MOBSF

ANDROID STATIC ANALYSIS REPORT

Day1Labs (1.3.0)

File Name:	org.goodlab.day1labs_10.apk
Package Name:	org.goodlab.day1labs
Scan Date:	Sept. 1, 2025, 3:06 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	23	3	1	1

FILE INFORMATION

File Name: org.goodlab.day1labs_10.apk
Size: 4.19MB
MD5: f668d270be59e411c16ba64a2c63783b
SHA1: f7995cfa3e5ef06e4fb237a4d47c9504be80bb2d
SHA256: fbaf210fdc2862dcff5870c8e5969c2c09fbf0387eab40855aaa4f30fbdfcd5c

APP INFORMATION

App Name: Day1Labs
Package Name: org.goodlab.day1labs
Main Activity: org.goodlab.day1labs.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.3.0

Android Version Code: 10

APP COMPONENTS

Activities: 12
Services: 13
Receivers: 18
Providers: 4
Exported Activities: 4
Exported Services: 1
Exported Receivers: 7
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, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-06-10 08:48:08+00:00
Valid To: 2054-06-10 08:48:08+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4f6a70e8af88b1f5eaca12d1142228da9da34c44
Hash Algorithm: sha256
md5: 3482c31856065b4ab1736862ca408ed8
sha1: 15e1567039b1d0b9e17ad387dcc8fd13418b8eeb
sha256: 6392e07b8454033ab9fdb5c9fb8f099e8050a1ce14e1b11a27889b95c84e084c
sha512: 2120c65fd953e4e3902f7ff27591707c88778179f3e2e1eebaeffddcdeb2b45d9c18f6c4d480a3744650db53bb40d6811e89bdea1431d79f644b079d835f92f0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: d7f548ea20007791286bf439b09373b01126ccfdebb0f74759ac6bcb0aade4df
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

PERMISSION	STATUS	INFO	DESCRIPTION
org.goodlab.day1labs.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
org.goodlab.day1labs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.org.goodlab.day1labs,

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 14 | 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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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
3	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 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.
4	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) 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	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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
9	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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	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.
11	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.
12	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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	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.
14	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.
15	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **3** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c6/b.java com/onesignal/debug/internal/logging/a.java d2/f0.java d2/m0.java d2/n0.java d2/w.java d5/a.java d6/c.java e5/a.java f0/a.java f4/b.java f4/b0.java f4/d.java f4/e0.java f4/f0.java f4/l.java f4/y.java f4/z.java g4/e.java g4/e0.java g4/i.java g4/j.java g4/j0.java g4/m.java g4/v.java g4/z.java h/e.java h/g.java h/h.java h/j.java h0/a.java h2/c.java h4/h.java i4/g0.java io/flutter/plugins/googlemobileads/b.java

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	io/flutter/plugins/googlemobileads/a.java io/flutter/plugins/googlemobileads/e0.java io/flutter/plugins/googlemobileads/f0.java io/flutter/plugins/googlemobileads/i0.java io/flutter/plugins/googlemobileads/k.java io/flutter/plugins/googlemobileads/p.java io/flutter/plugins/googlemobileads/u.java io/flutter/plugins/googlemobileads/w.java io/flutter/plugins/googlemobileads/x.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/o3.java j4/a.java j4/a0.java j4/a1.java j4/c.java j4/c1.java j4/d0.java j4/h0.java j4/i1.java j4/m1.java j4/v0.java j4/y0.java j4/z0.java k3/a.java k3/d.java l/g.java l0/a.java l5/e.java m/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m1/a.java m2/e.java m4/b.java n1/g.java n1/j0.java n1/n0.java n1/x0.java n2/a0.java n2/x.java n4/g.java n4/r.java n4/s.java o1/d.java o1/g.java o1/n.java o1/o0.java o1/s.java o5/f.java o5/n.java pa/a.java pa/d.java q0/c.java qa/f.java r0/k0.java r0/o.java r0/o0.java r0/r.java r1/l.java r3/u1.java r4/b.java r8/c.java ra/i.java s1/e.java s1/f.java t/d.java t0/a.java t4/l.java u1/a.java u2/k.java v0/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w/f.java w1/d.java w1/f.java w1/i.java w1/j.java w1/m.java x0/a.java x2/a.java x4/b3.java x4/d1.java x4/n3.java x4/o.java x4/p0.java x4/q.java x4/r1.java x4/v0.java x4/w2.java x4/y2.java x9/b.java y/a.java z0/b.java z1/a.java
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	com/onesignal/core/internal/http/impl/d.java com/onesignal/inAppMessages/internal/display/impl/i.java com/onesignal/inAppMessages/internal/prompt/impl/b.java com/onesignal/notifications/bridges/a.java com/onesignal/notifications/internal/c.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java i1/d.java q1/g.java u8/a.java x8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	a2/b.java n1/b.java n1/l0.java n1/o0.java n1/x0.java n2/z.java u1/j.java
4	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	b3/m0.java b3/t0.java com/onesignal/session/internal/outcomes/impl/m.java g7/c.java w0/c.java
5	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/onesignal/inAppMessages/internal/display/impl/i.java
6	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/onesignal/inAppMessages/internal/display/impl/i.java
7	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	o1/e.java w1/m.java x4/o1.java
8	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	d2/m0.java ra/a.java ra/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/flutter/plugin/editing/d.java io/flutter/plugin/platform/g.java
10	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	c6/c.java r0/o0.java
11	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/onesignal/common/AndroidUtils.java d2/m0.java jb/a.java jb/b.java kb/a.java n1/n.java o3/v.java
12	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	c6/b.java m2/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	d6/c.java k3/d.java q1/g.java x4/n3.java
00022	Open a file from given absolute path of the file	file	aa/d.java r0/o0.java ra/i.java w0/d.java x0/a.java
00091	Retrieve data from broadcast	collection	com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java d2/f0.java n2/d0.java r3/j2.java x8/c.java
00003	Put the compressed bitmap data into JSON object	camera	n1/e0.java r1/l.java x4/d1.java
00096	Connect to a URL and set request method	command network	d6/c.java n1/e0.java q1/g.java x4/n3.java
00089	Connect to a URL and receive input stream from the server	command network	d6/c.java m2/c.java q1/g.java x4/n3.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java d2/a.java d2/f0.java d2/m0.java d2/n0.java d2/r0.java g4/f.java n2/c.java n3/s.java q3/a.java x4/d1.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java d2/m0.java d2/n0.java g4/f.java n3/s.java q3/a.java
00189	Get the content of a SMS message	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java
00188	Get the address of a SMS message	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java
00191	Get messages in the SMS inbox	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/a.java d2/f0.java d2/m0.java
00200	Query data from the contact list	collection contact	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java
00201	Query data from the call log	collection calllog	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java d2/f0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java d2/a.java d2/m0.java d2/n0.java d2/r0.java g4/f.java x8/e.java
00014	Read file into a stream and put it into a JSON object	file	a2/a.java c6/c.java f2/k.java x1/j.java
00013	Read file and put it into a stream	file	a2/a.java c6/c.java f2/k.java o1/g.java r0/o0.java t0/b.java w1/m.java x1/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	f2/c.java j2/a.java x1/f.java
00034	Query the current data network type	collection network	r3/c.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/e.java
00012	Read data and put it into a buffer stream	file	o1/g.java w1/m.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/l.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/l.java
00147	Get the time of current location	collection location	h/j.java
00075	Get location of the device	collection location	h/j.java
00115	Get last known location of the device	collection location	h/j.java
00015	Put buffer stream (data) to JSON object	file	d2/m0.java
00078	Get the network operator name	collection telephony	com/onesignal/common/b.java d2/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	d2/m0.java
00125	Check if the given file path exist	file	x1/f.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/733255903428/namespaces/firebase:fetch?key=AIzaSyD75O4RQKbRxqpzeiAbki2WzBcSrcdXzyw. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.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
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
api.onesignal.com	ok	**IP:** 104.16.160.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 216.58.207.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fundingchoicesmessages.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
graph.s	ok	No Geolocation information available.
googlemobileadssdk.page.link	ok	**IP:** 142.250.74.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	g4/u.java

TRACKERS

TRACKER	CATEGORIES	URL
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
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "76427e21adc1669875d4041eec3061d5"
"google_api_key" : "AIzaSyD75O4RQKbRxqpzeiAbki2WzBcSrcdXzyw"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyD75O4RQKbRxqpzeiAbki2WzBcSrcdXzyw"
TOlHmdp8XsKJiprHSu957VTnJJL2Dj58ytcwt3QLHDQ=
wsk3Vojf7RmX+WtFiGWOJo7xhFKFeiDn9iUtTCe0eNY=
FdxRYG9/HOndmgVdj1eVgDulreHUGSjsWl31nKn2TzY=
6diiPm6leEU3dn6Yh3093iP+CyZAN47Ila9hmZbBOygAlbw7IfYBD8oUvevGhzQp
ki2ip3Sp4zD5u1iHxdI5CQP+nQytWboRZ8YxUMq1u4GDs7rHoXiw6vz07EKttNE7
0BurIdBwA1Yjcso9P1TmQgVgvpSOR3INLha4uP5JdYXgWQEacWBPKA8E9hy+9dAe
t0k+Q4WGODPCHlTh1fiMgaVG6LJXWEyq2lqorD4gMCo=
zuOSwgzLq/YXiyJNPWGjICL0KrcqY8eXUxyiBgiihdg=
5BsC37pqFx3Fp5Qtv0y+RSU8LVttAMXjX8aFccLrzxg=
XE2927Ta6gTWmjrPmk4in7GLLwsXJnqTbhVN3N+/b3M=
8UEA9TmdE+sqV3zcsNgnFI5Sf8uIsQHU61W37Ddl8zaNqY23x/FpuoK+mm9MWruA
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
m4BHDSYRnsEEIrYlgM0yy1C5NfyYnIIeJvwgjuCY5HY=
af60eb711bd85bc1e4d3e0a462e074eea428a8

POSSIBLE SECRETS
8lD2ezwwsI93agi51tjtw1sdZVRU2vHPSc7HynOlFDE=
tk45mDotIpTZidmNYxxiIBsjVftw/e0h3Unlwpf2Me4=
ae2044fb577e65ee8bb576ca48a2f06e
c56fb7d591ba6704df047fd98f535372fea00211
ZzhYXgKMhken/ic2sDR8A53WLOTMzsBN7DfnMjKoyhk=
GZJYAQ87uqT/39Vw1xO4VkKaUA+BZKFiVkKasBC0VSw=
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
U5Ngb8pPuPEbyAEAeNCt0wgGFK4YAtkNGCrOQKfD/ONzQcV8GTtSZ6EoO3NY8V1s
nKZwK8oioxkTwDfG9V2sR2xNb9GbO72JaQ9OaUpmWGl7ZX+EiCwiESnhzEGly7cm

POSSIBLE SECRETS
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a1Na7bntM+sktGxZBhUnqailj8ITQ7piLQZ5OyqVU2HU4R0rOCZ63N/fUHG081A+
tJ+SvALjKnpAv9FF8u56pKKRS55/vzUDe+m9ct97Lx4=
36864200e0eaf5284d884a0e77d31646
ChMYhePBDqkXl5DeRTg9cgSXXNPVEcIqgEVciYHEVlkZyx/HkVQXSnen8aw33G2s
eISRjanjhAfdgJ9+lE3tGViJFRMvsuX1oVbmo+9k2XU=
J3qHQsXE9gxUWY3EQze3pD9LpRQkp3i0z4IBb3xvxMfPfsFZNBOU+l2pHi8zC3DO
gziBDgIPHk3UnbqAN9Ta9zRxJ8KBrTfiKBXyCZDQ588=
Q0EftCh9LNoL/97bVNRGH4YGKN2mjVuI8Ruidx0q8xs=
f+0D9BT8zkFXnX9yG742KHeQy11nhCJFb6PFndn+zMk=
W1peSRrFFzj+W6DyflucA6CQWTsphM4X4AkhjKjRy/o=
eEgPK4FD9N/fpMPwsM6h+Wvbqi3j4L5DBTwMY2KteC4=
9b8f518b086098de3d77736f9458a3d2f6f95a37
hIbo0WHjc5N2XBD7HI+Mwh9BXu/nIzOhdTaHZ1DPjeizuR48SZNCpBdtOxY4cHlb
c682b8144a8dd52bc1ad63

POSSIBLE SECRETS
69psxaRqrIVZzPpt4pN0wGmA/kc6O8gjOJlblyEzW1E=
WIPKXsZv2l0NBmLvWdV3TkucPJ5dkfbRYYrTASAxFfQ=
qlbJd0rViXaFpU2SvrkcezPlE/VtgXulMFWFUXmIBBg=
B3EEABB8EE11C2BE770B684D95219ECB
JHENilgoa32pdW2+FQZfbiKa1To+b6hAFc5hyxP6u/LWvHbIhkfTDC3kQMR4mpq3
IWYMNwupvIr4nCzhi63Y96rPhOxZK2U2oV0yQU5ISOuxDdywn/U6CBTwu78HOm4H
mLbfRIQxtPVbZphUgAhWqMeuqa25Ale/5rz8vv9YVkc=
CbnHJiUmcb7bV3nHtVfkQJESWUzuF9spYS2HkpVPEQ4sOQCQUFomcsL6vpMTm+JY
m4uJd6hJYeAUgFAUB1OT370Awen8YINd4hKC7XM/6ec=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
IcH9chIM8pdQBP/eeaIVQOxIkEFtHwPKwBzAXjYRdyw5KOKrZsfN3FYxHItVH2IL
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
JQeYWB/Ar5LqSSZ5i6IhxYZ+uXn8SEDYL9xPjgGTx2M=
CYcH4LBpiH+KaEScKuk48/IbmIORuaeHTHx2iwUA0vRWrbIkTWIgIbVYJ8eozDwX
somG6HzRa3YZJrwwnfL6K8d6jP9Npv493BtTLjfx2vaqxDUDPiPCNzpi42Jpggs8

POSSIBLE SECRETS
d4INySQwKXrFgcw/Yp0O6t4YGx7HF+F75DncE44LSIy22mr4UP50R657OPRB1jqZ
cc2751449a350f668590264ed76692694a80308a
AemuwIJaLmYE+nU5fadET3FINkdby4LnWDkawsC9pWk=
5181942b9ebc31ce68dacb56c16fd79f
Q2oRzQFBrNQ6PISKRcfuekSxxMHiBiKCGVgSnsIVkCh9YR7J4L17zMBZU0VVyUEU
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040 7130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403 1307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e 636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009 060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713 0d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403 1307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e 636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe 2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed 5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23 ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa 6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c 7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151 d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301 d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081 be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b300906035504061 3025553311330110603550408130a43616c69666f726e69631163014060355040713 0d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403 1307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e 636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d010104050003820101 0019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e6181 86673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c196 2fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb 21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
PyZj3I+LGZvAhJ9n3OQrlENydgM2JwW0T6dRxf3as8iTDiIpqvAE/3692CSblz+3
F0+pSvx9GtXcjR12oFzzp5apK08MRky74IYez805WxvZBZTjFs672zxMax8w5kp9

POSSIBLE SECRETS
2ZUgS25mCfmBpvNAAnoop42ZvK9H4E17vIqHMHWBgDSruAgpJ0/PRWhyN3sqcUbC
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
AtCF0F/Ugi3KOt6zYtgfLSsd+8KzXVTsnhwfj9NoYBY=
WQCGmUFTrgSOZ83nswxrNh39wVE6t1Ouq3E0zMLvIMA=
pY1LPqV65osROa0AkcabhXHjwpz5nP0HOapDW2QtdtU=
bae8e37fc83441b16034566b
ZqqofhkB4+yK9ARzF+IbcECpWBtuTXlqWFDkC/AVdcM=
nK4MIXXv/sY+coqtAjalB6f9NiJ1zVnlRnfsJ++LIaOoNJXY+cpXhUK9rjjc0N2G
hvOzu3pRF2dcNdvDy8db1rttL97bOQyvLLd+NabZhD5sRaprNsAQL2vdtDd+eY16
Srq4/7DDafVhhxKPQvFzGwPCcbAxjsRhBUoTZMyZ8i1elMwCHCPiECib9I+dpg+U

PLAYSTORE INFORMATION

Title: Day1Lab - Paid Clinical Trials

Score: 3.63 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** org.goodlab.day1labs

Developer Details: Day1Lab, Day1Lab, None, https://day1labs.org/gl2/, app@goodlab.org,

Release Date: Jun 10, 2024 **Privacy Policy:** Privacy link

Description:

Day1Labs is where patients go to get matched with clinical trials. Whether you are healthy, or have a mental or physical condition, we'll find the right trial for you, and keep you informed of upcoming trials suitable for you in your area. Not only will you get access to cutting edge medical treatment, you may also be compensated to participate in the clinical trials you qualify for.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 15:06:19	Generating Hashes	OK
2025-09-01 15:06:19	Extracting APK	OK
2025-09-01 15:06:19	Unzipping	OK
2025-09-01 15:06:19	Parsing APK with androguard	OK
2025-09-01 15:06:19	Extracting APK features using aapt/aapt2	OK
2025-09-01 15:06:19	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 15:06:20	Parsing AndroidManifest.xml	OK
2025-09-01 15:06:20	Extracting Manifest Data	OK

2025-09-01 15:06:20	Manifest Analysis Started	OK
2025-09-01 15:06:20	Performing Static Analysis on: Day1Labs (org.goodlab.day1labs)	OK
2025-09-01 15:06:22	Fetching Details from Play Store: org.goodlab.day1labs	OK
2025-09-01 15:06:23	Checking for Malware Permissions	OK
2025-09-01 15:06:23	Fetching icon path	OK
2025-09-01 15:06:23	Library Binary Analysis Started	OK
2025-09-01 15:06:23	Reading Code Signing Certificate	OK
2025-09-01 15:06:24	Running APKiD 2.1.5	OK
2025-09-01 15:06:27	Detecting Trackers	OK
2025-09-01 15:06:28	Decompiling APK to Java with JADX	OK
2025-09-01 15:06:39	Converting DEX to Smali	OK

2025-09-01 15:06:39	Code Analysis Started on - java_source	OK
2025-09-01 15:06:40	Android SBOM Analysis Completed	OK
2025-09-01 15:06:44	Android SAST Completed	OK
2025-09-01 15:06:44	Android API Analysis Started	OK
2025-09-01 15:06:48	Android API Analysis Completed	OK
2025-09-01 15:06:48	Android Permission Mapping Started	OK
2025-09-01 15:06:51	Android Permission Mapping Completed	OK
2025-09-01 15:06:52	Android Behaviour Analysis Started	OK
2025-09-01 15:06:56	Android Behaviour Analysis Completed	OK
2025-09-01 15:06:56	Extracting Emails and URLs from Source Code	OK

2025-09-01 15:06:58	Email and URL Extraction Completed	OK
2025-09-01 15:06:58	Extracting String data from APK	OK
2025-09-01 15:06:58	Extracting String data from Code	OK
2025-09-01 15:06:58	Extracting String values and entropies from Code	OK
2025-09-01 15:07:00	Performing Malware check on extracted domains	OK
2025-09-01 15:07:02	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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

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