MobSF

ANDROID STATIC ANALYSIS REPORT

app_icon

GPSMapApp

File Name:	GPSMapApp1-master.zip
Package Name:	com.example.gpsmapapp
Scan Date:	Oct. 28, 2025, 9:56 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	2	1	1	1

FILE INFORMATION

File Name: GPSMapApp1-master.zip
Size: 0.11MB
MD5: a907c86c63ab29d3ae92f95e7068477f
SHA1: 8a5fed817b5432ebc147fc94db8200ad091dd5e4
SHA256: 8523e1dc8721e3cd94bbf6b6e0855678e1a674d5082fa3142b8b1a12b65b80a1

APP INFORMATION

App Name: GPSMapApp
Package Name: com.example.gpsmapapp
Main Activity: .MainActivity
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

APPLICATION PERMISSIONS

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **1** | INFO: **0** | SUPPRESSED: **0**

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 (.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.

CODE ANALYSIS

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

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/example/gpsmapapp/GPS.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	com/example/gpsmapapp/GPS.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/example/gpsmapapp/DescargarImagen.java
00030	Connect to the remote server through the given URL	network	com/example/gpsmapapp/DescargarImagen.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET
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

DOMAIN	STATUS	GEOLOCATION
maps.googleapis.com	ok	**IP:** 64.233.186.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
upload.wikimedia.org	ok	**IP:** 195.200.68.240 **Country:** Finland **Region:** Etela-Karjala **City:** Lappeenranta **Latitude:** 61.058708 **Longitude:** 28.188709 **View:** Google Map

SCAN LOGS

Timestamp	Event	Error
2025-10-28 21:56:46	Generating Hashes	OK
2025-10-28 21:56:46	Extracting ZIP	OK
2025-10-28 21:56:46	Unzipping	OK

2025-10-28 21:56:46	Detecting source code type	OK
2025-10-28 21:56:46	Source code type - studio	OK
2025-10-28 21:56:46	Getting Hardcoded Certificates/Keystores	OK
2025-10-28 21:56:46	Parsing AndroidManifest.xml	OK
2025-10-28 21:56:46	Extracting Manifest Data	OK
2025-10-28 21:56:46	Manifest Analysis Started	OK
2025-10-28 21:56:46	Performing Static Analysis on: GPSMapApp (com.example.gpsmapapp)	OK
2025-10-28 21:56:47	Fetching Details from Play Store: com.example.gpsmapapp	OK
2025-10-28 21:56:47	Checking for Malware Permissions	OK
2025-10-28 21:56:47	Guessing icon path	OK
2025-10-28 21:56:47	Code Analysis Started on - java	OK

2025-10-28 21:56:47	Android SBOM Analysis Completed	OK
2025-10-28 21:56:48	Android SAST Completed	OK
2025-10-28 21:56:48	Android API Analysis Started	OK
2025-10-28 21:56:48	Android API Analysis Completed	OK
2025-10-28 21:56:48	Android Permission Mapping Started	OK
2025-10-28 21:56:48	Android Permission Mapping Completed	OK
2025-10-28 21:56:48	Android Behaviour Analysis Started	OK
2025-10-28 21:56:49	Android Behaviour Analysis Completed	OK
2025-10-28 21:56:49	Extracting Emails and URLs from Source Code	OK
2025-10-28 21:56:49	Email and URL Extraction Completed	OK
2025-10-28 21:56:49	Extracting String data from Code	OK

2025-10-28 21:56:49	Extracting String values and entropies from Code	OK
2025-10-28 21:56:49	Performing Malware check on extracted domains	OK
2025-10-28 21:56:51	Detecting Trackers from Domains	OK
2025-10-28 21:56:51	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.