# ANDROID STATIC ANALYSIS REPORT

## WiFi Service (1.0)

| | |
|---|---|
| File Name: | WiFiService.apk |
| Package Name: | com.pwamtsdb.wadswxwp |
| Scan Date: | Aug. 10, 2024, 7:34 p.m. |

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

## FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 2 | 21 | 2 | 2 | 1 |

## FILE INFORMATION

**File Name:** WiFiService.apk
**Size:** 3.47MB
**MD5:** 647f5b103be22efc22f2b015e5eb7405
**SHA1:** ae8c7639fa68527cebb19de8221ba83adb580b5f
**SHA256:** 85b4caf13687e73bb03a7d1245cd14e9b35b7ed85b0061141ca06eab09540d49

# APP INFORMATION

**App Name:** WiFi Service
**Package Name:** com.pwamtsdb.wadswxwp
**Main Activity:** com.pwamtsdb.wadswxwp.pBZYAxynTm
**Target SDK:** 28
**Min SDK:** 19
**Max SDK:**
**Android Version Name:** 1.0
**Android Version Code:** 1

# APP COMPONENTS

**Activities:** 20
**Services:** 13
**Receivers:** 10
**Providers:** 1
**Exported Activities:** 3
**Exported Services:** 4
**Exported Receivers:** 6
**Exported Providers:** 0

# CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=EQ, ST=DJutGacANq, L=qpjimbTgZV, O=gybwRrLbRs, OU=zDTZIuJijm, CN=clyzqtbbod@agqexoqgtp.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-04-22 18:30:07+00:00
Valid To: 2051-09-08 18:30:07+00:00
Issuer: C=EQ, ST=DJutGacANq, L=qpjimbTgZV, O=gybwRrLbRs, OU=zDTZIuJijm, CN=clyzqtbbod@agqexoqgtp.com
Serial Number: 0x7f3c5b53
Hash Algorithm: sha256
md5: 10c559a2cf4c0708f494d16727402ae4
sha1: 6d9f6b1ea93db3e2c632b90783cc36cfe3205286
sha256: fa92fbff587d79538543a2c5ce6c784d11a24a69989d3ade5c992da4382d8723
sha512: 0164eba92e64cd50c2689c125750de15ae0defd94b09b570845b521c3975b403254aae843759e384b62ecf0c294337fbe1987b91720a97d27e008a299cc04100
PublicKey Algorithm: rsa

Bit Size: 2048
Fingerprint: fd1f4cb5a4e4e59f491ab12d6cdf19f583edc01b02138e5ddaea6b0142998be6
Found 1 unique certificates

# APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| com.pwamtsdb.wadswxwp.permission.C2D_MESSAGE | unknown | Unknown permission | Unknown permission from android reference |
| 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. |
| 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.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.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.ANSWER_PHONE_CALLS | dangerous | permits an app to answer incoming phone calls. | Allows the app to answer an incoming phone call. |
| 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_LOGS | dangerous | read sensitive log data | Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information. |
| 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.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| android.permission.SDCARD_WRITE | unknown | Unknown permission | Unknown permission from android reference |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| 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_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_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| 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.MODIFY_AUDIO_SETTINGS | normal | change your audio settings | Allows application to modify global audio settings, such as volume and routing. |
| android.permission.RECORD_AUDIO | dangerous | record audio | Allows application to access the audio record path. |
| 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.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| 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.CHANGE_WIFI_STATE | normal | change Wi-Fi status | Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks. |
| android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS | normal | permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS. | Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| 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.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.BIND_DEVICE_ADMIN | signature | interact with device admin | Allows the holder to send intents to a device administrator. Should never be needed for common applications. |
| android.permission.CHANGE_NETWORK_STATE | normal | change network connectivity | Allows applications to change network connectivity state. |
| android.permission.ACCESS_SUPERUSER | unknown | Unknown permission | Unknown permission from android reference |
| 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.PACKAGE_USAGE_STATS | signature | update component usage statistics | Allows the modification of collected component usage statistics. Not for use by common applications. |
| android.permission.USES_POLICY_WIPE_DATA | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.BLUETOOTH_ADMIN | normal | bluetooth administration | Allows applications to discover and pair bluetooth devices. |
| 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.WRITE_SECURE_SETTINGS | SignatureOrSystem | modify secure system settings | Allows an application to modify the system's secure settings data. Not for use by common applications. |
| 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.GET_PACKAGE_SIZE | normal | measure application storage space | Allows an application to find out the space used by any package. |
| 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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.CHANGE_WIFI_MULTICAST_STATE | normal | allow Wi-Fi Multicast reception | Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode. |
| android.permission.BATTERY_STATS | signature | modify battery statistics | Allows the modification of collected battery statistics. Not for use by common applications. |
| android.permission.CHANGE_CONFIGURATION | SignatureOrSystem | change your UI settings | Allows an application to change the current configuration, such as the locale or overall font size. |
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |

## APKID ANALYSIS

| FILE | DETAILS |
|---|---|
| classes.dex | FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check<br>Build.TAGS check<br>FINDINGS: Compiler — DETAILS: dexlib 2.x |

## NETWORK SECURITY

| NO | SCOPE | SEVERITY | DESCRIPTION |
|---|---|---|---|

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

# MANIFEST ANALYSIS

HIGH: **2** | WARNING: **19** | INFO: **0** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | App can be installed on a vulnerable upatched Android version<br>Android 4.4-4.4.4, [minSdk=19] | 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 | Activity (com.pwamtsdb.wadswxwp.gWulxbGbub) is not Protected.<br>An intent-filter exists. | 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. The presence of intent-filter indicates that the Activity is explicitly exported. |
| 3 | Activity (com.pwamtsdb.wadswxwp.core.XxGoQwEmZD) is vulnerable to StrandHogg 2.0 | high | Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level. |
| 4 | Activity (com.pwamtsdb.wadswxwp.core.XxGoQwEmZD) is not Protected.<br>[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 | Launch Mode of activity (com.pwamtsdb.wadswxwp.NewAppSetting) is not standard. | warning | An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent. |
| 6 | Launch Mode of activity (com.pwamtsdb.wadswxwp.wekMutbUNH) is not standard. | warning | An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent. |
| 7 | Launch Mode of activity (com.pwamtsdb.wadswxwp.RLvqrAMqlY) is not standard. | warning | An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 8 | Activity-Alias (com.pwamtsdb.wadswxwp.cCfpUHmmwk) is not Protected.<br>An intent-filter exists. | warning | An Activity-Alias 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 Activity-Alias is explicitly exported. |
| 9 | Broadcast Receiver (com.pwamtsdb.wadswxwp.core.DecOYtEQmx) is not Protected.<br>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. |
| 10 | Broadcast Receiver (com.pwamtsdb.wadswxwp.core.bXjTjgzMou) is not Protected.<br>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. |
| 11 | Broadcast Receiver (com.pwamtsdb.wadswxwp.core.GeEpzzGilA) is not Protected.<br>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. |
| 12 | Broadcast Receiver (com.pwamtsdb.wadswxwp.LdZHhlvoaj) is Protected by a permission, but the protection level of the permission should be checked.<br>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. |
| 13 | Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected.<br>[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. |
| 14 | Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>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. |
| 15 | Broadcast Receiver (com.pwamtsdb.wadswxwp.core.EeMfergUzm) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 16 | Service (com.pwamtsdb.wadswxwp.core.listener.yGDGWuETWF) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_ACCESSIBILITY_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. |
| 17 | Service (com.pwamtsdb.wadswxwp.core.listener.uqNwrYmDmI) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_NOTIFICATION_LISTENER_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. |
| 18 | Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected.<br>[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. |
| 19 | High Intent Priority (1000)<br>[android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |
| 20 | High Intent Priority (1000)<br>[android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |
| 21 | High Intent Priority (2147483647)<br>[android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |

# </> CODE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **2** | SECURE: **1** | 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<br>OWASP MASVS: MSTG-STORAGE-3 | X/C0AF.java<br>X/C0At.java<br>X/C0bq.java<br>defpackage/vut.java<br>defpackage/vuu.java<br>u4/b.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 2 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | bo/app/f4.java<br>bo/app/g6.java |
| 3 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | defpackage/vuu.java |

## NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|

## ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 18/24 | android.permission.READ_CONTACTS, android.permission.READ_SMS, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WRITE_SETTINGS |
| Other Common Permissions | 16/45 | android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.READ_CALENDAR, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, android.permission.CHANGE_WIFI_STATE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.BIND_DEVICE_ADMIN, android.permission.CHANGE_NETWORK_STATE, android.permission.ACCESS_SUPERUSER, android.permission.PACKAGE_USAGE_STATS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY, android.permission.BATTERY_STATS, 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 |
|---|---|---|
| www.zetetic.net | ok | **IP:** 13.32.110.128<br>**Country:** United States of America<br>**Region:** California<br>**City:** Los Angeles<br>**Latitude:** 34.052231<br>**Longitude:** -118.243683<br>**View:** Google Map |
| github.com | ok | **IP:** 140.82.121.3<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

# HARDCODED SECRETS

| POSSIBLE SECRETS |
|---|
| "heLkOSCpWd" : "swxwp.CQ0J9BzwDrgO9llP6Dq2RehM9ky6hBzmCNMPJQniEAseFGNP3lDmT+sKug/bVwzXC8Ud1jvkR/xF3AbmSOBP64EKFBz4H/gMDhsbCbIQ+QgKWDzuTLSXc5hbnHVVqV5SZQ==" |
| "heLkOSCpWd" : "swxwp.dtGR0a/SVZ6a4qbgtNSb3LGUuuJUzKzGlV2p3J3Qrslm4aProt6d2qWln6agV6aVnqK5lsdQ47KNb05clWqbtIhSmw==" |
| "library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/" |
| "heLkOSCpWd" : "swxwp.gcSX0LHOnZejkJrlqIGizqvdtOep0LLWUJyYl5nVmcu1opXjouud5WSSpJ5SpaOkm6eulMSk2LLbVZyWkKfYttaZ26TtZuaVhH2CV1Nom6OIWJI=" |
| "heLkOSCpWd" : "swxwp.cs6k2KnYlpxV2bPgr4Gn27fpsZOhybHblZuZ7J7aoc+n4WPknuab36Whq6pSp5mdlKa3mteR17jOo06p1aviosqmjafZtNqV0mOcUFVcqFTUX4R0" |
| "heLkOSCpWd" : "swxwp.dMufj7PV+NelkBox6s9h5QYnp5OozAYWnpVX2fMCp4Sy3Pchp5il7KWfVvvDGO7voGF/UYpVoGfgXE5j" |
| "heLkOSCpWd" : "swxwp.ecSS2K/WqZNV1aWXscak2qzntZOkxbXDUJ2a7JzVmdZ12KDgpuGi2LZRpKamoJqZlaKomtKe1LaNp5Oh0ZzgsM+T0aTnZtaj0n2CV1Nom6OIZg==" |
| "heLkOSCpWd" : "swxwp.AQYAIRQDBeoFKgk0EuQD7xMsZkPoNAEy5/7pSMYx85BmRL1H90jllxTwB7cC7wW1Av8V4zPgQMU97V0FlgkvERUCHRMvFisF5hMaUP+4R+8x9jT4RMpIwkjpRwEB8wjBY1QA8REDARUS79w+xP7sQOlH/jLljRMrgJNbiXSGo1Vl" |

| POSSIBLE SECRETS |
| --- |
| c7bdf24df36c34d3f38547c084675fa6 |
| 9a88f3f80fa3930a8acb506b8ba7ca77 |

## SCAN LOGS

| Timestamp | Event | Error |
| --- | --- | --- |
| 2024-08-10 19:34:21 | Generating Hashes | OK |
| 2024-08-10 19:34:21 | Extracting APK | OK |
| 2024-08-10 19:34:21 | Unzipping | OK |
| 2024-08-10 19:34:21 | Getting Hardcoded Certificates/Keystores | OK |
| 2024-08-10 19:34:22 | Parsing AndroidManifest.xml | OK |
| 2024-08-10 19:34:22 | Parsing APK with androguard | OK |
| 2024-08-10 19:34:22 | Extracting Manifest Data | OK |
| 2024-08-10 19:34:22 | Performing Static Analysis on: WiFi Service (com.pwamtsdb.wadswxwp) | OK |
| 2024-08-10 19:34:22 | Fetching Details from Play Store: com.pwamtsdb.wadswxwp | OK |
| 2024-08-10 19:34:22 | Manifest Analysis Started | OK |

| | | |
|---|---|---|
| 2024-08-10 19:34:22 | Checking for Malware Permissions | OK |
| 2024-08-10 19:34:22 | Fetching icon path | OK |
| 2024-08-10 19:34:22 | Library Binary Analysis Started | OK |
| 2024-08-10 19:34:22 | Analyzing lib/armeabi-v7a/libeotcnzru.so | OK |
| 2024-08-10 19:34:22 | Analyzing lib/armeabi-v7a/libcrashlytics-handler.so | OK |
| 2024-08-10 19:34:22 | Analyzing lib/armeabi-v7a/libssfcxyix.so | OK |
| 2024-08-10 19:34:22 | Analyzing lib/arm64-v8a/libdoywgmmo.so | OK |
| 2024-08-10 19:34:22 | Analyzing apktool_out/lib/armeabi-v7a/libeotcnzru.so | OK |
| 2024-08-10 19:34:22 | Analyzing apktool_out/lib/armeabi-v7a/libcrashlytics-handler.so | OK |
| 2024-08-10 19:34:22 | Analyzing apktool_out/lib/armeabi-v7a/libssfcxyix.so | OK |
| 2024-08-10 19:34:23 | Analyzing apktool_out/lib/arm64-v8a/libdoywgmmo.so | OK |
| 2024-08-10 19:34:23 | Reading Code Signing Certificate | OK |
| 2024-08-10 19:34:23 | Running APKiD 2.1.5 | OK |
| 2024-08-10 19:34:24 | Detecting Trackers | OK |

| | | |
|---|---|---|
| 2024-08-10 19:34:24 | Decompiling APK to Java with jadx | OK |
| 2024-08-10 19:34:27 | Converting DEX to Smali | OK |
| 2024-08-10 19:34:27 | Code Analysis Started on - java_source | OK |
| 2024-08-10 19:34:28 | Android SAST Completed | OK |
| 2024-08-10 19:34:28 | Android API Analysis Started | OK |
| 2024-08-10 19:34:29 | Android Permission Mapping Started | OK |
| 2024-08-10 19:34:34 | Android Permission Mapping Completed | OK |
| 2024-08-10 19:34:34 | Finished Code Analysis, Email and URL Extraction | OK |
| 2024-08-10 19:34:34 | Extracting String data from APK | OK |
| 2024-08-10 19:34:34 | Extracting String data from SO | OK |
| 2024-08-10 19:34:35 | Extracting String data from Code | OK |
| 2024-08-10 19:34:35 | Extracting String values and entropies from Code | OK |
| 2024-08-10 19:34:35 | Performing Malware check on extracted domains | OK |
| 2024-08-10 19:34:38 | Saving to Database | 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.