MOBSF

ANDROID STATIC ANALYSIS REPORT

DamnVulnerableBank (1.0)

File Name:	dvba.apk
Package Name:	com.app.damnvulnerablebank
Scan Date:	May 1, 2023, 2:38 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	7	1	2	0

FILE INFORMATION

File Name: dvba.apk
Size: 3.61MB
MD5: 5b40b49cd80dbe20ba611d32045b57c6
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

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
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: e9637ca397b8c7197333f1b6da9ddb4ad5bb1fcef1f123f1415751e103fda196

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

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: 1 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/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

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	b/b/p/w.java b/b/p/z0.java b/d/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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 c/c/a/a/c/l/b.java c/c/a/a/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/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libfrida-check.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
2	lib/arm64-v8a/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libfrida-check.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
4	lib/x86/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/x86_64/libfrida-check.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
6	lib/x86_64/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/armeabi-v7a/libfrida-check.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
8	lib/armeabi-v7a/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
damn-vulnerable-bank.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
plus.google.com	ok	**IP:** 173.194.73.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.xe.com	ok	**IP:** 108.156.22.101 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://damn-vulnerable-bank.firebaseio.com	info App talks to a Firebase Database.

EMAILS

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

HARDCODED SECRETS

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

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"
"google_crash_reporting_api_key" : "AIzaSyBbOHG6DDa6DOcRGEg57mw9nXYXcw6la3c"

Report Generated by - MobSF v3.6.6 Beta

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.