MOBSF

ANDROID STATIC ANALYSIS REPORT

test_app (1.0.0)

File Name:	newapp.apk
Package Name:	com.example.test_app
Scan Date:	Nov. 17, 2024, 2:02 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	2	1	0

FILE INFORMATION

File Name: newapp.apk
Size: 18.81MB
MD5: 97ff4af35b59dbdf8dc21fee9dbeac3a
SHA1: 4db5f86cdff032e41e44e8aecce623e62823ce94
SHA256: e039c442a968b41cab30dd1c88221bf83548ba5825f68b9f5474daddff7511d1

APP INFORMATION

App Name: test_app
Package Name: com.example.test_app
Main Activity: com.example.test_app.MainActivity
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 1
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: True
v4 signature: False
X.509 Subject: C=., ST=., O=., OU=., CN=.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-11-17 14:01:55+00:00
Valid To: 2052-04-04 14:01:55+00:00
Issuer: C=., ST=., O=., OU=., CN=.
Serial Number: 0x3b7b582b65737938
Hash Algorithm: sha384
md5: 200711bc9439d285890c8a23765b8f93
sha1: f8e70318e1d79cb4232439bb0884eafbb2a227ba
sha256: 70d6dd6f8369b785de03e6a624aec835e527b7838f7711dadf65d25fbf5d4c46
sha512: e04e64a4fa0e696e9316962cd022df37fcedf6533ce0c0c94921044828d691896fd54ae7b034e988611ff4814ebd1ba596099fdf72ca475dcf35d6d7de178efb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c35ff074e8eda71b30e565ad233b854e7f83c86126fb7aa8da115d726d5ff302
Found 1 unique certificates

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dexlib 2.x</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 upatched Android version Android 4.4-4.4.4, [minSdk=19]	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] 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.

CODE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 2 | SECURE: 0 | 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	h/c.java h/f.java j/a.java l/b.java
2	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	io/flutter/plugin/editing/h.java io/flutter/plugin/platform/j.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	l0/a.java l0/b.java m0/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/24	
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
github.com	ok	IP: 20.200.245.247 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.flutter.dev	ok	IP: 199.36.158.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
flutter.dev	ok	IP: 199.36.158.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 142.250.206.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
dartbug.com	ok	IP: 216.239.38.21 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 104.18.22.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
_uri@0150898.directory _imagefilter@15065589.composed _assertionerror@0150898._create _growablelist@0150898._ofgrowabl ngstreamsubscription@4048458.zoned _imagefilter@15065589.fromcolorf _future@4048458.immediate _growablelist@0150898._literal2 _growablelist@0150898._literal5 _file@14069316.fromrawpat _imagefilter@15065589.blur _invocationmirror@0150898._withtype _growablelist@0150898._literal3 _colorfilter@15065589.lineartosr _directory@14069316.fromrawpat _list@0150898._ofother _list@0150898.of _timer@1026248.periodic _list@0150898._ofarray _uri@0150898.file _list@0150898._ofgrowabl _double@0150898.fromintege	apktool_out/lib/armeabi-v7a/libapp.so

EMAIL	FILE
_growablelist@0150898._literal4 _colorfilter@15065589.srgbtoline _growablelist@0150898._ofefficie	
_hashcollisionnode@38137193.fromcollis _list@0150898._ofefficie _typeerror@0150898._create _future@4048458.immediatee _growablelist@0150898.generate _bytebuffer@7027147._new _compressednode@38137193.single _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._ofarray _growablelist@0150898.withcapaci _growablelist@0150898._literal1 _growablelist@0150898._literal _list@0150898.empty _growablelist@0150898.of _uri@0150898.notsimple _link@14069316.fromrawpat	
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so
appro@openssl.org	apktool_out/lib/x86_64/libflutter.so
_uri@0150898.directory _imagefilter@15065589.composed _assertionerror@0150898._create _growablelist@0150898._ofgrowabl ngstreamsubscription@4048458.zoned _imagefilter@15065589.fromcolorf _future@4048458.immediate _growablelist@0150898._literal2 _growablelist@0150898._literal5 _file@14069316.fromrawpat _imagefilter@15065589.blur _invocationmirror@0150898._withtype _growablelist@0150898._literal3 _colorfilter@15065589.lineartosr _directory@14069316.fromrawpat _list@0150898._ofother	

EMAIL	FILE
_list@0150898.of _timer@1026248.periodic _list@0150898._ofarray _uri@0150898.file _list@0150898._ofgrowabl _double@0150898.fromintege _growablelist@0150898._literal4 _colorfilter@15065589.srgbtoline _growablelist@0150898._ofefficie _hashcollisionnode@38137193.fromcollis _list@0150898._ofefficie _typeerror@0150898._create _future@4048458.immediatee _growablelist@0150898.generate _bytebuffer@7027147._new _compressednode@38137193.single _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._ofarray _growablelist@0150898.withcapaci _growablelist@0150898._literal1 _growablelist@0150898._literal _list@0150898.empty _growablelist@0150898.of _uri@0150898.notsimple _link@14069316.fromrawpat	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/x86_64/libflutter.so

SCAN LOGS

Timestamp	Event	Error

2024-11-17 14:02:02	Generating Hashes	OK
2024-11-17 14:02:02	Extracting APK	OK
2024-11-17 14:02:02	Unzipping	OK
2024-11-17 14:02:02	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 14:02:03	Parsing AndroidManifest.xml	OK
2024-11-17 14:02:03	Parsing APK with androguard	OK
2024-11-17 14:02:03	Extracting Manifest Data	OK
2024-11-17 14:02:03	Performing Static Analysis on: test_app (com.example.test_app)	OK
2024-11-17 14:02:03	Fetching Details from Play Store: com.example.test_app	OK
2024-11-17 14:02:03	Manifest Analysis Started	OK
2024-11-17 14:02:03	Checking for Malware Permissions	OK

2024-11-17 14:02:03	Fetching icon path	OK
2024-11-17 14:02:03	Library Binary Analysis Started	OK
2024-11-17 14:02:03	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2024-11-17 14:02:04	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2024-11-17 14:02:04	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2024-11-17 14:02:04	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2024-11-17 14:02:04	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2024-11-17 14:02:04	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2024-11-17 14:02:04	Analyzing lib/armeabi-v7a/libflutter.so	OK
2024-11-17 14:02:04	Analyzing lib/armeabi-v7a/libapp.so	OK
2024-11-17 14:02:04	Analyzing lib/arm64-v8a/libflutter.so	OK

2024-11-17 14:02:04	Analyzing lib/arm64-v8a/libapp.so	OK
2024-11-17 14:02:04	Analyzing lib/x86_64/libflutter.so	OK
2024-11-17 14:02:04	Analyzing lib/x86_64/libapp.so	OK
2024-11-17 14:02:05	Reading Code Signing Certificate	OK
2024-11-17 14:02:05	Running APKiD 2.1.5	OK
2024-11-17 14:02:07	Updating Trackers Database....	OK
2024-11-17 14:02:07	Detecting Trackers	OK
2024-11-17 14:02:08	Decompiling APK to Java with jadx	OK
2024-11-17 14:02:09	Converting DEX to Smali	OK
2024-11-17 14:02:09	Code Analysis Started on - java_source	OK
2024-11-17 14:02:10	Android SAST Completed	OK

2024-11-17 14:02:10	Android API Analysis Started	OK
2024-11-17 14:02:10	Finished Code Analysis, Email and URL Extraction	OK
2024-11-17 14:02:10	Extracting String data from APK	OK
2024-11-17 14:02:10	Extracting String data from SO	OK
2024-11-17 14:02:11	Extracting String data from Code	OK
2024-11-17 14:02:11	Extracting String values and entropies from Code	OK
2024-11-17 14:02:11	Performing Malware check on extracted domains	OK
2024-11-17 14:02:11	Saving to Database	OK
2024-11-17 14:03:57	Performing Malware check on extracted domains	OK
2024-11-17 14:04:00	Detecting Trackers from Domains	OK
2024-11-17 14:04:00	Detecting Trackers from Runtime dependencies	OK

Report Generated by - MobSF v4.1.4

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.