# MOBSF

## ANDROID STATIC ANALYSIS REPORT

Warehouse_Management (1.0)

| | |
|---|---|
| File Name: | app-debug.apk |
| Package Name: | put.dkotynski.warehouse.management |
| Scan Date: | Nov. 25, 2022, 5:54 p.m. |
| App Security Score: | 34/100 (HIGH RISK) |
| Grade: |  |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 3 | 1 | 0 | 1 | 0 |

# FILE INFORMATION

**File Name:** app-debug.apk
**Size:** 11.17MB
**MD5:** 139dd7de7e75f2ba712959aaf6424c66
**SHA1:** 7d283b7214faf132e22c9eaef9f25491453a3d1e
**SHA256:** 3b26ea2c15a6ef528b525cb79d7cc1e9b5567abba2e38f793485882c398e74f0

# APP INFORMATION

**App Name:** Warehouse_Management
**Package Name:** put.dkotynski.warehouse.management
**Main Activity:** put.dkotynski.warehouse.management.ui.login.LoginActivity
**Target SDK:** 32
**Min SDK:** 28
**Max SDK:**
**Android Version Name:** 1.0
**Android Version Code:** 1

# APP COMPONENTS

Activities: 4
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

# CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-07-11 08:20:51+00:00
Valid To: 2052-07-03 08:20:51+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: 3e38fb96381658a12ee0d7c3212f4844
sha1: 06b890f5b8d4d35b7b2ea7539c3393cde6f3adc5
sha256: c7178e25da5ebeb6bf7eeee2909d4b91bf9ddf6ebab6f687835830359eba66d8
sha512: aa7c62a924de99ee75127d3a66cd490ba87749aaf4079f4728b77f99bcd1c1299b021ff26c188b490c3e0b2d02113415cc9b6e1b074d80c119735f1f24260bad
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6ac6d4b99c9234b4f237c48551ecaeac321cd54cc1992f15f4e31a970160ceb1

| TITLE | SEVERITY | DESCRIPTION |
| --- | --- | --- |
| Signed Application | info | Application is signed with a code signing certificate |
| Application signed with debug certificate | high | Application signed with a debug certificate. Production application must not be shipped with a debug certificate. |

| | | |
|---|---|---|
| Certificate algorithm vulnerable to hash collision | high | Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. |

# APKID ANALYSIS

| FILE | DETAILS |
|---|---|
| classes3.dex | FINDINGS: DETAILS<br>yara_issue: yara issue - dex file recognized by apkid but not yara module<br>Compiler: unknown (please file detection issue!) |
| classes6.dex | FINDINGS: DETAILS<br>yara_issue: yara issue - dex file recognized by apkid but not yara module<br>Compiler: unknown (please file detection issue!) |
| classes4.dex | FINDINGS: DETAILS<br>yara_issue: yara issue - dex file recognized by apkid but not yara module<br>Compiler: unknown (please file detection issue!) |
| | FINDINGS: DETAILS |

| | | |
|---|---|---|
| classes5.dex | yara_issue | yara issue - dex file recognized by apkid but not yara module |
| | Compiler | unknown (please file detection issue!) |

| | | |
|---|---|---|
| classes2.dex | FINDINGS | DETAILS |
| | yara_issue | yara issue - dex file recognized by apkid but not yara module |
| | Compiler | unknown (please file detection issue!) |

| | | |
|---|---|---|
| classes.dex | FINDINGS | DETAILS |
| | yara_issue | yara issue - dex file recognized by apkid but not yara module |
| | Anti-VM Code | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check |
| | Compiler | unknown (please file detection issue!) |

## NETWORK SECURITY

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

## MANIFEST ANALYSIS

| | | | |
|---|---|---|---|

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | 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. |
| 2 | 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. |

# </> CODE ANALYSIS

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

# NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 1 | FCS_RBG_EXT.1.1 | Security Functional Requirements | Random Bit Generation Services | The application use no DRBG functionality for its cryptographic operations. |
| 2 | FCS_STO_EXT.1.1 | Security Functional Requirements | Storage of Credentials | The application does not store any credentials to non-volatile memory. |
| 3 | FCS_CKM_EXT.1.1 | Security Functional Requirements | Cryptographic Key Generation Services | The application generate no asymmetric cryptographic keys. |
| 4 | FDP_DEC_EXT.1.1 | Security Functional Requirements | Access to Platform Resources | The application has access to no hardware resources. |
| | | Security Functional | Access to Platform | |

| | | | | |
|---|---|---|---|---|
| 5 | FDP_DEC_EXT.1.2 | Requirements | Resources | The application has access to no sensitive information repositories. |
| 6 | FDP_NET_EXT.1.1 | Security Functional Requirements | Network Communications | The application has no network communications. |
| 7 | FDP_DAR_EXT.1.1 | Security Functional Requirements | Encryption Of Sensitive Application Data | The application implement functionality to encrypt sensitive data in non-volatile memory. |
| 8 | FMT_MEC_EXT.1.1 | Security Functional Requirements | Supported Configuration Mechanism | The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options. |
| 9 | FTP_DIT_EXT.1.1 | Security Functional Requirements | Protection of Data in Transit | The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product. |

---

## Report Generated by - MobSF v3.5.2 Beta

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.