



ANDROID STATIC ANALYSIS REPORT

app_icon

 PrivacyCheck (1.0)






File Name: app-debug.apk
Package Name: hu.hegedusblanka.privacycheck
Scan Date: March 19, 2026, 4:57 a.m.

App Security Score: **35/100 (HIGH RISK)**

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	4	1	1	1

FILE INFORMATION

File Name: app-debug.apk

Size: 5.82MB

MD5: ebaa6e869823a1f95c24e75b06ba5529

SHA1: 341446dedadd68015bd145b0ff391b64438234d7

SHA256: c5e47ad8f2002149903029deaeb14d5cee2691eddef9ddf459740502b54e49e6

APP INFORMATION

App Name: PrivacyCheck

Package Name: hu.hegedusblanka.privacycheck

Main Activity: hu.hegedusblanka.privacycheck.MainActivity

Target SDK: 34

Min SDK: 24

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 9

Services: 0

Receivers: 1

Providers: 2

Exported Activities: 0

Exported Services: 0

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: CN=Android Debug, O=Android, C=US

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2026-02-28 12:13:43+00:00

Valid To: 2056-02-21 12:13:43+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1

Hash Algorithm: sha256

md5: a09ce3336013b4d785d7c3de0c40592f

sha1: d103fd58059d8c9ef7ebd5beaa29ad3eb552bf4f

sha256: 01dd3d6683f8593b7f869141639905b6dde14196798b03ccd73e34d6bf11d49

sha512: b2db44828aaa521c46df9c239a06f61c73bbd0eaaaf11a0ac28539ecaf6e895233997fc310a1ba591ddfe6960b4ac4e13f72ecc81e6f9b9bee2c614a82f36991c

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: bfab84b696aef4923bd16ca88621410527e426e235bd97a3298b74cedf6b4168

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
hu.hegedusblanka.privacycheck.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Compiler	r8
classes5.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)
classes4.dex	FINDINGS	DETAILS
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)

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

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

Q MANIFEST ANALYSIS

HIGH: 3 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App[android:usesCleartextTraffic=true]	high	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". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

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

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/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java hu/hegedusblanka/privacycheck/PasswordCheckActivity.java
2	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	com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	hu/hegedusblanka/privacycheck/AdviceSettingsActivity.java hu/hegedusblanka/privacycheck/PasswordCheckActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/github/mikephil/charting/charts/Chart.java hu/hegedusblanka/privacycheck/PrivacyReportActivity.java
00096	Connect to a URL and set request method	command network	hu/hegedusblanka/privacycheck/NetworkSecurityActivity.java
00089	Connect to a URL and receive input stream from the server	command network	hu/hegedusblanka/privacycheck/NetworkSecurityActivity.java
00109	Connect to a URL and get the response code	network command	hu/hegedusblanka/privacycheck/NetworkSecurityActivity.java
00121	Create a directory	file command	hu/hegedusblanka/privacycheck/PrivacyReportActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	hu/hegedusblanka/privacycheck/PrivacyReportActivity.java

🔍 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO
Other Common Permissions	0/44	

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
example.com	ok	IP: 104.18.27.120 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
9aaf5f34c4c84da429ef7f8f6217a1817876f2618cfcf539aba3d7d5a0c703e0

SCAN LOGS

Timestamp	Event	Error
2026-03-19 04:57:38	Generating Hashes	OK
2026-03-19 04:57:38	Extracting APK	OK

2026-03-19 04:57:38	Unzipping	OK
2026-03-19 04:57:38	Parsing APK with androguard	OK
2026-03-19 04:57:39	Extracting APK features using aapt/aapt2	OK
2026-03-19 04:57:39	Getting Hardcoded Certificates/Keystores	OK
2026-03-19 04:57:43	Parsing AndroidManifest.xml	OK
2026-03-19 04:57:43	Extracting Manifest Data	OK
2026-03-19 04:57:43	Manifest Analysis Started	OK
2026-03-19 04:57:43	Performing Static Analysis on: PrivacyCheck (hu.hegedusblanka.privacycheck)	OK
2026-03-19 04:57:43	Fetching Details from Play Store: hu.hegedusblanka.privacycheck	OK
2026-03-19 04:57:44	Checking for Malware Permissions	OK
2026-03-19 04:57:44	Fetching icon path	OK

2026-03-19 04:57:44	Library Binary Analysis Started	OK
2026-03-19 04:57:44	Reading Code Signing Certificate	OK
2026-03-19 04:57:44	Running APKiD 3.0.0	OK
2026-03-19 04:57:46	Detecting Trackers	OK
2026-03-19 04:57:47	Decompiling APK to Java with JADX	OK
2026-03-19 04:57:58	Converting DEX to Smali	OK
2026-03-19 04:57:58	Code Analysis Started on - java_source	OK
2026-03-19 04:57:58	Android SBOM Analysis Completed	OK
2026-03-19 04:58:02	Android SAST Completed	OK
2026-03-19 04:58:02	Android API Analysis Started	OK
2026-03-19 04:58:05	Android API Analysis Completed	OK

2026-03-19 04:58:05	Android Permission Mapping Started	OK
2026-03-19 04:58:08	Android Permission Mapping Completed	OK
2026-03-19 04:58:08	Android Behaviour Analysis Started	OK
2026-03-19 04:58:15	Android Behaviour Analysis Completed	OK
2026-03-19 04:58:15	Extracting Emails and URLs from Source Code	OK
2026-03-19 04:58:15	Email and URL Extraction Completed	OK
2026-03-19 04:58:15	Extracting String data from APK	OK
2026-03-19 04:58:15	Extracting String data from Code	OK
2026-03-19 04:58:15	Extracting String values and entropies from Code	OK
2026-03-19 04:58:16	Performing Malware check on extracted domains	OK
2026-03-19 04:58:17	Saving to Database	OK

Report Generated by - MobSF v4.4.5

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.

© 2026 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).