



ANDROID STATIC ANALYSIS REPORT



Android DamnVulnerableBank (1.0)

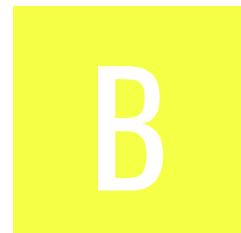
File Name: dvba.apk

Package Name: com.app.damnvulnerablebank

Scan Date: Dec. 26, 2025, 10:01 a.m.

App Security Score: **44/100 (MEDIUM RISK)**

Grade:



FINDINGS SEVERITY



FILE INFORMATION

File Name: dvba.apk

Size: 3.61MB

MD5: 5b40b49cd80dbe20ba611d32045b57c

SHA1: 23dcd688fe4dd830cf92309755a5bbd603df8789

SHA256: 76c308fac6a655a3534771777780e004feb1d91be032857768c891b2baf40ba6

APP INFORMATION

App Name: DamnVulnerableBank

Package Name: com.app.damnvulnerablebank

Main Activity: com.app.damnvulnerablebank.SplashScreen

Target SDK: 29

Min SDK: 21

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 19

Services: 1

Receivers: 0

Providers: 1

Exported Activities: 5

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: None

X.509 Subject: O=dvba, OU=dvba, CN=damncorp

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-10-29 07:43:13+00:00

Valid To: 2045-10-23 07:43:13+00:00

Issuer: O=dvba, OU=dvba, CN=damncorp

Serial Number: 0x1230704c

Hash Algorithm: sha256

md5: 41d413f665c0f789b190b96341e540c8

sha1: e26ea75bdc6ab4769acedc4c78027aab8580a858

sha256: 0d770dd2df7f63e949e8ca87b7e97ba6827762e289bd281679910609568acdde

sha512: 0943f72dcc5c543af6bf2648ba2f928f5652987b713622d2f015709af490e1b33174e7f18e149cce039e1d0303ab7e80fe47977eceed4ae28e91c6b9a66a58a5

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: e9637ca397b8c7197333f1b6da9ddb4ad5bb1fce1f123f1415751e103fda196

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8

FILE	DETAILS	
	FINDINGS	DETAILS
lib/armeabi-v7a/libtool-checker.so	anti_root	RootBeer
lib/x86/libtool-checker.so	anti_root	RootBeer
lib/x86_64/libtool-checker.so	anti_root	RootBeer

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.app.damnvulnerablebank.CurrencyRates	Schemes: http://, https://, Hosts: xe.com,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	high	Base config is configured to trust user installed certificates.
3	*	warning	Base config is configured to trust system certificates.

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: 4 | WARNING: 6 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
5	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=http://xe.com]	high	App Link asset verification URL (http://xe.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
6	App Link assetlinks.json file not found [android:name=com.app.damnvulnerablebank.CurrencyRates] [android:host=https://xe.com]	high	App Link asset verification URL (https://xe.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
7	Activity (com.app.damnvulnerablebank.CurrencyRates) 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.
8	Activity (com.app.damnvulnerablebank.SendMoney) 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 (com.app.damnvulnerablebank.ViewBalance) 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.
10	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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	<p>Activity (com.google.firebaseio.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission:</p> <pre>com.google.firebaseio.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]</pre>	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: 0 | WARNING: 1 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/a/a/a.java b/b/k/h.java b/b/k/k.java b/b/k/r.java b/b/k/t.java b/b/l/a/a.java b/b/o/f.java b/b/o/i/d.java b/b/o/i/g.java b/b/p/a0.java b/b/p/a1.java b/b/p/d1.java b/b/p/k0.java b/b/p/m0.java b/b/p/n0.java b/b/p/r0.java b/b/p/s0.java b/b/p/w.java b/b/p/z0.java h/d/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<u>The App logs information. Sensitive information should never be logged.</u>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	b/a.java b/d/c.java b/d/e.java b/g/c/c.java b/g/c/d.java b/g/c/e.java b/i/d/b.java b/i/d/c.java b/i/d/e.java b/i/f/c.java b/i/f/d.java b/i/f/e.java b/i/f/f.java b/i/f/g.java b/i/f/k/d.java b/i/g/a/a.java b/i/i/b.java b/i/l/a.java b/i/m/a.java b/i/m/b.java b/i/m/f.java b/i/m/l.java b/i/m/p.java b/i/m/u.java b/j/a/b.java b/k/b/e.java b/l/a/e.java b/l/a/k.java b/p/a/a.java b/t/b0.java b/u/a/a/f.java c/a/b/j.java c/a/b/v.java c/a/b/w/h.java c/b/a/j.java c/b/a/n.java c/c/a/a/c/d.java c/c/a/a/c/g.java c/c/a/a/c/h.java c/c/a/a/c/k/k/b0.java c/c/a/a/c/k/k/d.java c/c/a/a/c/k/k/u.java c/c/a/a/c/l/a.java

NO	ISSUE	SEVERITY	STANDARDS	c/c/a/a/c/l/b.java FILEs/c/l/d.java c/c/a/a/c/l/d0.java
				c/c/a/a/c/l/e.java c/c/a/a/c/l/e0.java c/c/a/a/c/l/i.java c/c/a/a/c/l/l.java c/c/a/a/c/m/a.java c/c/a/a/c/t.java c/c/a/a/f/c/a1.java c/c/a/a/g/b/a.java c/c/a/b/a0/b.java c/c/a/b/b0/a.java c/c/a/b/l/g.java c/c/b/b.java c/c/b/h/c0/a/e.java c/c/b/h/c0/a/j0.java c/c/b/h/c0/a/k0.java c/c/b/h/c0/a/x0.java c/c/b/h/d0/i.java c/c/b/h/d0/k.java c/c/b/h/d0/p.java c/c/b/h/d0/z.java c/c/b/h/y.java com/app/damnvulnerablebank/BankLogin.java com/app/damnvulnerablebank/MainActivity.java
2	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	com/app/damnvulnerablebank/MainActivity.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a/a/a/a.java

FLAG SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libfrida-check.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.</p> <p>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/libtool-checker.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
3	arm64-v8a/libfrida-check.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.</p> <p>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	arm64-v8a/libtool-checker.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>False high</p> <p>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.</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
5	x86_64/libfrida-check.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
6	x86_64/libtool-checker.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>False high</p> <p>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.</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
7	x86/libfrida-check.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
8	x86/libtool-checker.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
9	armeabi-v7a/libfrida-check.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.</p> <p>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
10	armeabi-v7a/libtool-checker.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
11	arm64-v8a/libfrida-check.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
12	arm64-v8a/libtool-checker.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>False high</p> <p>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.</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
13	x86_64/libfrida-check.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	x86_64/libtool-checker.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
15	x86/libfrida-check.so	<p>True info 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 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 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 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>	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	x86/libtool-checker.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
00125	Check if the given file path exist	file	a/a/a/a/a.java com/app/damnvulnerablebank/MMainActivity.java
00013	Read file and put it into a stream	file	a/a/a/a/a.java b/i/f/e.java b/i/f/f.java c/a/b/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a/a/a/a/a.java c/c/a/a/c/l/f0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	c/c/a/a/c/l/f0.java
00022	Open a file from given absolute path of the file	file	c/a/b/d.java c/a/b/w/d.java
00012	Read data and put it into a buffer stream	file	c/a/b/d.java
00024	Write file after Base64 decoding	reflection file	a/a/a/a/a.java
00036	Get resource file from res/raw directory	reflection	a/a/a/a/a.java b/b/p/r0.java
00075	Get location of the device	collection location	b/b/k/t.java
00096	Connect to a URL and set request method	command network	c/a/b/w/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	c/a/b/w/f.java
00109	Connect to a URL and get the response code	network command	c/a/b/w/f.java
00153	Send binary data over HTTP	http	c/a/b/w/f.java
00191	Get messages in the SMS inbox	sms	b/b/p/r0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://damn-vulnerable-bank.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firbaseremoteconfig.googleapis.com/v1/projects/932398433474/namespaces.firebaseio:fetch?key=AlzaSyBbOHG6DDa6DOcRGEg57mw9nXXcw6la3c . This is indicated by the response: {'state': 'NO_TEMPLATE'}

:::: ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	1/25	android.permission.INTERNET

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
www.xe.com	ok	IP: 13.224.106.119 Country: Spain Region: Madrid, Comunidad de Madrid City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	IP: 172.217.26.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
damn-vulnerable-bank.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
schemas.android.com	ok	No Geolocation information available.

✉️ EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	c/c/a/a/c/y.java

🔑 HARDCODED SECRETS

POSSIBLE SECRETS

"google_crash_reporting_api_key" : "AlzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"

"google_api_key" : "AlzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"

"firebase_database_url" : "https://damn-vulnerable-bank.firebaseio.com"

GmdBWksdEwAZFAILVEdDX1FKS0jtQU1DHggaBkNXQQFjTkdBUMJBgMCFQUIFA5MXUFPDxDdBg4PCkNWY05HQU1DFAYaDwgDBlhTTkUSAgwfHQcjBk9rWkkTbRw=

SCAN LOGS

Timestamp	Event	Error
2025-12-26 10:01:54	Generating Hashes	OK
2025-12-26 10:01:54	Extracting APK	OK
2025-12-26 10:01:54	Unzipping	OK
2025-12-26 10:01:54	Parsing APK with androguard	OK
2025-12-26 10:01:54	Extracting APK features using aapt/aapt2	OK

2025-12-26 10:01:55	Getting Hardcoded Certificates/Keystores	OK
2025-12-26 10:02:00	Parsing AndroidManifest.xml	OK
2025-12-26 10:02:00	Extracting Manifest Data	OK
2025-12-26 10:02:00	Manifest Analysis Started	OK
2025-12-26 10:02:02	Reading Network Security config from network_security_config.xml	OK
2025-12-26 10:02:02	Parsing Network Security config	OK
2025-12-26 10:02:02	Performing Static Analysis on: DamnVulnerableBank (com.app.damnvulnerablebank)	OK
2025-12-26 10:02:03	Fetching Details from Play Store: com.app.damnvulnerablebank	OK
2025-12-26 10:02:03	Checking for Malware Permissions	OK
2025-12-26 10:02:03	Fetching icon path	OK

2025-12-26 10:02:03	Library Binary Analysis Started	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/armeabi-v7a/libfrida-check.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/armeabi-v7a/libtool-checker.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/arm64-v8a/libfrida-check.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/arm64-v8a/libtool-checker.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/x86_64/libfrida-check.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/x86_64/libtool-checker.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/x86/libfrida-check.so	OK
2025-12-26 10:02:03	Analyzing apktool_out/lib/x86/libtool-checker.so	OK
2025-12-26 10:02:03	Analyzing lib/armeabi-v7a/libfrida-check.so	OK

2025-12-26 10:02:03	Analyzing lib/armeabi-v7a/libtool-checker.so	OK
2025-12-26 10:02:03	Analyzing lib/arm64-v8a/libfrida-check.so	OK
2025-12-26 10:02:04	Analyzing lib/arm64-v8a/libtool-checker.so	OK
2025-12-26 10:02:04	Analyzing lib/x86_64/libfrida-check.so	OK
2025-12-26 10:02:04	Analyzing lib/x86_64/libtool-checker.so	OK
2025-12-26 10:02:04	Analyzing lib/x86/libfrida-check.so	OK
2025-12-26 10:02:04	Analyzing lib/x86/libtool-checker.so	OK
2025-12-26 10:02:04	Reading Code Signing Certificate	OK
2025-12-26 10:02:04	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/5b40b49cd80dbe20ba611d32045b57c6/5b40b49cd80dbe20ba611d32045b57c6.apk'])

2025-12-26 10:02:04	Running APKiD 3.0.0	OK
2025-12-26 10:02:07	Detecting Trackers	OK
2025-12-26 10:02:07	Decompiling APK to Java with JADX	OK
2025-12-26 10:02:23	Converting DEX to Smali	OK
2025-12-26 10:02:23	Code Analysis Started on - java_source	OK
2025-12-26 10:02:25	Android SBOM Analysis Completed	OK
2025-12-26 10:02:29	Android SAST Completed	OK
2025-12-26 10:02:29	Android API Analysis Started	OK
2025-12-26 10:02:30	Android API Analysis Completed	OK
2025-12-26 10:02:31	Android Permission Mapping Started	OK
2025-12-26 10:02:32	Android Permission Mapping Completed	OK

2025-12-26 10:02:32	Android Behaviour Analysis Started	OK
2025-12-26 10:02:34	Android Behaviour Analysis Completed	OK
2025-12-26 10:02:34	Extracting Emails and URLs from Source Code	OK
2025-12-26 10:02:35	Email and URL Extraction Completed	OK
2025-12-26 10:02:35	Extracting String data from APK	OK
2025-12-26 10:02:35	Extracting String data from SO	OK
2025-12-26 10:02:35	Extracting String data from Code	OK
2025-12-26 10:02:36	Extracting String values and entropies from Code	OK
2025-12-26 10:02:37	Performing Malware check on extracted domains	OK
2025-12-26 10:02:38	Saving to Database	OK

Report Generated by - MobSF v4.4.4

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

