ANDROID STATIC ANALYSIS REPORT

qr_validator_app (1.0.0)

File Name:	app-release.apk
Package Name:	com.example.qr_validator_app
Scan Date:	April 11, 2025, 8:59 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	6	3	1	1

FILE INFORMATION

File Name: app-release.apk
Size: 61.14MB
MD5: 706707e38a2f75fd7543ee87208a7c1c
SHA1: b32f85e78a1d0f624716048e3e5ee1cf64003c52
SHA256: 51d49fd77bb7d13b59f7316a6f8def833533dcb6ee4690965da3c9304700f9aa

APP INFORMATION

App Name: qr_validator_app
Package Name: com.example.qr_validator_app
Main Activity: com.example.qr_validator_app.MainActivity
Target SDK: 33
Min SDK: 29
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=singapore, ST=singapore, L=singapore, O=example, OU=example, CN=example
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-03-23 13:05:23+00:00
Valid To: 2052-08-08 13:05:23+00:00
Issuer: C=singapore, ST=singapore, L=singapore, O=example, OU=example, CN=example
Serial Number: 0xab53f095a583d0a7
Hash Algorithm: sha256
md5: a9c714a3fde3d63ca068730e266c612a
sha1: e78adc3350dd4f64846b250b4054363ecff3a77e
sha256: 2e03aa0869d4f3d6334faa4e196d5c26e286b9bea38ad4b117a6fda1ef95911d
sha512: 4650ddc1991faf0f917a8fd328d78218ff55bb764d375da924b0aaf9aa5d8bc62d7d9a96cda3130a18810d518bea8a028097c6c6bca7d933eef330df8ba32ed6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a4c97d044d9b5e80505f9c36b4bc6fff33c98be50f4900a69cfc3bdefd99d123
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.example.qr_validator_app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **3** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c0/b.java c0/e0.java c0/j.java c0/k0.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	c0/v.java com/journeyapps/barcodescanner/a.java com/journeyapps/barcodescanner/b.java d0/c.java e/e.java e/g.java e/j.java e0/d.java f0/m.java g1/a.java g1/b.java g1/c.java i/g.java j/c.java k/b1.java k/d0.java k/l0.java k/o0.java k/r0.java k/s0.java k/w.java k/z.java n0/b.java n3/i.java o/b.java o3/k.java p2/a.java p2/e.java p3/i.java q2/h.java r/e.java r/h.java r0/a.java r2/l.java s2/a.java s2/c.java s2/g.java s2/h.java s2/l.java s2/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s2/n.java s2/q.java t/f.java u1/e.java u1/g.java v1/a.java v2/b.java
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	v0/k.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	d4/a.java d4/b.java e4/a.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	v0/f.java v0/i.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	n3/a.java n3/i.java
6	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/d.java io/flutter/plugin/platform/c.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/journeyapps/barcodescanner/b.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	u2/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	q2/h.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/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.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
3	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
6	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
9	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
11	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86_64/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libsqlite3.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
00189	Get the content of a SMS message	sms	z/d.java
00188	Get the address of a SMS message	sms	z/d.java
00200	Query data from the contact list	collection contact	z/d.java
00187	Query a URI and check the result	collection sms calllog calendar	z/d.java
00201	Query data from the call log	collection calllog	z/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	z/d.java
00013	Read file and put it into a stream	file	u/g.java
00191	Get messages in the SMS inbox	sms	k/r0.java
00036	Get resource file from res/raw directory	reflection	k/r0.java v0/a.java
00147	Get the time of current location	collection location	e/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00075	Get location of the device	collection location	e/j.java
00115	Get last known location of the device	collection location	e/j.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	o/b.java p3/h.java v0/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	p3/h.java v0/a.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	d0/c.java io/flutter/view/AccessibilityViewEmbedder.java
00022	Open a file from given absolute path of the file	file	com/journeyapps/barcodescanner/b.java n3/i.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00183	Get current camera parameters and change the setting.	camera	s2/h.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/25	android.permission.INTERNET, android.permission.CAMERA

TYPE	MATCHES	PERMISSIONS
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
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 108.157.252.63 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
example.com	ok	**IP:** 23.192.228.80 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
developer.android.com	ok	**IP:** 74.125.24.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.mozilla.org	ok	**IP:** 34.111.97.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
journeyapps.com	ok	**IP:** 18.155.68.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
docs.amplify.aws	ok	**IP:** 3.165.102.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

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

✉ EMAILS

EMAIL	FILE
_immutablelist@0150898._ok _bytebuffer@7027147._new _double@0150898.fromintege _lga@112287047.zfc _growablelist@0150898._literal support@qrvalidator.example _assertionerror@0150898._create _typeerror@0150898._create	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/x86_64/libflutter.so

EMAIL	FILE
_immutablelist@0150898._ok _bytebuffer@7027147._new _double@0150898.fromintege _lga@112287047.zfc _growablelist@0150898._literal support@qrvalidator.example _assertionerror@0150898._create _typeerror@0150898._create	apktool_out/lib/armeabi-v7a/libapp.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so
appro@openssl.org	apktool_out/lib/x86_64/libflutter.so

HARDCODED SECRETS

POSSIBLE SECRETS
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
515d6767-01b7-49e5-8273-c8d11b0f331d
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK

POSSIBLE SECRETS
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg

SCAN LOGS

Timestamp	Event	Error
2025-04-11 08:59:30	Generating Hashes	OK
2025-04-11 08:59:32	Extracting APK	OK
2025-04-11 08:59:33	Unzipping	OK
2025-04-11 08:59:34	Parsing APK with androguard	OK
2025-04-11 08:59:36	Extracting APK features using aapt/aapt2	OK
2025-04-11 08:59:37	Getting Hardcoded Certificates/Keystores	OK
2025-04-11 08:59:44	Parsing AndroidManifest.xml	OK

2025-04-11 08:59:44	Extracting Manifest Data	OK
2025-04-11 08:59:45	Manifest Analysis Started	OK
2025-04-11 08:59:47	Performing Static Analysis on: qr_validator_app (com.example.qr_validator_app)	OK
2025-04-11 08:59:48	Fetching Details from Play Store: com.example.qr_validator_app	OK
2025-04-11 09:01:57	Checking for Malware Permissions	OK
2025-04-11 09:01:57	Fetching icon path	OK
2025-04-11 09:01:57	Library Binary Analysis Started	OK
2025-04-11 09:01:57	Analyzing lib/armeabi-v7a/libflutter.so	OK
2025-04-11 09:01:57	Analyzing lib/armeabi-v7a/libsqlite3.so	OK
2025-04-11 09:01:57	Analyzing lib/armeabi-v7a/libapp.so	OK
2025-04-11 09:01:57	Analyzing lib/arm64-v8a/libflutter.so	OK

2025-04-11 09:01:58	Analyzing lib/arm64-v8a/libsqlite3.so	OK
2025-04-11 09:01:58	Analyzing lib/arm64-v8a/libapp.so	OK
2025-04-11 09:01:58	Analyzing lib/x86_64/libflutter.so	OK
2025-04-11 09:01:58	Analyzing lib/x86_64/libsqlite3.so	OK
2025-04-11 09:01:59	Analyzing lib/x86_64/libapp.so	OK
2025-04-11 09:01:59	Analyzing lib/x86/libsqlite3.so	OK
2025-04-11 09:01:59	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2025-04-11 09:01:59	Analyzing apktool_out/lib/armeabi-v7a/libsqlite3.so	OK
2025-04-11 09:01:59	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2025-04-11 09:02:00	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2025-04-11 09:02:00	Analyzing apktool_out/lib/arm64-v8a/libsqlite3.so	OK

2025-04-11 09:02:00	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2025-04-11 09:02:00	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2025-04-11 09:02:00	Analyzing apktool_out/lib/x86_64/libsqlite3.so	OK
2025-04-11 09:02:01	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2025-04-11 09:02:01	Analyzing apktool_out/lib/x86/libsqlite3.so	OK
2025-04-11 09:02:01	Reading Code Signing Certificate	OK
2025-04-11 09:02:02	Running APKiD 2.1.5	OK
2025-04-11 09:02:05	Detecting Trackers	OK
2025-04-11 09:02:06	Decompiling APK to Java with JADX	OK
2025-04-11 09:02:14	Converting DEX to Smali	OK
2025-04-11 09:02:15	Code Analysis Started on - java_source	OK

2025-04-11 09:02:15	Android SBOM Analysis Completed	OK
2025-04-11 09:02:18	Android SAST Completed	OK
2025-04-11 09:02:18	Android API Analysis Started	OK
2025-04-11 09:02:19	Android API Analysis Completed	OK
2025-04-11 09:02:20	Android Permission Mapping Started	OK
2025-04-11 09:02:21	Android Permission Mapping Completed	OK
2025-04-11 09:02:21	Android Behaviour Analysis Started	OK
2025-04-11 09:02:23	Android Behaviour Analysis Completed	OK
2025-04-11 09:02:23	Extracting Emails and URLs from Source Code	OK
2025-04-11 09:02:24	Email and URL Extraction Completed	OK
2025-04-11 09:02:25	Extracting String data from APK	OK

2025-04-11 09:02:25	Extracting String data from SO	OK
2025-04-11 09:02:26	Extracting String data from Code	OK
2025-04-11 09:02:26	Extracting String values and entropies from Code	OK
2025-04-11 09:02:27	Performing Malware check on extracted domains	OK
2025-04-11 09:02:29	Saving to Database	OK

Report Generated by - MobSF v4.3.2

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.