ANDROID STATIC ANALYSIS REPORT

Rejoyn (1.2.2)

File Name:	com.oph.prod.ct152.rejoyn_2801.apk
Package Name:	com.oph.prod.ct152.rejoyn
Scan Date:	Sept. 1, 2025, 6:41 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	1	1

FILE INFORMATION

File Name: com.oph.prod.ct152.rejoyn_2801.apk
Size: 68.44MB
MD5: 19a9b2acae7ddd2aa49d508653cf4e62
SHA1: 01591b29308bc11a95806df97b37a6a0562a62ae
SHA256: 13238c1504aa5bd6632b5dc4fa3cd7a3add1c5b1dd6440bc76fcef1f4506b558

APP INFORMATION

App Name: Rejoyn
Package Name: com.oph.prod.ct152.rejoyn
Main Activity: com.clicktherapeutics.ct152dev.MainActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.2.2

Android Version Code: 2801

APP COMPONENTS

Activities: 2
Services: 9
Receivers: 13
Providers: 3
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
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=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-07-08 20:45:59+00:00
Valid To: 2054-07-08 20:45:59+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x75b1dced379dbd08da5c4f150a0c8214458471b6
Hash Algorithm: sha256
md5: 70ad4a6ea846a570e58b391829e7a500
sha1: f0457087ea3144fe19800d4fd6ed61263a4036ca
sha256: 3db9c91da9bbaa0c3799229e2b10ba9828dda176864671f2366692cdcd523cb0
sha512: 1dca74de8e03d1f212e420d1ad9b6e27c858a9f99e2c916c7b4826012590237b75e6052a09d96dde4d74680f5ab9880aa647dd2290ee8dd3b92aa93007246bf6
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 95bb312cbe478cbafc1c4736fd7a7731123609d57dd6dcca3e3f21ef593868d3
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
com.oph.prod.ct152.rejoyn.deveventspermission	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>possible Build.SERIAL 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>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>Anti-VM Code</td><td>possible Build.SERIAL check</td></tr>
<tr><td>Protector</td><td>Appdome (dex)</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes3.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>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.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>network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.clicktherapeutics.ct152dev.MainActivity	Schemes: @string/deep_link_host://, http://, https://, Hosts: @string/deep_link_host, Path Prefixes: @string/deep_link_path_prefix,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	10.0.2.2 localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: **0** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	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.
4	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.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/next/MIGRATION_TO_NEXT.java mx_com/mixpanel/android/mpmetrics/AnalyticsMessages.java mx_com/mixpanel/android/mpmetrics/ConfigurationChecker.java mx_com/mixpanel/android/mpmetrics/MPConfig.java mx_com/mixpanel/android/mpmetrics/MPDbAdapter.java mx_com/mixpanel/android/mpmetrics/MixpanelAPI.java mx_com/mixpanel/android/mpmetrics/PersistentIdentity.java mx_com/mixpanel/android/mpmetrics/ResourceReader.java mx_com/mixpanel/android/mpmetrics/SessionMetadata.java mx_com/mixpanel/android/mpmetrics/SystemInformation.java mx_com/mixpanel/android/util/HttpService.java mx_com/mixpanel/android/util/MPLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java mx_com/mixpanel/android/mpmetrics/MPDbAdapter.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/a.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/a.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/a.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/a.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/a.java
00036	Get resource file from res/raw directory	reflection	me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java me/leolin/shortcutbadger/impl/a.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00013	Read file and put it into a stream	file	com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java okio/p.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java mx_com/mixpanel/android/mpmetrics/MPDbAdapter.java
00096	Connect to a URL and set request method	command network	mx_com/mixpanel/android/util/HttpService.java
00089	Connect to a URL and receive input stream from the server	command network	mx_com/mixpanel/android/util/HttpService.java
00109	Connect to a URL and get the response code	network command	mx_com/mixpanel/android/util/HttpService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	mx_com/mixpanel/android/util/HttpService.java
00108	Read the input stream from given URL	network command	mx_com/mixpanel/android/util/HttpService.java
00078	Get the network operator name	collection telephony	mx_com/mixpanel/android/mpmetrics/SystemInformation.java
00004	Get filename and put it to JSON object	file collection	mx_com/mixpanel/android/mpmetrics/MPDbAdapter.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.VIBRATE, android.permission.WRITE_SETTINGS, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.READ_CALENDAR, 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
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
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

TRACKERS

TRACKER	CATEGORIES	URL
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

HARDCODED SECRETS

POSSIBLE SECRETS
"library_bottomdialogs_author" : "]!`~+-4821"
"library_bottomdialogs_authorWebsite" : "]!`~+-4822"
85053bf24bba75239b16a601d9387e17

PLAYSTORE INFORMATION

Title: Rejoyn™

Score: 3.8444445 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.oph.prod.ct152.rejoyn

Developer Details: Otsuka Precision Health, Inc., Otsuka+Precision+Health,+Inc., None, https://www.rejoyn.com, Connect@otsuka-oph.com,

Release Date: Jul 25, 2024 **Privacy Policy:** Privacy link

Description:

Meet Rejoyn™, the first and only add-on prescription app for the treatment of major depressive disorder symptoms, also known as depression. Rejoyn is authorized by the FDA for adults age 22+ who want to add to their antidepressant medication. Over the course of 6 weeks, Rejoyn delivers proven brain-training exercises and short skills-based therapy lessons. Unlike wellness apps, Rejoyn was studied in a phase 3 clinical trial and is classified as a medical device. Rejoyn requires a prescription from a healthcare provider. The brain-training exercises in Rejoyn were developed and studied by a team of psychologists, psychiatrists, and neuroscientists. In a clinical trial, adding Rejoyn to antidepressant medication reduced depression symptoms with zero side effects related to Rejoyn. The exercises and lessons in Rejoyn tap into the brain's natural ability to change, known as neuroplasticity. You can think of it like physical therapy, but for your brain. Using Rejoyn for less than 2 hours per week for 6 weeks is designed to change how the brain works, which can improve depression symptoms. Rejoyn core functionality also includes reminders to help keep you on schedule. For example, if your treatment session is interrupted, you will be prompted to return to complete your exercise within 15 minutes so that you don't lose your progress. Interested in trying Rejoyn? Rejoyn must be prescribed by a healthcare provider. Talk to your provider about Rejoyn or learn how you can consult with a provider online at www.rejoyn.com. Already have a prescription? Download the app to get started. Once Rejoyn is downloaded, the app will guide you through setting up your account. For more information, visit www.rejoyn.com. See Patient Instructions for Use at https://www.rejoyn.com/Patient-Instructions-for-Use.pdf. INDICATION: Rejoyn is a prescription digital therapeutic for the treatment of Major Depressive Disorder (MDD) symptoms as an adjunct to clinician-managed outpatient care for adult patients with MDD age 22 years and older who are on antidepressant medication. It is intended to reduce MDD symptoms. SAFETY INFORMATION: Rejoyn is not intended to be used as a standalone treatment. Rejoyn does not replace your current medication, including medication for treatment of MDD. You should continue your current treatment as directed by your healthcare provider. Rejoyn cannot send alerts or warnings to your healthcare provider. If you feel that your depression symptoms are worsening or if you have feelings or thoughts of harming yourself or others, please contact your healthcare provider, dial 911, or go to the nearest emergency room immediately. To review the developer's Privacy Policy, visit http://www.rejoyn.com/app-privacy-policy-html. © 2024 Otsuka Precision Health, Inc. All rights reserved. September 2024 20US24EBC0073

SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:41:40	Generating Hashes	OK
2025-09-01 06:41:43	Extracting APK	OK
2025-09-01 06:41:43	Unzipping	OK
2025-09-01 06:41:49	Parsing APK with androguard	OK
2025-09-01 06:41:50	Extracting APK features using aapt/aapt2	OK

2025-09-01 06:41:50	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:41:52	Parsing AndroidManifest.xml	OK
2025-09-01 06:41:52	Extracting Manifest Data	OK
2025-09-01 06:41:52	Manifest Analysis Started	OK
2025-09-01 06:41:52	Reading Network Security config from network_security_config.xml	OK
2025-09-01 06:41:52	Parsing Network Security config	OK
2025-09-01 06:41:52	Performing Static Analysis on: Rejoyn (com.oph.prod.ct152.rejoyn)	OK
2025-09-01 06:41:54	Fetching Details from Play Store: com.oph.prod.ct152.rejoyn	OK
2025-09-01 06:41:55	Checking for Malware Permissions	OK
2025-09-01 06:41:55	Fetching icon path	OK
2025-09-01 06:41:55	Library Binary Analysis Started	OK

2025-09-01 06:41:55	Reading Code Signing Certificate	OK
2025-09-01 06:41:56	Running APKiD 2.1.5	OK
2025-09-01 06:41:59	Detecting Trackers	OK
2025-09-01 06:42:00	Decompiling APK to Java with JADX	OK
2025-09-01 06:42:09	Converting DEX to Smali	OK
2025-09-01 06:42:09	Code Analysis Started on - java_source	OK
2025-09-01 06:42:09	Android SBOM Analysis Completed	OK
2025-09-01 06:42:13	Android SAST Completed	OK
2025-09-01 06:42:13	Android API Analysis Started	OK
2025-09-01 06:42:16	Android API Analysis Completed	OK
2025-09-01 06:42:17	Android Permission Mapping Started	OK

2025-09-01 06:42:20	Android Permission Mapping Completed	OK
2025-09-01 06:42:20	Android Behaviour Analysis Started	OK
2025-09-01 06:42:23	Android Behaviour Analysis Completed	OK
2025-09-01 06:42:23	Extracting Emails and URLs from Source Code	OK
2025-09-01 06:42:24	Email and URL Extraction Completed	OK
2025-09-01 06:42:24	Extracting String data from APK	OK
2025-09-01 06:42:24	Extracting String data from Code	OK
2025-09-01 06:42:24	Extracting String values and entropies from Code	OK
2025-09-01 06:42:24	Performing Malware check on extracted domains	OK
2025-09-01 06:42:25	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment

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.