Mobile App Vulnerability Scan Report

Table of Contents

Scan Information Summary

Target Scanned	TestApp.apk ✓ TestApp.ipa ✗
App Score	CVSS: 7.1 Security Score: 55/100 Trackers Detection: 3/407
Start time	2021-06-24 14:49:44 UTC+03
End time	2021-06-24 14:59:44 UTC+03
Scan Duration	3 Hours, 27 Minutes
Scan Status	FINISHED

Information Gathered

Activities: 20
Exported Activities: 1

Services: 15
Exported Services: 2

Receivers: 8
Exported Receivers: 5

Providers: 1
Exported Providers: 0

Decompiled Code

- ✓ AndroidManifest.xml
- ✓ Java Code
- ✓ Smali Code

Tests Performed

Total: 10

- ✓ Improper Platform Usage
- ✓ Insecure Data Storage
- ✓ Insecure Communication
- ✓ Insecure Authentication
- ✓ Insufficient Cryptography
- ✓ Insecure Authorization
- ✓ Client Code Inspection
- ✓ Code Tampering
- ✓ Reverse Engineering
- ✓ Extraneous Functionality

App Permissions Discovered

Total: 3
Status: Dangerous

- Android.permission.CAMERA View More ⬆

Info:

Display system-level alerts

Recommendation:
Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

- Android.permission.READ_PHONE_STATE View More ⬇
- Android.permission.SYSTEM_ALERT_WINDOW View More ⬆

Info:

Display system-level alerts

Recommendation:
Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

Browsable Activities

Activity	*Intent*
net.openid.appauth.RedirectUriReceiverActivity *modules.payments.stripe.RedirectUriReceiver*	Schemes: package.test.app://, **.payments.stripe.aabb-aaa-bbb-ccc-0x66://

Network Security

Nothing Found

Manifest Analysis

No	Severity	Issue	Details
1	High	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	View More ⬇
		Description: 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"	
2	Medium	Application Data can be Backed up [android:allowBackup=true]	View More ⬇
		Description: This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off the device	
3	High	**Activity** (package.com.app.LauncherActivity) is not Protected. [android:exported=true]	View More ⬇

Source Code Analysis

No	Severity	Issue	Standard	Files
1	Info	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	OWASP MASVS: MSTG-STORAGE-3	FileSystemModule.java Login.java FuncionCall.java ViewsC.java MainController.java MediaController.java Picker.java
2	High	App can read/write to External Storage	OWASP Top 10: M2: Insecure Data Storage	CreateAsset.java CreateAlbum.java StoreCred.java
3	Secure	This App is using a SSL certificate pinning to prevent MiTM attack on secure channels.	CVSS V2: 0 (info)	com/amplitude/api/PinnedAmplitudeClient.java

URL Discovered

Total URL discovered: 5

URL	File
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java

API discovered

API	File
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java
http://example.com	Net/openid/appauth/class.java

Hardcoded Secrets

- "com_auth_master" : AIzaSyDqB6JepnlPJJJX******
- "google_api_key" : " AIzaSyDqB6JepnlPJJJX******"
- "google_crash_reporting_api_key" : " AIzaSyDqB6JepnlPJJJX******"
- "Admin" : Pas%$w****

Contact Us

Ionut Staniu

ionut.staniu@blackbullet.ro

+40 767890619

www.blackbullet.ro

21 Elena Caragiani Street, Bucharest, Romania