



ANDROID STATIC ANALYSIS REPORT



 InjuredAndroid (1.0.9)

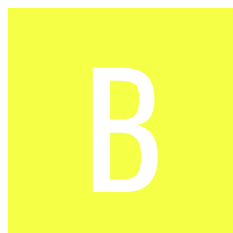
File Name: InjuredAndroid-1.0.12-release.apk

Package Name: b3nac.injuredandroid






Scan Date: Nov. 14, 2025, 1:09 p.m.

App Security Score: 49/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	14	3	2	1

FILE INFORMATION

File Name: InjuredAndroid-1.0.12-release.apk

Size: 23.58MB

MD5: 6744eaa4c0802c1086d1e8a38f58fe48

SHA1: 9df4a98867f847a75b9c76f3fec9cce23f37afbb

SHA256: b6b8d2dbd7a428b7754e6e537ba5790c35a73253533454e0768dbf1520a7ed15

APP INFORMATION

App Name: InjuredAndroid

Package Name: b3nac.injuredandroid

Main Activity: b3nac.injuredandroid.MainActivity

Target SDK: 29

Min SDK: 21

Max SDK:

Android Version Name: 1.0.9

Android Version Code: 17

APP COMPONENTS

Activities: 31
Services: 1
Receivers: 1
Providers: 2
Exported Activities: 9
Exported Services: 0
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: C=US, ST=CA, L=Sacramento, O=B3nac Sec, OU=B3nac Sec, CN=Kyle Benac
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-17 16:58:18+00:00
Valid To: 2045-05-11 16:58:18+00:00
Issuer: C=US, ST=CA, L=Sacramento, O=B3nac Sec, OU=B3nac Sec, CN=Kyle Benac
Serial Number: 0x1e6182c6
Hash Algorithm: sha256
md5: 755e4d6261b08766d610cfc582026568
sha1: 9c582658a48d5ca75cf26b56531d7d9e1540055f
sha256: df392dad8fc6acc1338df3e45833050fdc0a29124f3917d2425a89f2d0229a7b
sha512: 76a933453b7f6cfe5a210f0b8e0fed412a366f9755cf28d9ec92bc428995bf8d131c7aee231ad15c14aeaea26a2527df355945359a8e6e70f4a7320e53e06c42
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3d8e6b46ff11d89e09a435acdd2a1ae6d82a4b67911f006c3b4eea5eaf086bf0
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

 **APKID ANALYSIS**

FILE	DETAILS	
assets/narnia.arm64	FINDINGS	DETAILS
	anti_hook	syscalls

FILE	DETAILS	
classes.dex		
	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8

 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
b3nac.injuredandroid.CSPBypassActivity	Schemes: http://, https://, Hosts: b3nac.com, Path Patterns: /.*/,
b3nac.injuredandroid.RCEActivity	Schemes: flag13://, Hosts: rce,
b3nac.injuredandroid.DeepLinkActivity	Schemes: flag11://, https://,

 NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

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: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
4	Activity (b3nac.injuredandroid.FlagEighteenActivity) 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 (b3nac.injuredandroid.CSPBypassActivity) 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	Activity (b3nac.injuredandroid.RCEActivity) 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.
7	Activity (b3nac.injuredandroid.ExportedProtectedIntent) 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.
8	Activity (b3nac.injuredandroid.QXV0aA) 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.
9	Activity (b3nac.injuredandroid.DeepLinkActivity) 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.
10	Activity (b3nac.injuredandroid.b25IAActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Broadcast Receiver (b3nac.injuredandroid.FlagFiveReceiver) 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.
12	Activity (b3nac.injuredandroid.TestBroadcastReceiver) 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.
13	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [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. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/a/k/a/a.java a/a/n/g.java a/g/d/c.java a/g/d/e.java a/g/d/f.java a/g/d/g.java a/g/d/j.java a/g/d/k.java a/g/g/c.java a/g/i/b.java a/g/j/c.java

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	a/g/k/a0.java a/g/k/a1.java a/g/k/b0/c.java a/g/k/f.java a/g/k/h.java a/g/k/s.java a/g/k/t.java a/g/k/v.java a/i/b/c.java a/l/a/b.java a/m/a/a.java a/p/i0.java a/p/y.java a/q/a/a/h.java b/a/a/u.java b/c/a/a/b/d.java b/c/a/a/b/g.java b/c/a/a/b/h.java b/c/a/a/b/k/a.java b/c/a/a/b/l/a.java b/c/a/a/b/p.java b/c/a/a/b/q.java b/c/a/a/d/c/q1.java b/c/a/a/e/b/a.java b/c/a/b/l/h.java b/c/a/b/n/a.java b/c/a/b/x/d.java b/c/a/b/y/b.java b/c/c/c.java b3nac/injuredandroid/AssemblyActivity.java b3nac/injuredandroid/CSPBypassActivity.java b3nac/injuredandroid/DeepLinkActivity.java b3nac/injuredandroid/FlagEightLoginActivity.java b3nac/injuredandroid/FlagEighteenActivity.java b3nac/injuredandroid/FlagFiveReceiver.java b3nac/injuredandroid/FlagNineFileActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rcbase/Activity.java b3nac/injuredandroid/FlagSeven SqliteActivity.java b3nac/injuredandroid/FlagSeven teenActivity.java b3nac/injuredandroid/RCEActivit y.java b3nac/injuredandroid/k.java c/a/b.java
2	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	b3nac/injuredandroid/k.java
3	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/b.java io/flutter/plugin/platform/d.java
4	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	b3nac/injuredandroid/f.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----	--------------	-------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/libencrypt.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/libapp.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libencrypt.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libapp.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libencrypt.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libapp.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libencrypt.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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
16	armeabi-v7a/libapp.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86_64/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	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: ['__memcpy_chk', '__vsprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86_64/libencrypt.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86_64/libapp.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/libnative-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Not Applicable info</p> <p>RELRO checks are not applicable for Flutter/Dart binaries</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libencrypt.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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64-v8a/libapp.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as 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
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	a/g/k/b0/c.java io/flutter/view/AccessibilityViewEmbedder.java
00091	Retrieve data from broadcast	collection	b3nac/injuredandroid/TestBroadcastReceiver.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	b/b/d.java b3nac/injuredandroid/CSPBypassActivity.java b3nac/injuredandroid/ContactActivity.java b3nac/injuredandroid/FlagTwelveProtectedActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	b3nac/injuredandroid/CSPBypassActivity.java
00022	Open a file from given absolute path of the file	file	b/a/a/v/e.java
00013	Read file and put it into a stream	file	a/g/d/e.java a/g/d/k.java b/a/a/v/e.java
00012	Read data and put it into a buffer stream	file	b/a/a/v/e.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/g.java
00096	Connect to a URL and set request method	command network	b/a/a/v/j.java
00089	Connect to a URL and receive input stream from the server	command network	b/a/a/v/j.java
00109	Connect to a URL and get the response code	network command	b/a/a/v/j.java
00153	Send binary data over HTTP	http	b/a/a/v/j.java
00028	Read file from assets directory	file	b3nac/injuredandroid/RCEActivity.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://injuredandroid.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/430943006316/namespaces/firebase:fetch?key=AlzaSyCUImEIOSvqAswLqFak75xhskkB6illd7A . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE
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.

! 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: 20.207.73.82 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.250.67.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
injuredandroid.firebaseio.com	ok	IP: 35.201.97.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
m.do.co	ok	IP: 104.21.61.61 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
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



EMAIL	FILE
u0013android@android.com0 u0013android@android.com	b/c/a/a/b/v.java
b3nac.sec@gmail.com	b3nac/injuredandroid/ContactActivity.java
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AlzaSyCUImEIOSvqAswLqFak75xhskkB6illd7A"
"firebase_database_url" : "https://injuredandroid.firebaseio.com"
"google_crash_reporting_api_key" : "AlzaSyCUImEIOSvqAswLqFak75xhskkB6illd7A"
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
115792089210356248762697446949407573530086143415290314195533631308867097853951
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573529996955224135760342422259061068512044369
VGhlIGZsYWcgaXMgYWxzbyBhIHBhc3N3b3JkIQ==
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

 SCAN LOGS

Timestamp	Event	Error
-----------	-------	-------

2025-11-14 13:09:43	Generating Hashes	OK
2025-11-14 13:09:43	Extracting APK	OK
2025-11-14 13:09:43	Unzipping	OK
2025-11-14 13:09:44	Parsing APK with androguard	OK
2025-11-14 13:09:44	Extracting APK features using aapt/aapt2	OK
2025-11-14 13:09:44	Getting Hardcoded Certificates/Keystores	OK
2025-11-14 13:09:47	Parsing AndroidManifest.xml	OK
2025-11-14 13:09:47	Extracting Manifest Data	OK
2025-11-14 13:09:47	Manifest Analysis Started	OK
2025-11-14 13:09:47	Reading Network Security config from network_security_config.xml	OK
2025-11-14 13:09:47	Parsing Network Security config	OK

2025-11-14 13:09:47	Performing Static Analysis on: InjuredAndroid (b3nac.injuredandroid)	OK
2025-11-14 13:09:49	Fetching Details from Play Store: b3nac.injuredandroid	OK
2025-11-14 13:09:50	Checking for Malware Permissions	OK
2025-11-14 13:09:50	Fetching icon path	OK
2025-11-14 13:09:50	Library Binary Analysis Started	OK
2025-11-14 13:09:50	Analyzing lib/armeabi-v7a/libnative-lib.so	OK
2025-11-14 13:09:50	Analyzing lib/armeabi-v7a/libflutter.so	OK
2025-11-14 13:09:50	Analyzing lib/armeabi-v7a/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing lib/armeabi-v7a/libapp.so	OK
2025-11-14 13:09:50	Analyzing lib/x86_64/libnative-lib.so	OK
2025-11-14 13:09:50	Analyzing lib/x86_64/libflutter.so	OK

2025-11-14 13:09:50	Analyzing lib/x86_64/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing lib/x86_64/libapp.so	OK
2025-11-14 13:09:50	Analyzing lib/arm64-v8a/libnative-lib.so	OK
2025-11-14 13:09:50	Analyzing lib/arm64-v8a/libflutter.so	OK
2025-11-14 13:09:50	Analyzing lib/arm64-v8a/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing lib/arm64-v8a/libapp.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/armeabi-v7a/libnative-lib.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/armeabi-v7a/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/x86_64/libnative-lib.so	OK

2025-11-14 13:09:50	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/x86_64/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/arm64-v8a/libnative-lib.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/arm64-v8a/libencrypt.so	OK
2025-11-14 13:09:50	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2025-11-14 13:09:50	Reading Code Signing Certificate	OK
2025-11-14 13:09:51	Running APKiD 3.0.0	OK
2025-11-14 13:09:56	Detecting Trackers	OK
2025-11-14 13:09:57	Decompiling APK to Java with JADX	OK

2025-11-14 13:10:07	Converting DEX to Smali	OK
2025-11-14 13:10:07	Code Analysis Started on - java_source	OK
2025-11-14 13:10:08	Android SBOM Analysis Completed	OK
2025-11-14 13:10:09	Android SAST Completed	OK
2025-11-14 13:10:09	Android API Analysis Started	OK
2025-11-14 13:10:10	Android API Analysis Completed	OK
2025-11-14 13:10:10	Android Permission Mapping Started	OK
2025-11-14 13:10:11	Android Permission Mapping Completed	OK
2025-11-14 13:10:11	Android Behaviour Analysis Started	OK
2025-11-14 13:10:12	Android Behaviour Analysis Completed	OK
2025-11-14 13:10:12	Extracting Emails and URLs from Source Code	OK

2025-11-14 13:10:13	Email and URL Extraction Completed	OK
2025-11-14 13:10:13	Extracting String data from APK	OK
2025-11-14 13:10:13	Extracting String data from SO	OK
2025-11-14 13:10:13	Extracting String data from Code	OK
2025-11-14 13:10:13	Extracting String values and entropies from Code	OK
2025-11-14 13:10:16	Performing Malware check on extracted domains	OK
2025-11-14 13:10:21	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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).