom.j ava
11	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/appsflyer/internal/AFa1aSDK.java com/twilio/voice/SidUtil.java us/zoom/video_sdk/z.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	P4/I.java
13	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/appsflyer/internal/AFa1aSDK.java s4/C3709b.java
14	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/betterhelp/b.java
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	s4/C3710c.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	Q8/E0.java R4/a.java U1/i.java X7/h.java Y3/B.java Z3/f.java com/iterable/iterableapi/M.java com/zipow/cmmlib/AppContext.java d4/e.java f4/C2949a.java k1/m.java s4/C3710c.java us/zoom/video_sdk/i.java us/zoom/video_sdk/r.java us/zoom/video_sdk/r.java us/zoom/video_sdk/r.java us/zoom/video_sdk/t.java
00014	Read file into a stream and put it into a JSON object	file	Z3/f.java f4/C2949a.java s4/C3710c.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1rSDK.java com/betterhelp/iterable/lterable.java com/iterable/iterableapi/G.java n7/J.java t4/C3773c.java

RULE ID	BEHAVIOUR LABEL		FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1rSDK.java com/appsflyer/internal/AFd1fSDK.java com/betterhelp/iterable/lterable.java com/iterable/iterableapi/G.java n2/d.java n7/J.java r2/RunnableC3601f.java t4/C3773c.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1tSDK.java com/betterhelp/GooglePayActivity.java com/betterhelp/MainActivity.java com/betterhelp/audioroom/AudioRoom.java com/betterhelp/videoroom/VideoRoom.java com/betterhelp/videosession/VideoSession.java com/betterhelp/zoomvideoroom/ZoomVideoRoom.java com/betterhelp/zoomvideoroom/ZoomVideoRoom.java com/iterable/iterableapi/C.java com/iterable/iterableapi/C2635g.java
00162	Create InetSocketAddress object and connecting to it		K8/b.java K8/j.java
00163	Create new Socket and connecting to it	socket	K8/b.java K8/j.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1wSDK.java us/zoom/video_sdk/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	T1/d.java Z3/f.java com/appsflyer/internal/AFa1dSDK.java com/zipow/cmmlib/AppContext.java k1/m.java us/zoom/video_sdk/g.java us/zoom/video_sdk/i.java us/zoom/video_sdk/p.java
00012	Read data and put it into a buffer stream	file	us/zoom/video_sdk/i.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1mSDK.java us/zoom/video_sdk/i.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1mSDK.java com/appsflyer/internal/AFf1oSDK.java com/betterhelp/a.java com/betterhelp/c.java com/iterable/iterableapi/A.java com/iterable/iterableapi/AbstractC2633e.java us/zoom/video_sdk/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	B1/Ljava I7/b.java I7/b.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFd1kSDK.java com/betterhelp/MainActivity.java com/betterhelp/a.java com/betterhelp/c.java com/betterhelp/videoroom/VideoRoom.java com/betterhelp/videoroom/VideoRoom.java com/iterable/iterableapi/A.java com/iterable/iterableapi/AbstractC2633e.java com/stripe/android/financialconnections/FinancialConnectionsSheetActivity.jav a com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectAct ivity.java com/stripe/android/financialconnections/d.java com/stripe/android/financialconnections/ui/FinancialConnectionsSheetNativeAct tivity.java com/stripe/android/payments/a.java com/stripe/android/view/C2707d0.java com/stripe/android/view/C2709e0.java us/zoom/video_sdk/k0.java
00005	Get absolute path of file and put it to JSON object	file	Z3/f.java com/appsflyer/internal/AFa1dSDK.java
00004	Get filename and put it to JSON object	file collection	com/appsflyer/internal/AFa1dSDK.java
00125	Check if the given file path exist	file	com/appsflyer/internal/AFa1dSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00199	Stop recording and release recording resources	record	com/betterhelp/AudioTest.java
00198	Initialize the recorder and start recording	record	com/betterhelp/AudioTest.java
00194	Set the audio source (MIC) and recorded file format	record	com/betterhelp/AudioTest.java
00197	Set the audio encoder and initialize the recorder	record	com/betterhelp/AudioTest.java
00196	Set the recorded file format and output path	record file	com/betterhelp/AudioTest.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	B1/C1224a.java I7/b.java com/betterhelp/a.java com/betterhelp/c.java com/iterable/iterableapi/AbstractC2633e.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectAct ivity.java com/stripe/android/payments/a.java us/zoom/video_sdk/k0.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1ISDK.java com/appsflyer/internal/AFc1rSDK.java com/iterable/iterableapi/G.java n7/J.java t4/C3773c.java v5/j.java

RULE ID	BEHAVIOUR LABEL		FILES
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFa1uSDK.java n7/J.java
00208	Capture the contents of the device screen	collection screen	com/vonage/webrtc/ScreenCapturerAndroid.java
00161	Perform accessibility service action on accessibility node info	accessibility service	b1/C2047x.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform accessibility service action		b1/C2047x.java
00056	Modify voice volume	control	com/vonage/webrtc/audio/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine61/WebRtcAudioTrack.java org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java tvo/webrtc/audio/WebRtcAudioTrack.java tvo/webrtc/voiceengine/WebRtcAudioTrack.java
00028	Read file from assets directory file		com/opentok/android/PublisherKit.java
00102	Set the phone speaker on	command	P1/e.java com/opentok/android/DefaultAudioDevice.java org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java
00094	Connect to a URL and read data from it	command network	c4/C2113a.java

RULE ID	BEHAVIOUR LABEL		FILES
00209	Get pixels from the latest rendered image	collection	com/zipow/nydus/camera/CameraCaptureImplV2.java us/zoom/internal/share/ScreenShareServer.java
00011	Query data from URI (SMS, CALLLOGS) sms calllog collection		com/appsflyer/internal/AFb1wSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1oSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1wSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1oSDK.java
00183	Get current camera parameters and change the setting.	camera	com/vonage/webrtc/Camera1Session.java com/zipow/nydus/camera/CameraCaptureImplV1.java com/zipow/nydus/camera/CameraMgrV1.java
00002	Open the camera and take picture camera		com/zipow/nydus/camera/CameraCaptureImplV1.java
00114	Create a secure socket connection to the proxy address	network command	G8/f.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFf1hSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFf1hSDK.java
00078	Get the network operator name collection telephony		com/appsflyer/internal/AFa1gSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://betterhelp-141121.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/870724514862/namespaces/firebase:fetch? key=AlzaSyAg5YDfsF3fviLetDITUdq2wzvpdVla4mA. This is indicated by the response: The response code is 403

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	7/44	com.google.android.c2dm.permission.RECEIVE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY

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

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
support.link.co	ok	IP: 18.238.109.117 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
sinapps.s	ok	No Geolocation information available.
api.opentok.com	ok	IP: 168.100.107.128 Country: United States of America Region: New Jersey City: Holmdel Latitude: 40.383961 Longitude: -74.170563 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.stripe.com	ok	IP: 54.149.153.72 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
issuetracker.google.com	ok	IP: 64.233.177.102 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	ok	IP: 172.253.124.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sdlsdk.s	ok	No Geolocation information available.
www.twilio.com	ok	IP: 18.238.96.15 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	IP: 162.159.140.229 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebase.google.com	ok	IP: 74.125.136.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sconversions.s	ok	No Geolocation information available.
errors.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
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 64.233.176.101 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
eventgw.twilio.com	ok	IP: 3.216.226.112 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
betterhelp.com	ok	IP: 166.117.115.19 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map

DOMAIN	STATUS	GEOLOCATION
sars.s	ok	No Geolocation information available.
www.betterhelp.com	ok	IP: 166.117.210.39 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map
pagead2.googlesyndication.com	ok	IP: 64.233.185.154 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
m.stripe.com	ok	IP: 52.40.40.91 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
link.co	ok	IP: 13.224.53.87 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
svalidate.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
www.cdn.stripe.com	ok	No Geolocation information available.
accounts.google.com	ok	IP: 172.217.215.84 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
static.afterpay.com	ok	IP: 104.19.176.211 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
b.stripecdn.com	ok	IP: 18.238.96.22 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
api.iterable.com	ok	IP: 34.198.98.21 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	IP: 44.240.26.72 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
stripe.com	ok	IP: 35.166.203.173 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
ers.twilio.com	ok	IP: 44.193.123.32 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sapp.s	ok	No Geolocation information available.
q.stripe.com	ok	IP: 54.186.23.98 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	IP: 142.250.9.94 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sviap.s	ok	No Geolocation information available.
dashboard.stripe.com	ok	IP: 54.189.200.54 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
betterhelp-141121.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
zoom.us	ok	IP: 170.114.52.2 Country: United States of America Region: California City: San Jose Latitude: 37.333698 Longitude: -121.889297 View: Google Map

DOMAIN	STATUS	GEOLOCATION
r.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

EMAILS

EMAIL	FILE
email@example.com	m6/C3350b.java
support@stripe.com	y6/C4314f.java
support@stripe.com	q5/C3540a.java
support@stripe.com	v5/h.java

A TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12

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

HARDCODED SECRETS

POSSIBLE SECRETS "com.google.firebase.crashlytics.mapping_file_id": "d24521d3b69e41f0b894ea48fea3c613" "firebase_database_url": "https://betterhelp-141121.firebaseio.com" "google_api_key": "AlzaSyAg5YDfsF3fviLetDITUdq2wzvpdVla4mA" "google_crash_reporting_api_key" : "AlzaSyAg5YDfsF3fviLetDITUdq2wzvpdVla4mA" "session_snap_close": "Close" "session_snap_disable": "Disable" "session_snap_v1_change" : "Change" "session_snap_v1_dismiss" : "Dismiss" 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 115792089237316195423570985008687907853269984665640564039457584007908834671663

POSSIBLE SECRETS

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a9 78d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

 $68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166\\43812574028291115057151$

27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

41058363725152142129326129780047268409114441015993725554835256314039467401291

c06c8400-8e06-11e0-9cb6-0002a5d5c51b

470fa2b4ae81cd56ecbcda9735803434cec591fa

362aa53c4499935d0f4d198115f16d2a055af9af

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

dcb428fea25c40e7b99f81ae5981ee6a

32670510020758816978083085130507043184471273380659243275938904335757337482424

FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057148

bb392ec0-8d4d-11e0-a896-0002a5d5c51b

POSSIBLE SECRETS
deca87e736574c5c83c07314051fd93a
10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910 12912142327488478985984
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
55066263022277343669578718895168534326250603453777594175500187360389116729240
48439561293906451759052585252797914202762949526041747995844080717082404635286
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965 80810124344277578376784
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
115792089237316195423570985008687907852837564279074904382605163141518161494337
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

POSSIBLE SECRETS

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

66f1fdf802dc4d79879076247e061b97



Title: BetterHelp - Therapy

Score: 4.6455326 Installs: 1,000,000+ Price: 0 Android Version Support: Category: Health & Fitness Play Store URL: com.betterhelp

Developer Details: BetterHelp - Therapy Made Easy, BetterHelp+-+Therapy+Made+Easy, None, https://www.betterhelp.com, contact@betterhelp.com,

Release Date: Nov 17, 2014 Privacy Policy: Privacy link

Description:

BetterHelp is the convenient way to get professional help from a licensed therapist. With over 20,000 trained, experienced, and accredited therapists covering a wide ------ BETTERHELP – FEATURES ------ • Over 20,000 licensed, accredited, and highly experienced therapists • Match with an available therapist who best fits your needs • Unlimited private one on one communication with your therapist • Schedule live sessions with your therapist or use the secure messenger • Gain access to constructive, educational group webinars PROFESSIONAL HELP, PERSONALIZED FOR YOU Facing obstacles alone can be daunting – receiving support and guidance from a professional therapist has been shown to make huge, positive changes to help you overcome personal challenges. When you sign up we'll match you to an available therapist who fits your objectives, preferences and the type of issues you're dealing with. Different therapists have different approaches and areas of expertise so we'll work with you to find the right person who can achieve the best results for you. LICENSED AND TRAINED THERAPISTS There are over 20,000 therapists on BetterHelp, each with at least 3 years and 1,000 hours of hands-on experience. They are licensed, trained, experienced, and accredited psychologists (Ph.D./PsyD), marriage and family therapists (MFT), clinical social workers (LCSW), licensed professional therapists (LPC), or similar credentials. All of our therapists have a Master's Degree or a Doctorate Degree in their respective fields. They have been qualified and certified by their state professional board and have completed the necessary education, exams, training, and practice. HOW DOES IT WORK? After filling out our questionnaire, you will be matched with a licensed therapist based on your needs and preferences. You and your therapist will get your own secure and private "therapy room" where you can message your therapist at any time, from any internet-connected device, wherever you are. You can also schedule a weekly session to speak live with your therapist over video or phone. You can write or talk about yourself, the things going on in your life, ask questions, and discuss the challenges you're facing and your therapist will provide feedback, insights, and guidance. This ongoing one-on-one dialogue is the foundation of your work with your therapist. Together you'll work towards making a positive change in your life, accomplishing your goals, and overcoming your problems. HOW MUCH DOES IT COST? The cost of therapy through BetterHelp ranges from \$60 to \$90 per week (billed every 4 weeks) but may be higher based on your location, preferences, and therapist availability. Unlike traditional in-office therapy which can cost over \$150 for a single session, your BetterHelp membership includes unlimited text, video, audio messaging as well as weekly live sessions. The subscription is billed and renewed every 4 weeks and includes both the use of the secured site and the therapy service itself. You can cancel your membership at any time for any reason.

E SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:09:26	Generating Hashes	ОК

2025-08-29 20:09:26	Extracting APK	OK
2025-08-29 20:09:26	Unzipping	OK
2025-08-29 20:09:26	Parsing APK with androguard	ОК
2025-08-29 20:09:27	Extracting APK features using aapt/aapt2	ОК
2025-08-29 20:09:27	Getting Hardcoded Certificates/Keystores	ОК
2025-08-29 20:09:29	Parsing AndroidManifest.xml	ОК
2025-08-29 20:09:29	Extracting Manifest Data	ОК
2025-08-29 20:09:29	Manifest Analysis Started	ОК
2025-08-29 20:09:29	Performing Static Analysis on: BetterHelp (com.betterhelp)	OK
2025-08-29 20:09:30	Fetching Details from Play Store: com.betterhelp	OK
2025-08-29 20:09:30	Checking for Malware Permissions	ОК

2025-08-29 20:09:30	Fetching icon path	ОК
2025-08-29 20:09:30	Library Binary Analysis Started	ОК
2025-08-29 20:09:31	Reading Code Signing Certificate	ОК
2025-08-29 20:09:31	Running APKiD 2.1.5	ОК
2025-08-29 20:09:35	Detecting Trackers	ОК
2025-08-29 20:09:37	Decompiling APK to Java with JADX	ОК
2025-08-29 20:09:51	Converting DEX to Smali	ОК
2025-08-29 20:09:51	Code Analysis Started on - java_source	ОК
2025-08-29 20:09:55	Android SBOM Analysis Completed	ОК
2025-08-29 20:10:02	Android SAST Completed	ОК

2025-08-29 20:10:02	Android API Analysis Started	ОК
2025-08-29 20:10:09	Android API Analysis Completed	ОК
2025-08-29 20:10:09	Android Permission Mapping Started	ОК
2025-08-29 20:10:22	Android Permission Mapping Completed	ОК
2025-08-29 20:10:22	Android Behaviour Analysis Started	ОК
2025-08-29 20:10:31	Android Behaviour Analysis Completed	ОК
2025-08-29 20:10:31	Extracting Emails and URLs from Source Code	ОК
2025-08-29 20:10:35	Email and URL Extraction Completed	ОК
2025-08-29 20:10:35	Extracting String data from APK	ОК
2025-08-29 20:10:35	Extracting String data from Code	ОК

2025-08-29 20:10:35	Extracting String values and entropies from Code	ОК
2025-08-29 20:10:37	Performing Malware check on extracted domains	ОК
2025-08-29 20:10:40	Saving to Database	ОК

Report Generated by - MobSF v4.4.0

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

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.