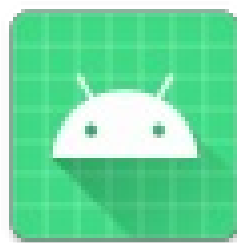




ANDROID STATIC ANALYSIS REPORT



 Oversecured Vulnerable
Android App

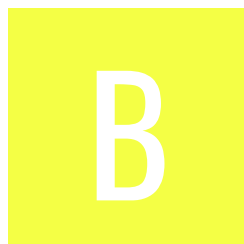
File Name: ovaa-master.zip

Package Name: oversecured.ovaa






Scan Date: April 15, 2022, 1:10 p.m.

App Security Score: 53/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	7	2	2	1

FILE INFORMATION

File Name: ovaa-master.zip

Size: 0.15MB

MD5: b04094fde20b1c20c3b927d0e0d2397f

SHA1: 1db5402202f6fe1a1bb093b4bac9d6efff6b3d10

SHA256: 85113e3007f43f0a5ea56b765cf542f3a945a0dfe95048c81b744db72d36dcd7

APP INFORMATION

App Name: Oversecured Vulnerable Android App

Package Name: oversecured.ovaa

Main Activity: .activities.EntranceActivity

Target SDK:

Min SDK:

Max SDK:

Android Version Name:

Android Version Code:

APP COMPONENTS

Activities: 5

Services: 1

Receivers: 1

Providers: 3

Exported Activities: 3

Exported Services: 1

Exported Receivers: 0

Exported Providers: 1

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
.activities.DeepLinkActivity	Schemes: oversecured://, Hosts: ovaa,

NETWORK SECURITY

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

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (.activities.DeepLinkActivity) is not Protected. 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 (.activities.LoginActivity) is not Protected. 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (.activities.MainActivity) is not Protected. 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.
5	Service (.services.InsecureLoggerService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
6	Content Provider (.providers.TheftOverwriteProvider) is not Protected. [android:exported=true]	high	A Content Provider 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
1	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	oversecured/ovaa/utils/LoginUtils.java
2	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	oversecured/ovaa/utils/LoginUtils.java oversecured/ovaa/activities/LoginActivity.java oversecured/ovaa/utils/WeakCrypto.java
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	oversecured/ovaa/providers/TheftOverwriteProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	oversecured/ovaa/network/RetrofitInstance.java
5	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	oversecured/ovaa/activities/LoginActivity.java
6	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	oversecured/ovaa/utis/WeakCrypto.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	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.
7	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.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).