MOBSF

ANDROID STATIC ANALYSIS REPORT

System Service (16.3)

File Name:	system-service.apk
Package Name:	com.sc.cocospy.v2
Scan Date:	Aug. 10, 2024, 6:38 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	20	1	2	1

FILE INFORMATION

File Name: system-service.apk
Size: 2.52MB
MD5: 755860f19e984c22b6d65dfeb376f4b0
SHA1: c537bfd4489a04813f1c3166929bb29113a670bb
SHA256: 176cd54005aeb64d2415685c0f97bdad0292e9ae2f307bb6908c2927d5edd3a2

APP INFORMATION

App Name: System Service
Package Name: com.sc.cocospy.v2
Main Activity: com.duiyun.activity.LauncherActivity
Target SDK: 22
Min SDK: 16
Max SDK:
Android Version Name: 16.3

Android Version Code: 92

APP COMPONENTS

Activities: 8
Services: 11
Receivers: 3
Providers: 1
Exported Activities: 0
Exported Services: 7
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=86, ST=sz, L=china, O=com.duiyun, OU=duiyun, CN=duiyun
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-14 10:05:53+00:00
Valid To: 2045-06-08 10:05:53+00:00
Issuer: C=86, ST=sz, L=china, O=com.duiyun, OU=duiyun, CN=duiyun
Serial Number: 0x7a6c6cdc
Hash Algorithm: sha256
md5: de469640523ae6e47a860ac2d83d411b
sha1: c377adff5df116ab7297d32850ade8a8fc3f8fb9
sha256: 613baa208b9d66a150d918a27146ecd9fbca9958d894cca590e9a4c4f4499746
sha512: 24be7fa16e8481ccb3a8c909f7fc2525953ff657c6d867edb01fec31a9ecd458f0b15c5135b3114744603e22101681ab5ab6fcf15dd76678f27e616e69d787af
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 247789f63db2b2b718f1a0dd576e0989cc4937900b219bfb91108e51e3519354
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.ACCOUNT_MANAGER	signature	act as the Account Manager Service	Allows an application to make calls to Account Authenticators.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.INSTALL_PACKAGES	SignatureOrSystem	directly install applications	Allows an application to install new or updated Android packages. Malicious applications can use this to add new applications with arbitrarily powerful permissions.
android.permission.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
android.permission.MODIFY_PHONE_STATE	SignatureOrSystem	modify phone status	Allows the application to control the phone features of the device. An application with this permission can switch networks, turn the phone radio on and off and the like, without ever notifying you.
com.sec.android.provider.logsprovider.permission.READ_LOGS	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.logsprovider.permission.WRITE_LOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.1-4.1.2, [minSdk=16]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
3	Broadcast Receiver (com.duiyun.activity.TakePhotoReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Service (com.duiyun.services.CancelNoticeService) 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.
5	Service (com.duiyun.services.UpdateDuanpingService) 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.
6	Service (com.duiyun.services.UpdateChangpingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.duiyun.services.UpdateRizhiService) 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.
8	Service (com.duiyun.services.UpdateLoggerNotificationService) 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.
9	Service (com.duiyun.account.TestSyncService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Service (com.duiyun.account.TestAuthService) 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.
11	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/duiyun/b.java com/umeng/analytics/pro/c.java com/umeng/analytics/pro/e.java com/umeng/analytics/pro/g.java
2	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/umeng/commonsdk/internal/utils/e.java com/umeng/commonsdk/internal/utils/l.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	c/a/a/f/h/t.java c/a/a/g/a.java com/duiyun/FileSender.java com/duiyun/activity/ScreenActivity.java com/duiyun/b.java com/duiyun/d.java com/duiyun/json/FileUtil.java com/duiyun/m/a.java com/duiyun/n/e.java com/duiyun/n/g.java com/umeng/commonsdk/internal/utils/f.java com/umeng/commonsdk/internal/utils/m.java
4	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/duiyun/util/e.java com/umeng/commonsdk/framework/e.java com/umeng/commonsdk/stateless/g.java rx/internal/util/i.java
5	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	c/a/a/f/g/a.java com/umeng/commonsdk/internal/utils/n.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	c/a/a/f/g/a.java com/umeng/commonsdk/stateless/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	c/a/a/f/g/a.java c/a/a/f/g/b.java c/a/a/f/g/c.java c/a/a/g/a.java com/duiyun/util/e.java com/umeng/commonsdk/stateless/g.java
8	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	c/a/a/f/g/a.java c/a/a/f/g/b.java c/a/a/g/a.java com/duiyun/util/e.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	c/a/a/f/i/f.java com/umeng/commonsdk/stateless/f.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	c/a/a/f/h/u.java c/a/a/f/i/f.java com/umeng/commonsdk/stateless/f.java
11	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	c/a/a/f/h/u.java com/alibaba/fastjson/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.GET_ACCOUNTS, android.permission.GET_TASKS, android.permission.INTERNET, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.READ_SMS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECEIVE_SMS, android.permission.SEND_SMS, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	9/45	android.permission.AUTHENTICATE_ACCOUNTS, android.permission.READ_CALENDAR, android.permission.ACCOUNT_MANAGER, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.WRITE_CONTACTS, android.permission.WRITE_SMS, android.permission.PACKAGE_USAGE_STATS, android.permission.CHANGE_NETWORK_STATE

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
developer.umeng.com	ok	No Geolocation information available.
alogus.umeng.com	ok	No Geolocation information available.
plbslog.umeng.com	ok	No Geolocation information available.
www.cocospy.com□□□□□□□□□	ok	No Geolocation information available.
ouplog.umeng.com	ok	No Geolocation information available.
lark.alipay.com	ok	No Geolocation information available.
opencellid.org	ok	No Geolocation information available.
cocospy.com	ok	No Geolocation information available.
ulogs.umengcloud.com	ok	No Geolocation information available.
cmnsguider.yunos.com	ok	No Geolocation information available.
ulogs.umeng.com	ok	No Geolocation information available.
alogsus.umeng.com	ok	No Geolocation information available.
www.cocospy.com	ok	No Geolocation information available.
www.cocospy.com□□□□□□□□□	ok	No Geolocation information available.
sp.kuuvv.com	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

HARDCODED SECRETS

POSSIBLE SECRETS
"please_input_pwd" : "□□□□□□□□□□□□□□□□"
FC1FE84794417B1BEF276234F6FB4E63
5b81591ff29d985f8d000069

SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:40:07	Reading Code Signing Certificate	OK
2024-08-10 18:40:08	Extracting APK	OK

2024-08-10 18:40:08	Unzipping	OK
2024-08-10 18:40:08	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:40:08	Parsing AndroidManifest.xml	OK
2024-08-10 18:40:08	Parsing APK with androguard	OK
2024-08-10 18:40:08	Running APKiD 2.1.5	OK
2024-08-10 18:40:08	Decompiling APK to Java with jadx	OK
2024-08-10 18:40:08	Extracting Manifest Data	OK
2024-08-10 18:40:09	Performing Static Analysis on: System Service (com.sc.cocospy.v2)	OK
2024-08-10 18:40:09	Fetching Details from Play Store: com.sc.cocospy.v2	OK
2024-08-10 18:40:09	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:40:09	Parsing AndroidManifest.xml	OK

2024-08-10 18:40:09	Parsing APK with androguard	OK
2024-08-10 18:40:09	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:40:09	Parsing AndroidManifest.xml	OK
2024-08-10 18:40:09	Parsing APK with androguard	OK
2024-08-10 18:40:09	Extracting Manifest Data	OK
2024-08-10 18:40:09	Manifest Analysis Started	OK
2024-08-10 18:40:10	Checking for Malware Permissions	OK
2024-08-10 18:40:10	Fetching icon path	OK
2024-08-10 18:40:10	Library Binary Analysis Started	OK
2024-08-10 18:40:10	Extracting Manifest Data	OK
2024-08-10 18:40:10	Performing Static Analysis on: System Service (com.sc.cocospy.v2)	OK

2024-08-10 18:40:10	Reading Code Signing Certificate	OK
2024-08-10 18:40:10	Fetching Details from Play Store: com.sc.cocospy.v2	OK
2024-08-10 18:40:10	Manifest Analysis Started	OK
2024-08-10 18:40:10	Checking for Malware Permissions	OK
2024-08-10 18:40:10	Fetching icon path	OK
2024-08-10 18:40:10	Library Binary Analysis Started	OK
2024-08-10 18:40:10	Reading Code Signing Certificate	OK
2024-08-10 18:40:10	Manifest Analysis Started	OK
2024-08-10 18:40:10	Checking for Malware Permissions	OK
2024-08-10 18:40:10	Fetching icon path	OK
2024-08-10 18:40:11	Library Binary Analysis Started	OK

2024-08-10 18:40:11	Reading Code Signing Certificate	OK
2024-08-10 18:40:11	Running APKiD 2.1.5	OK
2024-08-10 18:40:12	Running APKiD 2.1.5	OK
2024-08-10 18:40:12	Running APKiD 2.1.5	OK
2024-08-10 18:40:12	Decompiling APK to Java with jadx	OK
2024-08-10 18:40:13	Detecting Trackers	OK
2024-08-10 18:40:15	Detecting Trackers	OK
2024-08-10 18:40:15	Detecting Trackers	OK
2024-08-10 18:40:16	Decompiling APK to Java with jadx	OK
2024-08-10 18:40:18	Decompiling APK to Java with jadx	OK
2024-08-10 18:40:18	Decompiling APK to Java with jadx	OK

2024-08-10 18:40:20	Converting DEX to Smali	OK
2024-08-10 18:40:20	Code Analysis Started on - java_source	OK
2024-08-10 18:40:49	Converting DEX to Smali	OK
2024-08-10 18:40:49	Code Analysis Started on - java_source	OK
2024-08-10 18:41:04	Converting DEX to Smali	OK
2024-08-10 18:41:04	Code Analysis Started on - java_source	OK
2024-08-10 18:41:16	Converting DEX to Smali	OK
2024-08-10 18:41:16	Code Analysis Started on - java_source	OK
2024-08-10 18:41:20	Converting DEX to Smali	OK
2024-08-10 18:41:20	Code Analysis Started on - java_source	OK

2024-08-10 18:41:20	Converting DEX to Smali	OK
2024-08-10 18:41:21	Code Analysis Started on - java_source	OK
2024-08-10 18:41:46	Android SAST Completed	OK
2024-08-10 18:41:46	Android API Analysis Started	OK
2024-08-10 18:41:56	Android SAST Completed	OK
2024-08-10 18:41:56	Android API Analysis Started	OK
2024-08-10 18:41:58	Android SAST Completed	OK
2024-08-10 18:41:58	Android API Analysis Started	OK
2024-08-10 18:42:03	Android SAST Completed	OK
2024-08-10 18:42:03	Android API Analysis Started	OK

2024-08-10 18:42:05	Android SAST Completed	OK
2024-08-10 18:42:05	Android API Analysis Started	OK
2024-08-10 18:42:07	Android SAST Completed	OK
2024-08-10 18:42:07	Android API Analysis Started	OK
2024-08-10 18:42:22	Android Permission Mapping Started	OK
2024-08-10 18:42:34	Android Permission Mapping Started	OK
2024-08-10 18:42:43	Android Permission Mapping Started	OK
2024-08-10 18:42:52	Android Permission Mapping Started	OK
2024-08-10 18:42:53	Android Permission Mapping Started	OK
2024-08-10 18:42:57	Android Permission Mapping Started	OK

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.