

## ANDROID STATIC ANALYSIS REPORT



• Lexica (1.3.1)

File Name:	installer355.apk
Package Name:	com.serwylo.lexica
Scan Date:	May 31, 2022, 4:12 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	<b>i</b> INFO	<b>✓</b> SECURE	<sup>®</sup> HOTSPOT
1	4	1	1	0

#### FILE INFORMATION

File Name: installer355.apk

Size: 6.98MB

MD5: 358d94d3d88ed71a4901ef4c9865b826

SHA1: 32b1ab456cab959e2931223f0f7d108c286b22db

SHA256: 07862ddb685190e8f6d76fc8c9aee7522e1dafd7bbf52dfd7ab046b72d13dcfb

### **i** APP INFORMATION

App Name: Lexica

Package Name: com.serwylo.lexica

Main Activity: com.serwylo.lexica.MainMenuActivity

Target SDK: 28 Min SDK: 18 Max SDK:

Android Version Name: 1.3.1
Android Version Code: 10301

#### **APP COMPONENTS**

Activities: 4 Services: 0 Receivers: 0 Providers: 0

Exported Activities: 2 Exported Services: 0 Exported Receivers: 0 Exported Providers: 0

## **\*** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2016-01-11 09:34:46+00:00 Valid To: 2043-05-29 09:34:46+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x28c2d86c Hash Algorithm: sha256

md5: 6968aaf44ae5f85e7b1858a897beaa69

sha1: 8ea53bea8de1d78b260701e2efe817ce308bdbd8

sha 256: c82e0 f64 ca 38b 88c 8a 6e 6a 459183 f8b 831eb 3eaffe 033db da 13852331d57542 february 1995 february 19

sha512: 63293486e1128ba2cf8dc9918b93588c01c2ab9164d21063aaa91b7267edbb8e940a89e1c3c67a242d298d0eac603521fdb76bdcb7f4c186e9b417d978ff21e6

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

## **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check	
	Compiler	r8	

## **△** NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

# **Q** 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 (com.serwylo.lexica.GameActivity) 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 (com.serwylo.lexica.activities.score.ScoreActivity) 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.

## </> CODE ANALYSIS

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 OWASP MASVS: MSTG-STORAGE-3	com/serwylo/lexica/GameActivity.java mehdi/sakout/fancybuttons/Utils.java com/serwylo/lexica/game/Game.java com/serwylo/lexica/Util.java mehdi/sakout/fancybuttons/FancyButton.j ava
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/serwylo/lexica/game/CharProbGener ator.java com/serwylo/lexica/view/LexicaLogo.java

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.
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform 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.

# **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sjp.pl	ok	IP: 145.239.10.41 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: Google Map

#### 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.