MOBSF

ANDROID STATIC ANALYSIS REPORT

BitbarSampleApp (1.0)

File Name:	bitbar-sample-app.apk
Package Name:	com.bitbar.testdroid
Scan Date:	April 21, 2025, 1:16 p.m.
App Security Score:	32/100 (HIGH RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	4	0	1	1

FILE INFORMATION

File Name: bitbar-sample-app.apk
Size: 0.11MB
MD5: 00cc5435151aa38a091781922c0390a4
SHA1: 40e991508120d6f5d653a6755d8209df4d20289d
SHA256: 3b4d462b8cce5f377a33417e1be7680717065f280a9f6e2f6af49325dbe89411

APP INFORMATION

App Name: BitbarSampleApp
Package Name: com.bitbar.testdroid
Main Activity: com.bitbar.testdroid.BitbarSampleApplicationActivity
Target SDK: 33
Min SDK: 4
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 2
Exported Services: 0
Exported Receivers: 0
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: 2022-07-05 09:35:34+00:00
Valid To: 2052-06-27 09:35:34+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: f5e77c7ea1c2102188be9eae9a3b8573
sha1: a7ce1335a1bbb135d34c208b51945cc93104c7ed
sha256: 93424fddcac08ed772ccaf7a20cd2cda4fc83f101656536154ef92846c2f3ffc
sha512: ec768feee2bcc63bdd65c642767b717a8cf0b855772497c302a4e0109c44f544a40338e9164be8053011f575a7e0a6196e08e9cca78a1589510a0820e4b4bd93
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ff557fc6f6139b576a27f7f3cb4efe09a12090029a11ab150eaddf7c79d6ec67
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler DETAILS: r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 1 | 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 vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 1.6, [minSdk=4]	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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	Activity (com.bitbar.testdroid.CorrectAnswerActivity) is not Protected. [android:exported=true]	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.
5	Activity (com.bitbar.testdroid.WrongAnswerActivity) is not Protected. [android:exported=true]	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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/bitbar/testdroid/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/25	android.permission.WRITE_EXTERNAL_STORAGE, 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.

SCAN LOGS

Timestamp	Event	Error
2025-04-21 13:16:43	Generating Hashes	OK
2025-04-21 13:16:43	Extracting APK	OK
2025-04-21 13:16:43	Unzipping	OK
2025-04-21 13:16:43	Parsing APK with androguard	OK
2025-04-21 13:16:43	Extracting APK features using aapt/aapt2	OK

2025-04-21 13:16:43	Getting Hardcoded Certificates/Keystores	OK
2025-04-21 13:16:44	Parsing AndroidManifest.xml	OK
2025-04-21 13:16:44	Extracting Manifest Data	OK
2025-04-21 13:16:44	Manifest Analysis Started	OK
2025-04-21 13:16:44	Performing Static Analysis on: BitbarSampleApp (com.bitbar.testdroid)	OK
2025-04-21 13:16:44	Fetching Details from Play Store: com.bitbar.testdroid	OK
2025-04-21 13:16:45	Checking for Malware Permissions	OK
2025-04-21 13:16:45	Fetching icon path	OK
2025-04-21 13:16:45	Library Binary Analysis Started	OK
2025-04-21 13:16:45	Reading Code Signing Certificate	OK

2025-04-21 13:16:45	Running APKiD 2.1.5	OK
2025-04-21 13:16:47	Detecting Trackers	OK
2025-04-21 13:16:47	Decompiling APK to Java with JADX	OK
2025-04-21 13:16:49	Converting DEX to Smali	OK
2025-04-21 13:16:49	Code Analysis Started on - java_source	OK
2025-04-21 13:16:49	Android SBOM Analysis Completed	OK
2025-04-21 13:16:50	Android SAST Completed	OK
2025-04-21 13:16:50	Android API Analysis Started	OK
2025-04-21 13:16:50	Android API Analysis Completed	OK
2025-04-21 13:16:50	Android Permission Mapping Started	OK

2025-04-21 13:16:51	Android Permission Mapping Completed	OK
2025-04-21 13:16:51	Android Behaviour Analysis Started	OK
2025-04-21 13:16:51	Android Behaviour Analysis Completed	OK
2025-04-21 13:16:51	Extracting Emails and URLs from Source Code	OK
2025-04-21 13:16:51	Email and URL Extraction Completed	OK
2025-04-21 13:16:51	Extracting String data from APK	OK
2025-04-21 13:16:51	Extracting String data from Code	OK
2025-04-21 13:16:51	Extracting String values and entropies from Code	OK
2025-04-21 13:16:51	Performing Malware check on extracted domains	OK
2025-04-21 13:16:51	Saving to Database	OK

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.