



## 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:	C		

### **FINDINGS SEVERITY**

<del>派</del> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	<b>◎</b> HOTSPOT
5	4	0	1	1

### FILE INFORMATION

File Name: bitbar-sample-app.apk

**Size:** 0.11MB

MD5: 00cc5435151aa38a091781922c0390a4

**SHA1**: 40e991508120d6f5d653a6755d8209df4d20289d

SHA256: 3b4d462b8cce5f377a33417e1be7680717065f280a9f6e2f6af49325dbe89411

# **i** 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

### **B** 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: ec768 feee 2 bcc63 bdd65 c642767 b717 a8cf0 b855772497 c302 a4e0109 c44 f544 a40338 e9164 be8053011 f575 a7e0 a6196 e08 e9cca78 a1589510 a0820 e4b4 bd9320 e4b4 bd9220 e4b4 bd9220 e4b4 bd9220 e4b4 bd92

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.

## **命 APKID ANALYSIS**

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

# **△** NETWORK SECURITY

NO SCOPE SEVERITY E	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.

# **Q** 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
----	------------	-------------	---------	-------------

### **SECOND SECOND PERMISSIONS**

ТҮРЕ	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	ОК
2025-04-21 13:16:43	Extracting APK	ОК
2025-04-21 13:16:43	Unzipping	ОК
2025-04-21 13:16:43	Parsing APK with androguard	ОК
2025-04-21 13:16:43	Extracting APK features using aapt/aapt2	ОК

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

2025-04-21 13:16:45	Running APKiD 2.1.5	ОК
2025-04-21 13:16:47	Detecting Trackers	OK
2025-04-21 13:16:47	Decompiling APK to Java with JADX	ОК
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	ОК
2025-04-21 13:16:50	Android API Analysis Started	ОК
2025-04-21 13:16:50	Android API Analysis Completed	ОК
2025-04-21 13:16:50	Android Permission Mapping Started	OK

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

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.

