

ANDROID STATIC ANALYSIS REPORT



HappyMod

Package Name:	com.happymod.apk
Scan Date:	Oct. 17, 2025, 4:28 p.m.
App Security Score:	57/100 (MEDIUM RIS
Grade:	



∰ HIGH	▲ MEDIUM	i INFO	✓ SECURE	[®] HOTSPOT
0	17	0	2	0

FILE INFORMATION

File Name: HappyMod-3-2-3.apk

Size: 18.89MB

MD5: 3228b04b9d1292134f9ac12196c0dc28

SHA1: 2c454d6e73c5ca2d583bc91947b0431817a01245

SHA256: 681be1221fa3ac3a18f7bc16048dd6bd0fb358df4964de0eca4cb8fc9b75996b

i APP INFORMATION

App Name: HappyMod

Package Name: com.happymod.apk

Main Activity: com.happymod.apk.hmmvp.main.LaunchActivity

Target SDK: 31 Min SDK:

Max SDK:

Android Version Name: Android Version Code:

EE APP COMPONENTS

Activities: 79
Services: 14
Receivers: 13
Providers: 4
Exported Activities: 5

Exported Services: 0 Exported Receivers: 10 Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: True v4 signature: False X.509 Subject: O=evz

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2018-03-15 08:11:53+00:00 Valid To: 2118-02-19 08:11:53+00:00

Issuer: O=evz

Serial Number: 0x3dec09c4 Hash Algorithm: sha256

md5: eb3c6564a7a7f8332a98bd9c139822d4 sha1: 8f16d0f9eab6ffb4ccef615c7a6b015210e09b1f

sha256: c3846f1b45b579e694f13553f5d7ae45615bac95647f8ed8bd76c9153ef4e0d3

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: caa9a620c516e161eb33edc349a203b28c641e6ccbbcd8140fb69c8ce8368e3f

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS			
3228b04b9d1292134f9ac12196c0dc28.apk	FINDINGS	DETAILS		
SZZOBO IBSU IZSZ IS IISUCIZ ISOCOUCZOJAPK	Packer Found	Jiagu		
classes.dex	FINDINGS	DETAILS		
Clubbes.dex	Compiler	dexlib 2.x		

△ NETWORK SECURITY

NO SCOPE	SEVERITY	DESCRIPTION
----------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity () 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.
3	Activity () 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.
4	Activity () 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.
5	Activity () 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 () 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	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
8	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
9	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
11	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
14	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
16	Broadcast Receiver () is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

</> CODE ANALYSIS

NO ISSUE SEVERITY STANDARDS	FILES
-----------------------------	-------



NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	assets/libjiagu.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
2	assets/libjiagu_a64.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: ['strlen_chk', '_snprintf_chk', 'FD_SET_chk', 'sprintf_chk', '_read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	assets/libjiagu_x86.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
4	assets/libjiagu_x64.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: ['read_chk', 'strlen_chk', 'FD_SET_chk', 'snprintf_chk', 'sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86/libHappymodPrincess.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
7	armeabi-v7a/libjlibtorrent- 1.2.15.2.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: ['memcpy_chk', 'vsprintf_chk', 'vsnprintf_chk', 'memmove_chk', 'write_chk', 'strchr_chk', 'strchr_chk', 'memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi- v7a/libHappymodPrincess.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
10	arm64-v8a/libjlibtorrent- 1.2.15.2.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: ['_memcpy_chk', '_vsprintf_chk', '_wrine_chk', '_memmove_chk', '_strchr_chk', '_stren_chk', '_read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64- v8a/libHappymodPrincess.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
13	assets/libjiagu.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
14	assets/libjiagu_a64.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: ['strlen_chk', 'snprintf_chk', 'FD_SET_chk', 'sprintf_chk', 'read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	assets/libjiagu_x86.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	assets/libjiagu_x64.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: ['read_chk', 'strlen_chk', 'FD_SET_chk', 'snprintf_chk', 'sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86/libHappymodPrincess.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
19	armeabi-v7a/libjlibtorrent- 1.2.15.2.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: ['_memcpy_chk', '_vsprintf_chk', '_wsnprintf_chk', '_memmove_chk', '_strchr_chk', '_strchr_chk', '_strlen_chk', '_memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	armeabi-v7a/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	armeabi- v7a/libHappymodPrincess.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
22	arm64-v8a/libjlibtorrent- 1.2.15.2.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: ['_memcpy_chk', '_vsprintf_chk', '_wsnprintf_chk', '_memmove_chk', '_strchr_chk', '_strchr_chk', '_strlen_chk', '_read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libCSTAMP.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: ['_memcpy_chk', '_strlen_chk', '_strcpy_chk', '_strcat_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64- v8a/libHappymodPrincess.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.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/tianyu/util/a.java
00012	Read data and put it into a buffer stream	file	com/tianyu/util/a.java
00022	Open a file from given absolute path of the file	file	com/stub/StubApp.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/379613389119/namespaces/firebase:fetch? key=AlzaSyDSXPSa8tDX7dsVnTFizTYBZ0ZsUP4-Y5Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

***: ::** ABUSED PERMISSIONS

ТҮРЕ	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.

• OFAC SANCTIONED COUNTRIES

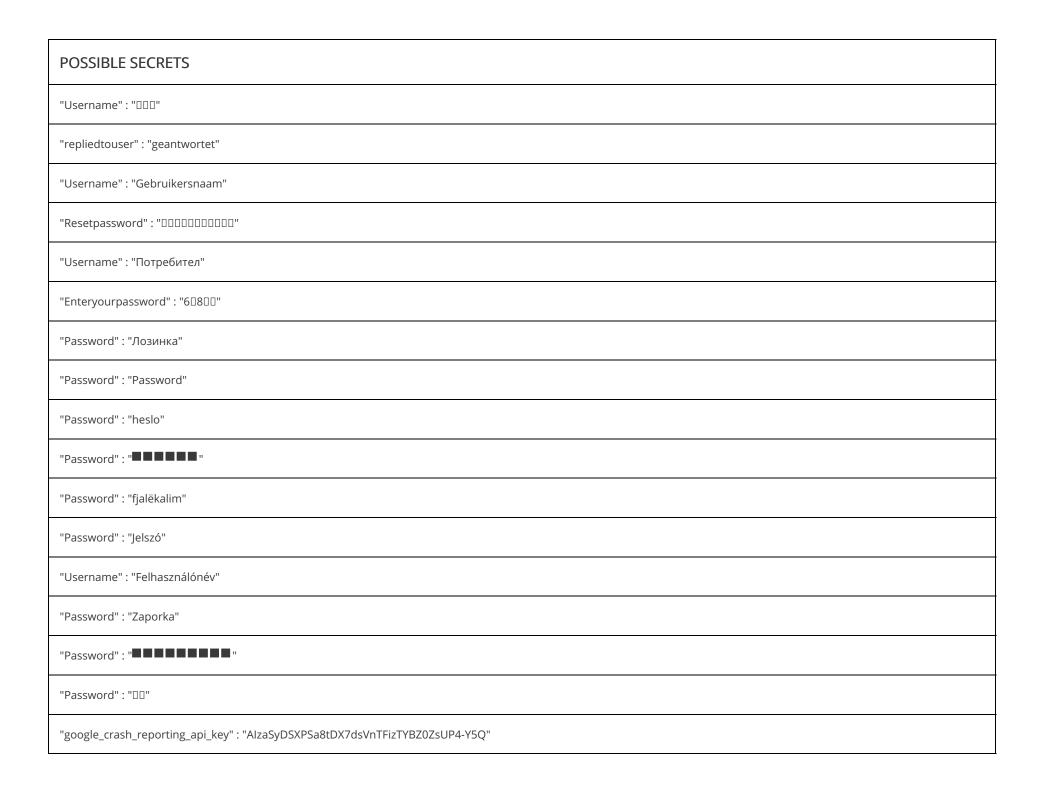
This app may communicate with the following OFAC sanctioned list of countries.

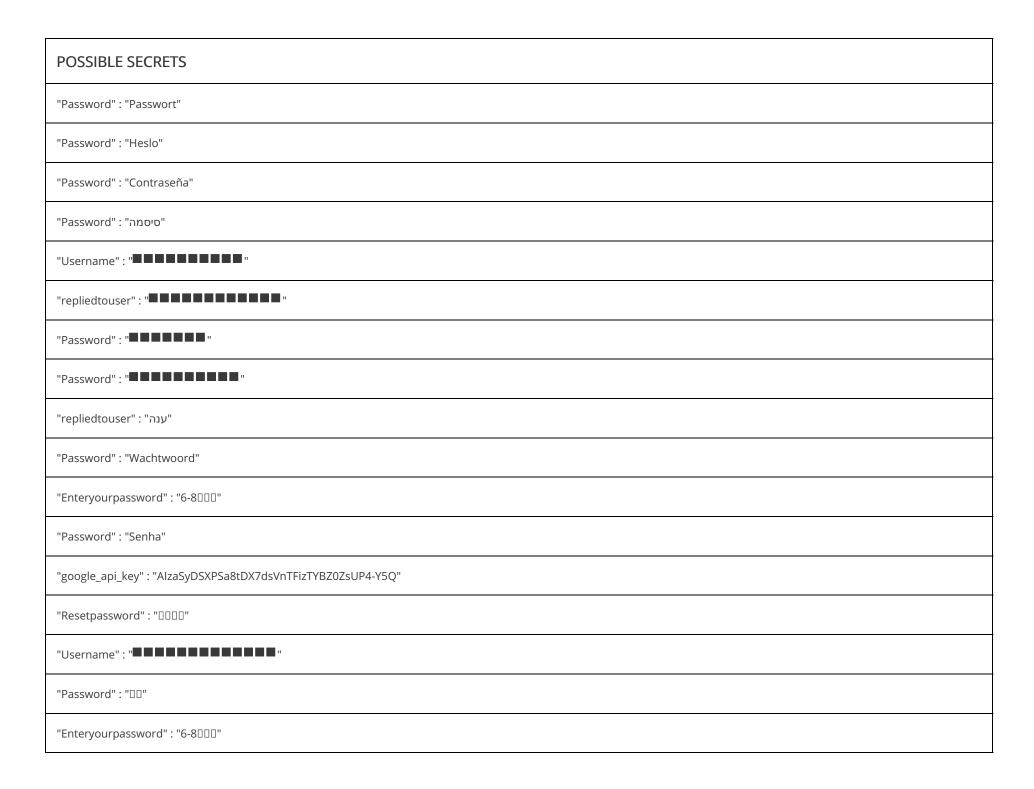
DOMAIN COUNTRY/REGION

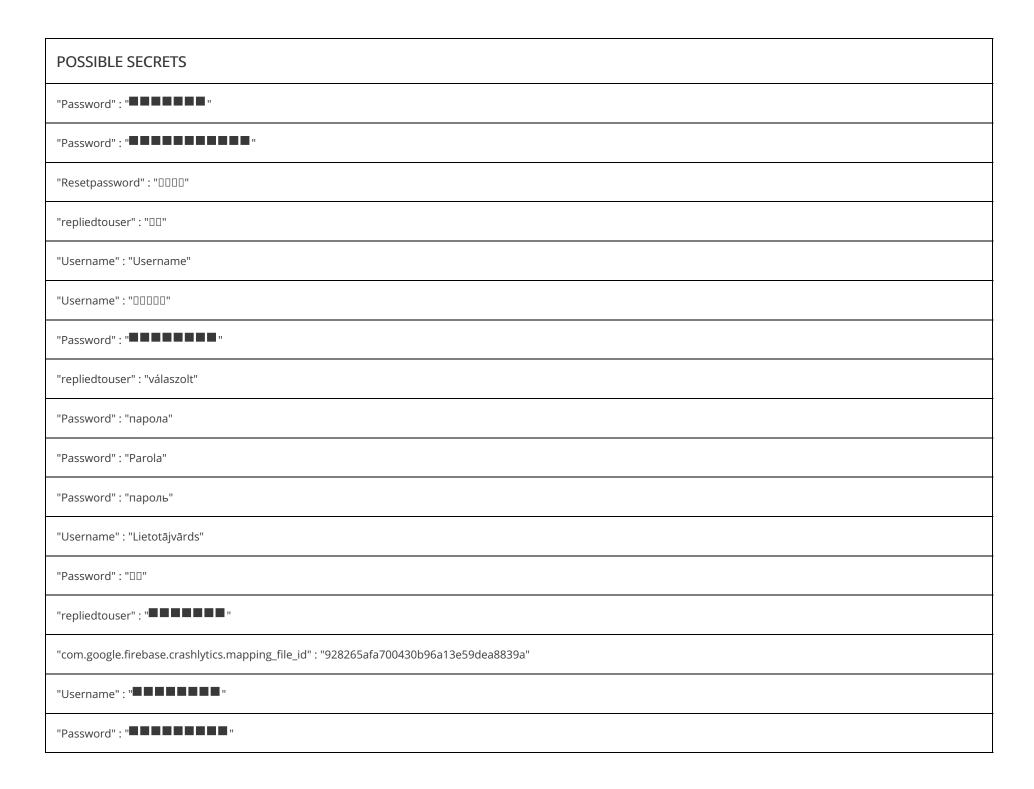
Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
schemas.xmlsoap.org	ok	IP: 13.107.246.58 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
www.winimage.com	ok	IP: 49.44.79.236 Country: India Region: Kerala City: Kochi Latitude: 9.939880 Longitude: 76.260223 View: Google Map









POSSIBLE SECRETS
"repliedtouser" : "
"repliedtouser" : "DDDDD"
"Username" : "DDD"
"Username" : "
"Username" : "
"Username" : "Nutzername"
"Password" : "Parole"
"repliedtouser" : "ロロ"
"Resetpassword": "
"dyStrategy.privateAddress" : "privateAddress"
"Password": "00000"
"repliedtouser" : "odpovedal"
"Password" : "Hasło"
"repliedtouser" : "απάντησε"

⋮≡ SCAN LOGS

Timestamp	Event	Error
2025-10-17 16:28:42	Generating Hashes	OK
2025-10-17 16:28:42	Extracting APK	ОК
2025-10-17 16:28:42	Unzipping	ОК
2025-10-17 16:28:42	Parsing APK with androguard	ОК
2025-10-17 16:28:43	Extracting APK features using aapt/aapt2	ОК
2025-10-17 16:28:43	Getting Hardcoded Certificates/Keystores	ОК
2025-10-17 16:28:46	Parsing AndroidManifest.xml	ОК
2025-10-17 16:28:46	Extracting Manifest Data	ОК
2025-10-17 16:28:46	Manifest Analysis Started	ОК
2025-10-17 16:28:46	Performing Static Analysis on: HappyMod (com.happymod.apk)	ОК
2025-10-17 16:28:47	Fetching Details from Play Store: com.happymod.apk	ОК

2025-10-17 16:28:48	Checking for Malware Permissions	ОК
2025-10-17 16:28:48	Fetching icon path	ОК
2025-10-17 16:28:48	Library Binary Analysis Started	ОК
2025-10-17 16:28:48	Analyzing assets/libjiagu.so	ОК
2025-10-17 16:28:48	Analyzing assets/libjiagu_a64.so	ОК
2025-10-17 16:28:48	Analyzing assets/libjiagu_x86.so	ОК
2025-10-17 16:28:48	Analyzing assets/libjiagu_x64.so	OK
2025-10-17 16:28:48	Analyzing lib/x86/libCSTAMP.so	OK
2025-10-17 16:28:48	Analyzing lib/x86/libHappymodPrincess.so	ОК
2025-10-17 16:28:48	Analyzing lib/armeabi-v7a/libjlibtorrent-1.2.15.2.so	ОК
2025-10-17 16:28:48	Analyzing lib/armeabi-v7a/libCSTAMP.so	ОК

2025-10-17 16:28:48	Analyzing lib/armeabi-v7a/libHappymodPrincess.so	ОК
2025-10-17 16:28:48	Analyzing lib/arm64-v8a/libjlibtorrent-1.2.15.2.so	OK
2025-10-17 16:28:48	Analyzing lib/arm64-v8a/libCSTAMP.so	ОК
2025-10-17 16:28:48	Analyzing lib/arm64-v8a/libHappymodPrincess.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/assets/libjiagu.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/assets/libjiagu_a64.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/assets/libjiagu_x86.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/assets/libjiagu_x64.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/lib/x86/libCSTAMP.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/lib/x86/libHappymodPrincess.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/lib/armeabi-v7a/libjlibtorrent-1.2.15.2.so	ОК

2025-10-17 16:28:48	Analyzing apktool_out/lib/armeabi-v7a/libCSTAMP.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/lib/armeabi-v7a/libHappymodPrincess.so	ОК
2025-10-17 16:28:48	Analyzing apktool_out/lib/arm64-v8a/libjlibtorrent-1.2.15.2.so	ОК
2025-10-17 16:28:49	Analyzing apktool_out/lib/arm64-v8a/libCSTAMP.so	ОК
2025-10-17 16:28:49	Analyzing apktool_out/lib/arm64-v8a/libHappymodPrincess.so	ОК
2025-10-17 16:28:49	Reading Code Signing Certificate	ОК
2025-10-17 16:28:49	Running APKiD 3.0.0	ОК
2025-10-17 16:28:53	Detecting Trackers	ОК
2025-10-17 16:28:53	Decompiling APK to Java with JADX	ОК
2025-10-17 16:28:55	Converting DEX to Smali	ОК
2025-10-17 16:28:55	Code Analysis Started on - java_source	ОК

2025-10-17 16:28:55	Android SBOM Analysis Completed	ОК
2025-10-17 16:28:56	Android SAST Completed	ОК
2025-10-17 16:28:56	Android API Analysis Started	ОК
2025-10-17 16:28:56	Android API Analysis Completed	ОК
2025-10-17 16:28:56	Android Permission Mapping Started	ОК
2025-10-17 16:28:57	Android Permission Mapping Completed	ОК
2025-10-17 16:28:57	Android Behaviour Analysis Started	ОК
2025-10-17 16:28:57	Android Behaviour Analysis Completed	ОК
2025-10-17 16:28:57	Extracting Emails and URLs from Source Code	ОК
2025-10-17 16:28:57	Email and URL Extraction Completed	ОК
2025-10-17 16:28:57	Extracting String data from APK	ОК

2025-10-17 16:28:58	Extracting String data from SO	ОК
2025-10-17 16:28:58	Extracting String data from Code	ОК
2025-10-17 16:28:58	Extracting String values and entropies from Code	ОК
2025-10-17 16:28:59	Performing Malware check on extracted domains	ОК
2025-10-17 16:29:01	Saving to Database	ОК

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.