MOBSF

ANDROID STATIC ANALYSIS REPORT

AndroGoat - Insecure App (Kotlin) (1.0)

File Name:	AndroGoat.apk
Package Name:	owasp.sat.agoat
Scan Date:	Aug. 17, 2024, 9:08 p.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	13	2	3	1

FILE INFORMATION

File Name: AndroGoat.apk
Size: 2.64MB
MD5: 3d351e8fc20c340cf03ff52b0ef125ae
SHA1: ea96f4adc27083696a449b1c6e5cd612a2cf0f5c
SHA256: a47a8b0d0b8466a25ccc67d3d2cbb5d69ef2b0de4d4f278b6bee357c7ba5f63b

APP INFORMATION

App Name: AndroGoat - Insecure App (Kotlin)
Package Name: owasp.sat.agoat
Main Activity: owasp.sat.agoat.SplashActivity
Target SDK: 26
Min SDK: 18
Max SDK:
Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 25
Services: 1
Receivers: 1
Providers: 0
Exported Activities: 1
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
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: 2016-09-22 18:39:24+00:00
Valid To: 2046-09-15 18:39:24+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: af5ff4235e641bae76eb04d55c2eb670
sha1: afbffdbd437c68395723c82190a5ea8a2904c2af
sha256: f1d42f18d738ff2908cc2274a688b6642df0379a0ea2623164e969a9086e0e20
sha512: 4eb8611881cbea7804116388aa5ec677d2054a189abf12ca3badbc2d204770af0ebcfb057f1f96e53e7edb9103c47c21695330ea2b8e02b795429eb8c1a955a7
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: c15e372e3066fe2dd58eef3d86a2c7b6e24647bb6522915ce2fba6c57280b33b
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check possible VM check FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.3-4.3.1, [minSdk=18]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
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.
5	Activity (owasp.sat.agoat.AccessControl1ViewActivity) 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.
6	Broadcast Receiver (owasp.sat.agoat.ShowDataReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (owasp.sat.agoat.DownloadInvoiceService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 5 | INFO: 2 | SECURE: 2 | 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	org/jetbrains/anko/Logging.java owasp/sat/agoat/DownloadInvoiceService.java owasp/sat/agoat/InsecureLoggingActivity.java owasp/sat/agoat/InsecureStorageSDCardActivity.java owasp/sat/agoat/InsecureStorageSQLiteActivity.java owasp/sat/agoat/InsecureStorageSharedPrefs1Activity.java owasp/sat/agoat/RootDetectionActivity.java owasp/sat/agoat/SQLinjectionActivity.java owasp/sat/agoat/TrafficActivity$doPinning$1.java owasp/sat/agoat/TrafficActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	owasp/sat/agoat/AccessControlIssue1Activity.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	owasp/sat/agoat/InsecureStorageSQLiteActivity.java owasp/sat/agoat/SQLinjectionActivity.java
4	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	owasp/sat/agoat/RootDetectionActivity.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	owasp/sat/agoat/RootDetectionActivity.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	owasp/sat/agoat/InsecureStorageSDCardActivity.java owasp/sat/agoat/InsecureStorageTempActivity.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	owasp/sat/agoat/TrafficActivity$doPinning$1.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	owasp/sat/agoat/ClipboardActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	owasp/sat/agoat/BuildConfig.java
10	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	owasp/sat/agoat/InsecureStorage SDCardActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/24	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	0/45	

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
androgoat-42597.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
demo.testfire.net	ok	**IP:** 65.61.137.117 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 20.201.28.151 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
owasp.org	ok	**IP:** 104.22.27.77 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://androgoat-42597.firebaseio.com/.json	high Firebase DB is exposed publicly.

EMAILS

EMAIL	FILE
satishkumarpatnayak@live.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"firebaseurl" : "https://androgoat-42597.firebaseio.com"
sha256/Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

SCAN LOGS

Timestamp	Event	Error
2024-08-17 21:08:25	Generating Hashes	OK
2024-08-17 21:08:25	Extracting APK	OK

2024-08-17 21:08:25	Unzipping	OK
2024-08-17 21:08:25	Getting Hardcoded Certificates/Keystores	OK
2024-08-17 21:08:26	Parsing AndroidManifest.xml	OK
2024-08-17 21:08:26	Parsing APK with androguard	OK
2024-08-17 21:08:26	Extracting Manifest Data	OK
2024-08-17 21:08:26	Performing Static Analysis on: AndroGoat - Insecure App (Kotlin) (owasp.sat.agoat)	OK
2024-08-17 21:08:26	Fetching Details from Play Store: owasp.sat.agoat	OK
2024-08-17 21:08:27	Manifest Analysis Started	OK
2024-08-17 21:08:27	Reading Network Security config from network_security_config.xml	OK
2024-08-17 21:08:27	Parsing Network Security config	OK
2024-08-17 21:08:27	Checking for Malware Permissions	OK

2024-08-17 21:08:27	Fetching icon path	OK
2024-08-17 21:08:27	Library Binary Analysis Started	OK
2024-08-17 21:08:27	Reading Code Signing Certificate	OK
2024-08-17 21:08:28	Running APKiD 2.1.5	OK
2024-08-17 21:08:30	Updating Trackers Database....	OK
2024-08-17 21:08:30	Detecting Trackers	OK
2024-08-17 21:08:30	Decompiling APK to Java with jadx	OK
2024-08-17 21:08:37	Converting DEX to Smali	OK
2024-08-17 21:08:37	Code Analysis Started on - java_source	OK
2024-08-17 21:08:38	Android SAST Completed	OK
2024-08-17 21:08:38	Android API Analysis Started	OK

2024-08-17 21:08:39	Android Permission Mapping Started	OK
2024-08-17 21:08:40	Android Permission Mapping Completed	OK
2024-08-17 21:08:40	Finished Code Analysis, Email and URL Extraction	OK
2024-08-17 21:08:40	Extracting String data from APK	OK
2024-08-17 21:08:40	Extracting String data from Code	OK
2024-08-17 21:08:40	Extracting String values and entropies from Code	OK
2024-08-17 21:08:41	Performing Malware check on extracted domains	OK
2024-08-17 21:08:44	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.