



ANDROID STATIC ANALYSIS REPORT



 My Scan APP (2.0)

File Name: sample.apk

Package Name: com.IdjSxw.heBbQd






Scan Date: Nov. 19, 2024, 1:14 a.m.

App Security Score: **37/100 (HIGH RISK)**

Grade:



FINDINGS SEVERITY

|  HIGH |  MEDIUM |  INFO |  SECURE |  HOTSPOT |
|--|--|--|--|---|
| 5 | 8 | 0 | 1 | 1 |

FILE INFORMATION

File Name: sample.apk

Size: 33.5MB

MD5: f90f81f7b47ca73de0e5aa5aaeba6735

SHA1: f5c894ac5aeb6f23953b0dad7ff57dc937d95149

SHA256: 82d644a1f3bba120327e7eb6029f6b986c95c35f0c40cd43001f2dbedee2ee6f

APP INFORMATION

App Name: My Scan APP

Package Name: com.IdjSxw.heBbQd

Main Activity: com.IdjSxw.heBbQd.IntroActivity

Target SDK: 28

Min SDK: 23

Max SDK:

Android Version Name: 2.0

Android Version Code: 20

APP COMPONENTS

Activities: 4

Services: 5

Receivers: 3

Providers: 2

Exported Activities: 2

Exported Services: 2

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: C=CN, ST=Shanghai, L=ZB, O=Shanghai University, OU=NC, CN=tmp

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2023-10-16 12:18:00+00:00

Valid To: 2123-09-22 12:18:00+00:00

Issuer: C=CN, ST=Shanghai, L=ZB, O=Shanghai University, OU=NC, CN=tmp

Serial Number: 0xa2cda5f

Hash Algorithm: sha256

md5: 7eb61921f7d6a137681b91903163044f

sha1: 85e7916ac9aa2a5700f73140a9e40fa4ac0abab1

sha256: 006a72fa8f6dc3e38ebe32189d2101c191671bef63ed9eb919ccab20080bded3

sha512: 7af031cfe1ba6579a87736786da1a258f985ae64ae68825d60cd5da70838421275c11773dce4150181bd84d4411a9836baf4b7307cf8f2f289993af8ed9a2722

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: dd8f6a3567c31bb2e77b04e031044b734f0b13e1b68832daed4e36bf43615304

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_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.REQUEST_INSTALL_PACKAGES | dangerous | Allows an application to request installing packages. | Malicious applications can use this to try and trick users into installing additional malicious packages. |
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| android.permission.REQUEST_DELETE_PACKAGES | normal | enables an app to request package deletions. | Allows an application to request deleting packages. |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| android.permission.DISABLE_KEYGUARD | normal | disable keyguard | Allows applications to disable the keyguard if it is not secure. |
| android.permission.BOOT_COMPLETED | unknown | Unknown permission | Unknown permission from android reference |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|------------|--------|------|-------------|
|------------|--------|------|-------------|

| | | | |
|---|-----------|---------------------------------|---|
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| 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.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.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.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.RECEIVE_USER_PRESENT | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.MODIFY_AUDIO_SETTINGS | normal | change your audio settings | Allows application to modify global audio settings, such as volume and routing. |
| 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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|-----------|-------------------------------|--|
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.IdjSxw.heBbQd.permission.C2D_MESSAGE | unknown | Unknown permission | Unknown permission from android reference |
| 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. |

APKID ANALYSIS

| FILE | DETAILS | |
|-------------------------------|----------|---------|
| assets/pgsHZz.apk!classes.dex | FINDINGS | DETAILS |
| | Compiler | dx |
| classes.dex | FINDINGS | DETAILS |
| | Compiler | dx |

BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
|--------------------------------|-----------------------|
| com.IdjSxw.heBbQd.ScanActivity | Schemes: openscan://, |

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: 5 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|---|----------|--|
| 1 | App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23] | 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 | Clear text traffic is Enabled For App [android:usesCleartextTraffic=true] | high | The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected. |
| 3 | Debug Enabled For App [android:debuggable=true] | high | Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes. |
| 4 | Application Data can be Backed up [android:allowBackup=true] | warning | This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|--|
| 5 | Activity (com.IdjSxw.heBbQd.ResultActivity) 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. |
| 6 | Activity (com.IdjSxw.heBbQd.ResultActivity) 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. |
| 7 | Activity (com.IdjSxw.heBbQd.ScanActivity) 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. |
| 8 | Activity (com.IdjSxw.heBbQd.ScanActivity) 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 | Service (com.lджSxw.heBbQd.iservice.TaskService) is Protected by a permission, but the protection level of the permission should be checked. 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. |
| 10 | Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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 | 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. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|---|
| 12 | Service (com.google.firebase.iid.FirebaseInstanceIdService) 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. |

</> CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
|----|-------|----------|-----------|-------|

🚩 SHARED LIBRARY BINARY ANALYSIS

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------|----|-----|-----------------|-------|-------|---------|---------|---------------------|
|----|------------------|----|-----|-----------------|-------|-------|---------|---------|---------------------|

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------|---|--|---|--|---|---|--|---|
| 1 | armeabi-v7a/libset.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fpic flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------|---|--|---|--|---|---|--|---|
| 2 | armeabi-v7a/libset.so | True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return. | Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only. | None info The binary does not have run-time search path or RPATH set. | None info The binary does not have RUNPATH set. | False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries. | True info Symbols are stripped. |

NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|--|--------------|--|
| 00022 | Open a file from given absolute path of the file | file | com/lzsEsq/dykSgp/jhvqZx/pupsPVIbod.java |
| 00121 | Create a directory | file command | com/lzsEsq/dykSgp/jhvqZx/pupsPVIbod.java |
| 00125 | Check if the given file path exist | file | com/lzsEsq/dykSgp/jhvqZx/pupsPVIbod.java |
| 00104 | Check if the given path is directory | file | com/lzsEsq/dykSgp/jhvqZx/pupsPVIbod.java |

ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|--------------------------|---------|---|
| Malware Permissions | 12/25 | android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.VIBRATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE |
| Other Common Permissions | 5/44 | android.permission.FOREGROUND_SERVICE, android.permission.BROADCAST_STICKY, android.permission.CHANGE_WIFI_STATE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE |

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.openssl.org | ok | IP: 34.49.79.89 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map |

☰ SCAN LOGS

| Timestamp | Event | Error |
|---------------------|-------------------|-------|
| 2024-11-19 01:14:44 | Generating Hashes | OK |

| | | |
|---------------------|--|----|
| 2024-11-19 01:14:44 | Extracting APK | OK |
| 2024-11-19 01:14:44 | Unzipping | OK |
| 2024-11-19 01:14:44 | Getting Hardcoded Certificates/Keystores | OK |
| 2024-11-19 01:14:44 | Parsing APK with androguard | OK |
| 2024-11-19 01:14:46 | Parsing AndroidManifest.xml | OK |
| 2024-11-19 01:14:46 | Extracting Manifest Data | OK |
| 2024-11-19 01:14:46 | Performing Static Analysis on: My Scan APP (com.IdjSxw.heBbQd) | OK |
| 2024-11-19 01:14:46 | Fetching Details from Play Store: com.IdjSxw.heBbQd | OK |
| 2024-11-19 01:14:46 | Manifest Analysis Started | OK |
| 2024-11-19 01:14:46 | Checking for Malware Permissions | OK |

| | | |
|---------------------|---|----|
| 2024-11-19 01:14:46 | Fetching icon path | OK |
| 2024-11-19 01:14:46 | Library Binary Analysis Started | OK |
| 2024-11-19 01:14:46 | Analyzing apktool_out/lib/armeabi-v7a/libset.so | OK |
| 2024-11-19 01:14:47 | Analyzing lib/armeabi-v7a/libset.so | OK |
| 2024-11-19 01:14:47 | Reading Code Signing Certificate | OK |
| 2024-11-19 01:14:47 | Running APKiD 2.1.5 | OK |
| 2024-11-19 01:14:50 | Detecting Trackers | OK |
| 2024-11-19 01:14:50 | Decompiling APK to Java with JADX | OK |
| 2024-11-19 01:14:52 | Converting DEX to Smali | OK |
| 2024-11-19 01:14:52 | Code Analysis Started on - java_source | OK |

| | | |
|---------------------|--------------------------------------|----|
| 2024-11-19 01:14:53 | Android SAST Completed | OK |
| 2024-11-19 01:14:53 | Android API Analysis Started | OK |
| 2024-11-19 01:14:53 | Android API Analysis Completed | OK |
| 2024-11-19 01:14:53 | Android Permission Mapping Started | OK |
| 2024-11-19 01:14:54 | Android Permission Mapping Completed | OK |
| 2024-11-19 01:14:54 | Email and URL Extraction Completed | OK |
| 2024-11-19 01:14:54 | Android Behaviour Analysis Started | OK |
| 2024-11-19 01:14:55 | Android Behaviour Analysis Completed | OK |
| 2024-11-19 01:14:55 | Extracting String data from APK | OK |
| 2024-11-19 01:14:55 | Extracting String data from SO | OK |
| 2024-11-19 01:14:55 | Extracting String data from Code | OK |

| | | |
|---------------------|--|----|
| 2024-11-19 01:14:55 | Extracting String values and entropies from Code | OK |
| 2024-11-19 01:14:55 | Performing Malware check on extracted domains | OK |
| 2024-11-19 01:14:55 | Saving to Database | OK |
| 2024-11-19 01:23:32 | Performing Malware check on extracted domains | OK |
| 2024-11-19 01:23:42 | Detecting Trackers from Domains | OK |

Report Generated by - MobSF v4.1.9

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.