MOBSF

ANDROID STATIC ANALYSIS REPORT

Dummy (1.0)

File Name:	Dummy-1.0.apk
Package Name:	com.techsquare.dummy
Scan Date:	Oct. 17, 2025, 12:04 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	0	1	0

FILE INFORMATION

File Name: Dummy-1.0.apk
Size: 1.62MB
MD5: 3882d336205f7a6a9a725421e70eeccb
SHA1: c2be798093c26046d0531cf34c1501f362f317d1
SHA256: 3f9a23c0a22bc8255d4f499a27ce99d1689150d6e604fb3fc805bc657512a97f

APP INFORMATION

App Name: Dummy
Package Name: com.techsquare.dummy
Main Activity: com.techsquare.dummy.SplashActivity
Target SDK: 25
Min SDK: 15
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
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: C=91, ST=Haryana, L=Gurgaon, O=Techsquare, OU=IT, CN=Uma Shanker
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-12-01 10:29:42+00:00
Valid To: 2041-11-25 10:29:42+00:00
Issuer: C=91, ST=Haryana, L=Gurgaon, O=Techsquare, OU=IT, CN=Uma Shanker
Serial Number: 0x465c324d
Hash Algorithm: sha256
md5: 4315a1990243bd1caf417e5c96aff8f0
sha1: 580c99700b0b179e55192ebefa9e88a8aeb361b3
sha256: 11bffaa22b4ad865f556fd950b8846c8e4a3af2db31a45dca39be60408d80f54
sha512: 37db495d5c864d88b5147ae30a537da0c9d4af8d5c5e9c6afce8becd42c6453a566011237b8115659ba73a9de282b6a073774b3c0f91808bb6912f9bf24e76b8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 36d9e5bbc5a59f3d84c8d7331ecd52034776f94669b911e309612ba1e329b49f
Found 1 unique certificates

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | 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.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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	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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/25	
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
2025-10-17 12:04:17	Generating Hashes	OK
2025-10-17 12:04:17	Extracting APK	OK
2025-10-17 12:04:17	Unzipping	OK
2025-10-17 12:04:17	Parsing APK with androguard	OK
2025-10-17 12:04:17	Extracting APK features using aapt/aapt2	OK

2025-10-17 12:04:17	Getting Hardcoded Certificates/Keystores	OK
2025-10-17 12:04:21	Parsing AndroidManifest.xml	OK
2025-10-17 12:04:21	Extracting Manifest Data	OK
2025-10-17 12:04:21	Manifest Analysis Started	OK
2025-10-17 12:04:21	Performing Static Analysis on: Dummy (com.techsquare.dummy)	OK
2025-10-17 12:04:22	Fetching Details from Play Store: com.techsquare.dummy	OK
2025-10-17 12:04:22	Checking for Malware Permissions	OK
2025-10-17 12:04:22	Fetching icon path	OK
2025-10-17 12:04:22	Library Binary Analysis Started	OK
2025-10-17 12:04:22	Reading Code Signing Certificate	OK
2025-10-17 12:04:23	Running APKiD 3.0.0	OK

2025-10-17 12:04:26	Detecting Trackers	OK
2025-10-17 12:04:27	Decompiling APK to Java with JADX	OK
2025-10-17 12:04:34	Converting DEX to Smali	OK
2025-10-17 12:04:34	Code Analysis Started on - java_source	OK
2025-10-17 12:04:34	Android SBOM Analysis Completed	OK
2025-10-17 12:04:34	Android SAST Completed	OK
2025-10-17 12:04:34	Android API Analysis Started	OK
2025-10-17 12:04:35	Android API Analysis Completed	OK
2025-10-17 12:04:35	Android Behaviour Analysis Started	OK
2025-10-17 12:04:36	Android Behaviour Analysis Completed	OK
2025-10-17 12:04:36	Extracting Emails and URLs from Source Code	OK

2025-10-17 12:04:36	Email and URL Extraction Completed	OK
2025-10-17 12:04:36	Extracting String data from APK	OK
2025-10-17 12:04:36	Extracting String data from Code	OK
2025-10-17 12:04:36	Extracting String values and entropies from Code	OK
2025-10-17 12:04:36	Performing Malware check on extracted domains	OK
2025-10-17 12:04:36	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.