MOBSF

ANDROID STATIC ANALYSIS REPORT

Secure Store (1.0)

File Name:	SecureStorev1.apk
Package Name:	com.androidpentesting.securestore
Scan Date:	May 17, 2023, 6 a.m.
App Security Score:	**73/100 (LOW RISK)**
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	2	0	1	1

FILE INFORMATION

File Name: SecureStorev1.apk
Size: 1.39MB
MD5: 66f893bcc5483c16b00a25e9c354987d
SHA1: b918e337105aab5cb5b80e11adacf5f7913df14e
SHA256: fb064bac413c3afc75e217d03412711098bac8ae13039c5497567a92c9c7a66c

APP INFORMATION

App Name: Secure Store
Package Name: com.androidpentesting.securestore
Main Activity: com.androidpentesting.securestore.UserMainActivity
Target SDK: 26
Min SDK: 16
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 4
Services: 0
Receivers: 0
Providers: 0
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: C=NA, ST=NA, L=NA, O=NA, OU=NA, CN=NA
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-11 01:53:08+00:00
Valid To: 2045-05-05 01:53:08+00:00
Issuer: C=NA, ST=NA, L=NA, O=NA, OU=NA, CN=NA
Serial Number: 0x6745c6b
Hash Algorithm: sha256
md5: 035dbbe4263c392687c0457858110ba9
sha1: 4c3cc5642b2f8a4b7cd67160edcbfa1d099be772
sha256: 611c6c332f4eb2bac485afa5e5cd8f5e26aad2058be1134f3108f77c1ec84cc9
sha512: 6c195d96d7808b5d6fddd3cea68f25a0747cfe87a4f93ead5bb4751aaf7b433f1b1ed67642c6aa94256e4639f6dcdcc8aa7d884893571bb3a91c20ef1c7f350f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5beae5b64592c17515b1338d4b4cd9bf3be4de961341f64ea3af2736ce3d5a56

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

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: 0 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=16]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
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 invoke platform-provided 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 ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book'].
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
12	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
13	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['RFC 5280 certificate validation and certificate path validation', 'The certificate path must terminate with a trusted CA certificate'].
14	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
