ANDROID STATIC ANALYSIS REPORT

app_icon

MiAplicacionEvaluacionOscar (1.0)

File Name:	app-debug.apk
Package Name:	com.example.miaplicacionevaluacionoscar
Scan Date:	Oct. 25, 2025, 6:12 p.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	3	0	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 6.69MB
MD5: 93b9984aa66ea188fb31045706d1c470
SHA1: 7b1862e6b2cc47f73ca6c4aaa4d68d8ec4533fd0
SHA256: f4115d5dff59bdfcadbd6b9f77a706ab7cf971d1c19a91572ef5932ad3db81d5

APP INFORMATION

App Name: MiAplicacionEvaluacionOscar
Package Name: com.example.miaplicacionevaluacionoscar
Main Activity: com.example.miaplicacionevaluacionoscar.Inicio
Target SDK: 35
Min SDK: 24
Max SDK:
Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 1
Providers: 1
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: 2025-09-07 01:32:31+00:00
Valid To: 2055-08-31 01:32:31+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 446f491406346d3677dac3b484841aa8
sha1: 4f044030c4045d874efa13748ee18c3e1c2c4d78
sha256: 767a3bfaae8e9f3746388ce27fca922fdb78bb5dd13401464744435a0e2db91f
sha512: 84a52d0244be84950d007218ea78e5e579c57e323f53a354963f3b443e8016bfd4b540ddb210228c8af9f235490d724f045a6e5faabc8b86bec5439349642efb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 09ce7dfb8bf0b3c47d2dacdd71206febc329bf4ab130bd8171493ec8c268d25f
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_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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.example.miaplicacionevaluacionoscar.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
<tr><td>classes4.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
<tr><td>classes3.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
</table>

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 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	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.
3	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
4	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: **1** | INFO: **0** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/miaplicacionevaluacionoscar/MainActivity.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/miaplicacionevaluacionoscar/Inicio.java
00030	Connect to the remote server through the given URL	network	com/example/miaplicacionevaluacionoscar/Inicio.java
00109	Connect to a URL and get the response code	network command	com/example/miaplicacionevaluacionoscar/Inicio.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE
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
tse4.mm.bing.net	ok	**IP:** 150.171.27.10 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyDuelOp_57iRkE2cDrUTcoNgjg2BcbrOKQ"

SCAN LOGS

Timestamp	Event	Error

2025-10-25 18:12:05	Generating Hashes	OK
2025-10-25 18:12:05	Extracting APK	OK
2025-10-25 18:12:05	Unzipping	OK
2025-10-25 18:12:05	Parsing APK with androguard	OK
2025-10-25 18:12:06	Extracting APK features using aapt/aapt2	OK
2025-10-25 18:12:06	Getting Hardcoded Certificates/Keystores	OK
2025-10-25 18:12:09	Parsing AndroidManifest.xml	OK
2025-10-25 18:12:09	Extracting Manifest Data	OK
2025-10-25 18:12:09	Manifest Analysis Started	OK
2025-10-25 18:12:09	Performing Static Analysis on: MiAplicacionEvaluacionOscar (com.example.miaplicacionevaluacionoscar)	OK
2025-10-25 18:12:10	Fetching Details from Play Store: com.example.miaplicacionevaluacionoscar	OK

2025-10-25 18:12:10	Checking for Malware Permissions	OK
2025-10-25 18:12:10	Fetching icon path	OK
2025-10-25 18:12:10	Library Binary Analysis Started	OK
2025-10-25 18:12:10	Reading Code Signing Certificate	OK
2025-10-25 18:12:10	Running APKiD 3.0.0	OK
2025-10-25 18:12:14	Detecting Trackers	OK
2025-10-25 18:12:17	Decompiling APK to Java with JADX	OK
2025-10-25 18:12:49	Converting DEX to Smali	OK
2025-10-25 18:12:49	Code Analysis Started on - java_source	OK
2025-10-25 18:12:50	Android SBOM Analysis Completed	OK
2025-10-25 18:12:59	Android SAST Completed	OK

2025-10-25 18:12:59	Android API Analysis Started	OK
2025-10-25 18:13:36	Android API Analysis Completed	OK
2025-10-25 18:13:36	Android Permission Mapping Started	OK
2025-10-25 18:14:13	Android Permission Mapping Completed	OK
2025-10-25 18:14:13	Android Behaviour Analysis Started	OK
2025-10-25 18:14:19	Android Behaviour Analysis Completed	OK
2025-10-25 18:14:19	Extracting Emails and URLs from Source Code	OK
2025-10-25 18:14:20	Email and URL Extraction Completed	OK
2025-10-25 18:14:20	Extracting String data from APK	OK
2025-10-25 18:14:20	Extracting String data from Code	OK
2025-10-25 18:14:20	Extracting String values and entropies from Code	OK

2025-10-25 18:14:22	Performing Malware check on extracted domains	OK
2025-10-25 18:14:24	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.