ANDROID STATIC ANALYSIS REPORT

DigiLocker (6.4.2)

File Name:	com.digilocker.apk
Package Name:	com.digilocker.android
Average CVSS Score:	6.6
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	3/335
Scan Date:	Jan. 20, 2021, 12:53 p.m.

FILE INFORMATION

File Name: com.digilocker.apk
Size: 54.75MB
MD5: 19766c8659b29e1d9594ae45586b9966
SHA1: cd5b517521f8b9e92a2be514b6b2cf340cd24940
SHA256: 923f5f00b673a8b077304d819928c00526f21be1a1b4053106222768e224676c

APP INFORMATION

App Name: DigiLocker
Package Name: com.digilocker.android
Main Activity: com.digilocker.android.ui.activity.dashboard.activity.MainDashboardActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 6.4.2
Android Version Code: 531

APP COMPONENTS

Activities: 101
Services: 26
Receivers: 11
Providers: 7
Exported Activities: 3
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: CN=Digi locker
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-10-16 04:35:15+00:00
Valid To: 2114-09-22 04:35:15+00:00
Issuer: CN=Digi locker
Serial Number: 0x466cbec1
Hash Algorithm: sha256
md5: ba370cd1de7f3ad7c35380bf2cc225c6
sha1: c3331c515e871a1d7f248a212388ea0eba1fd39d
sha256: 5cb0d90e404df479494ff46a3550a93d71f370c4e49cad659ec7a6f009d6d9f0
sha512: a93422f102bdb773f0058c058ed7fc2836a238850a166ca287e7dbd42e075f79041562e230d26697209534a9b58d078947d183fbb217b12b61c1fe9b2a991c50
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9cc3c8d0e1d14ede8b20be4dc191a7fd4fab7f3df828589fb89a4bc8d881f914

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0

APPLICATION PERMISSIONS

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

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.apps.photos.permission.GOOGLE_PHOTOS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_INTERNAL_STORAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.TAGS check SIM operator check possible ro.secure check
	FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check
	FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

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

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.digilocker.android.ui.activity.Uploader) is not Protected. An intent-filter exists.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	A Service 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.
6	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 None (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	defpackage/lz2.java defpackage/zf1.java defpackage/px.java defpackage/ug1.java defpackage/a73.java defpackage/u31.java defpackage/wq.java defpackage/t60.java defpackage/my.java defpackage/e50.java defpackage/oq.java defpackage/nb3.java defpackage/sq1.java defpackage/bq.java com/digilocker/android/ui/activity/ConflictsResolveActivity.java defpackage/xx.java defpackage/aa0.java defpackage/m13.java defpackage/ar2.java defpackage/bu.java defpackage/j70.java defpackage/ka2.java defpackage/sb0.java defpackage/u60.java defpackage/cx0.java defpackage/kb1.java defpackage/e60.java defpackage/a91.java defpackage/kg.java defpackage/r90.java defpackage/ty2.java defpackage/z12.java defpackage/qy2.java defpackage/my2.java defpackage/w40.java defpackage/n50.java com/digilocker/android/ui/activity/uploadedonactivity/ActivityUpload.java defpackage/m51.java defpackage/j60.java defpackage/pq1.java defpackage/v13.java defpackage/c9.java defpackage/mb3.java defpackage/y90.java defpackage/lw.java defpackage/n91.java defpackage/r92.java defpackage/gz2.java defpackage/a13.java defpackage/q50.java defpackage/q60.java defpackage/va3.java defpackage/j13.java defpackage/iz2.java defpackage/b60.java defpackage/hz2.java defpackage/r50.java defpackage/ob3.java com/digilocker/android/ui/activity/FolderPickerActivity.java defpackage/w13.java defpackage/oz2.java defpackage/h80.java defpackage/nb0.java defpackage/m50.java defpackage/no4.java defpackage/fz.java defpackage/kw.java in/gov/digilocker/ui/activity/PullAuthorizedDocumentActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CVSS V2: 4.3 None (medium) CWE: CWE-200 Information Exposure OWASP MASVS: MSTG-CODE-2	defpackage/n04.java defpackage/o04.java defpackage/xv3.java defpackage/tv3.java defpackage/ov.java defpackage/tz3.java defpackage/mx3.java defpackage/ry3.java defpackage/yw3.java defpackage/lz3.java defpackage/rv3.java com/digilocker/android/ui/activity/webview/LoginActivity.java defpackage/sv3.java defpackage/oy3.java defpackage/ev3.java defpackage/c14.java defpackage/gw3.java defpackage/wx3.java defpackage/hw3.java defpackage/vv3.java defpackage/wv.java defpackage/so4.java defpackage/uv3.java defpackage/aw3.java defpackage/qs.java defpackage/py3.java defpackage/p04.java defpackage/ru3.java defpackage/qu.java defpackage/hv3.java com/digilocker/android/authentication/AuthenticatorActivity.java defpackage/s43.java defpackage/ov3.java defpackage/su3.java defpackage/l83.java defpackage/cy3.java defpackage/iw3.java defpackage/ay3.java defpackage/mw3.java defpackage/m04.java defpackage/iv3.java defpackage/hy3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 None (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	defpackage/zl0.java defpackage/oi1.java defpackage/d81.java defpackage/t71.java defpackage/zj1.java defpackage/a33.java defpackage/fh1.java defpackage/gi1.java defpackage/j81.java defpackage/t73.java defpackage/gh0.java defpackage/dm0.java defpackage/y61.java defpackage/bl0.java defpackage/ps1.java defpackage/yf0.java defpackage/ah0.java defpackage/jf0.java defpackage/sh1.java defpackage/je2.java defpackage/xi1.java defpackage/of3.java defpackage/av1.java defpackage/dt1.java defpackage/ki1.java defpackage/ds1.java defpackage/tg0.java defpackage/yt1.java defpackage/pg0.java defpackage/gt1.java defpackage/b71.java defpackage/st1.java defpackage/mf0.java defpackage/d82.java defpackage/uh0.java defpackage/wi0.java defpackage/qk1.java defpackage/vj.java defpackage/vh4.java defpackage/k40.java defpackage/th4.java defpackage/mg0.java defpackage/rf3.java defpackage/ch1.java defpackage/dj1.java defpackage/gl0.java defpackage/o23.java defpackage/m81.java defpackage/vm2.java defpackage/mt1.java defpackage/kk4.java defpackage/sm0.java defpackage/xu2.java defpackage/pc3.java defpackage/rv1.java defpackage/as1.java defpackage/pf3.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/digilocker/android/ui/activity/UploadFilesActivity.java com/digilocker/android/ui/fragment/LocalFileListFragment.java defpackage/or.java defpackage/xy.java com/digilocker/android/utils/UriUtils.java com/digilocker/android/ui/activity/uploadedonactivity/ActivityUpload.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 None (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/stripe/android/networking/AnalyticsDataFactory.java com/stripe/android/model/parsers/SetupIntentJsonParser.java com/stripe/android/model/parsers/SourceJsonParser.java com/stripe/android/model/SourceParams.java com/stripe/android/model/parsers/EphemeralKeyJsonParser.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/networking/ApiRequest.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/view/Stripe3ds2CompletionActivity.java com/stripe/android/model/parsers/PaymentIntentJsonParser.java com/stripe/android/view/PaymentAuthWebView.java com/stripe/android/PaymentConfiguration.java
6	App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/tj.java defpackage/j03.java
7	This App uses an SSL Pinning Library (org.thoughtcrime.ssl.pinning) to prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-NETWORK-4	defpackage/c73.java defpackage/ea3.java defpackage/vn3.java defpackage/fz.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	CVSS V2: 5.9 None (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	defpackage/vk.java com/digilocker/android/db/DBProvider.java defpackage/z91.java defpackage/v93.java defpackage/u60.java defpackage/n82.java com/digilocker/android/providers/FileContentProvider.java defpackage/wr.java defpackage/r30.java defpackage/t72.java defpackage/ll.java defpackage/n30.java defpackage/l30.java defpackage/v12.java defpackage/tv.java defpackage/nx1.java defpackage/aa1.java defpackage/p30.java defpackage/q30.java defpackage/m82.java defpackage/o30.java
9	SHA-1 is a weak hash known to have hash collisions.	high	CVSS V2: 5.9 None (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/vr2.java defpackage/i03.java defpackage/yy2.java
10	This App may have root detection capabilities.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-RESILIENCE-1	defpackage/vr2.java defpackage/yf1.java com/digilocker/android/ui/activity/dashboard/activity/MainDashboardActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CVSS V2: 8.8 None (high) CWE: CWE-749 Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/digilocker/android/ui/webtemplate/ActivityProfileTemplate.java
12	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 None (info) OWASP MASVS: MSTG-STORAGE-10	com/digilocker/android/ui/activity/CopyToClipboardActivity.java
13	This App may request root (Super User) privileges.	high	CVSS V2: 0 None (info) CWE: CWE-250 Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	defpackage/ft.java
14	MD5 is a weak hash known to have hash collisions.	high	CVSS V2: 7.4 None (high) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/g91.java defpackage/d82.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libtoolChecker.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	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.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libnative-lib-DL.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	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.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86_64/libtoolChecker.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86_64/libnative-lib-DL.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/x86/libtoolChecker.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	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.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/x86/libnative-lib-DL.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	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.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/arm64-v8a/libtoolChecker.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/arm64-v8a/libnative-lib-DL.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 The shared object is built without Position Independent Code flag. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack,heap and libraries. Use compiler option -fPIC to enable Position Independent Code.	False high This shared object does not have a stack canary value added to the stack. Stack canraies are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False 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 fority 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 implement 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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', '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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
14	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
16	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
17	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
18	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
19	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate', 'The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'RFC 5280 certificate validation and certificate path validation', 'The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066'].
20	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
21	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
22	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
23	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
24	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
google.com	good	**IP:** 142.250.67.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssl.google-analytics.com	good	**IP:** 142.250.182.200 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
q.stripe.com	good	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
oauth2.authorization.server.org	good	**IP:** 91.195.241.137 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.95 **View:** Google Map
elibom.digitallocker.gov.in	good	**IP:** 164.100.161.225 **Country:** India **Region:** Delhi **City:** Delhi **Latitude:** 28.66667 **Longitude:** 77.216667 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
files.stripe.com	good	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
firebase.google.com	good	**IP:** 142.250.182.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.stripe.com	good	**IP:** 34.211.99.245 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
developers.facebook.com	good	**IP:** 31.13.79.18 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.01441 **Longitude:** 72.847939 **View:** Google Map
plus.google.com	good	**IP:** 142.250.67.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google-analytics.com	good	**IP:** 142.250.67.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
digilocker.gov.in	good	**IP:** 164.100.161.225 **Country:** India **Region:** Delhi **City:** Delhi **Latitude:** 28.66667 **Longitude:** 77.216667 **View:** Google Map
twitter.com	good	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
reports.crashlytics.com	good	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
errors.stripe.com	good	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
stripe.com	good	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.apache.org	good	**IP:** 95.216.24.32 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.93545 **View:** Google Map
owncloud.org	good	**IP:** 78.46.146.179 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.37129 **View:** Google Map
owncloud.com	good	**IP:** 78.46.146.179 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.37129 **View:** Google Map
www.googleapis.com	good	**IP:** 142.250.182.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
hooks.stripe.com	good	**IP:** 13.228.224.121 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.28967 **Longitude:** 103.850067 **View:** Google Map
fake.url	good	No Geolocation information available.
schemas.android.com	good	No Geolocation information available.
play.google.com	good	**IP:** 172.217.27.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	good	**IP:** 142.250.67.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	good	**IP:** 142.250.182.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.slf4j.org	good	**IP:** 83.166.144.67 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.13921 **View:** Google Map
firebase-settings.crashlytics.com	good	**IP:** 172.217.167.163 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	good	**IP:** 172.217.174.226 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
update.crashlytics.com	good	**IP:** 172.217.167.163 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	good	**IP:** 216.58.196.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
img1.digitallocker.gov.in	good	**IP:** 23.48.225.11 **Country:** India **Region:** Maharashtra **City:** Pune **Latitude:** 18.519569 **Longitude:** 73.855347 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	good	**IP:** 74.50.62.60 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
utils.digitallocker.gov.in	good	**IP:** 164.100.161.225 **Country:** India **Region:** Delhi **City:** Delhi **Latitude:** 28.66667 **Longitude:** 77.216667 **View:** Google Map
www.google.com	good	**IP:** 142.250.183.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.stripe.com	good	**IP:** 13.228.224.121 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.28967 **Longitude:** 103.850067 **View:** Google Map
digilocker-1032.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
source.android.com	good	**IP:** 142.250.183.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://stripe.com/docs/mobile/android/basic	com/stripe/android/EphemeralKeyManager.java
https://stripe.com/docs/keys	com/stripe/android/ApiKeyValidator.java
https://q.stripe.com	com/stripe/android/networking/AnalyticsRequest.java
https://m.stripe.com/6	com/stripe/android/networking/FingerprintRequest.java
https://api.stripe.com/edge-internal/ https://api.stripe.com/v1/	com/stripe/android/networking/StripeApiRepository.java

URL	FILE
https://api.stripe.com	com/stripe/android/networking/ApiRequest.java
https://files.stripe.com/v1/files	com/stripe/android/networking/FileUploadRequest.java
https://hooks.stripe.com/three_d_secure/authenticate https://hooks.stripe.com/redirect/complete/src_ https://hooks.stripe.com/3d_secure/complete/tdsrc_	com/stripe/android/view/PaymentAuthWebView.java
https://twitter.com/stripestatus,	com/stripe/android/exception/APIConnectionException.java
https://play.google.com/store/apps/details?id=com.digilocker.android https://img1.digitallocker.gov.in/assets/img/banner/	com/digilocker/android/MainApp.java
file:///	com/digilocker/android/ui/webtemplate/ActivityProfileTemplate.java
https://img1.digitallocker.gov.in/public/assets/logo/issuers/002292.png https://img1.digitallocker.gov.in/public/assets/logo/issuers/000027.png	com/digilocker/android/ui/activity/NotificationActivity.java
https://img1.digitallocker.gov.in/public/assets/logo/issuers/002292.png https://img1.digitallocker.gov.in/public/assets/logo/issuers/000027.png	com/digilocker/android/ui/activity/FileDisplayActivity.java
https://play.google.com/store/apps/details?id=	com/digilocker/android/ui/activity/dashboard/activity/MainDashboardActivity.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivitySigninHelp.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivitySignupHelp.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivityForgetPassword.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivityFaq.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivityHelp.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivityAboutUs.java
file:///android_asset/loader.html	com/digilocker/android/ui/activity/webview/ActivityContactUs.java
https://google.com/search?	defpackage/l52.java
javascript:(file:///android_asset/loader.html file:///android_asset/errors/connection_lost.html	defpackage/ow.java
https://fake.url	defpackage/lw.java
https://app-measurement.com/a	defpackage/bm1.java
http://goo.gl/8Rd3yj	defpackage/fa1.java
https://update.crashlytics.com/spi/v1/platforms/android/apps https://update.crashlytics.com/spi/v1/platforms/android/apps/%s https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps	defpackage/qw2.java
http://localhost	defpackage/k61.java

URL	FILE
javascript:(file:///android_asset/errors/connection_lost_after_login.html file:///android_asset/loader.html	defpackage/ov.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	defpackage/k83.java
https://firebase.google.com/support/guides/disable-analytics	defpackage/w12.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	defpackage/wq2.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	defpackage/n42.java
http://hostname/?	defpackage/k40.java
https://img1.digitallocker.gov.in/assets/img/banner/	defpackage/jv.java
javascript:(file:///android_asset/errors/connection_lost.html file:///tryagain file:///android_asset/loader.html	defpackage/wv.java
https://emv3ds/challenge	defpackage/y2.java
https://%s/%s/%s	defpackage/n03.java
file:///android_asset/errors/connection_lost_after_login.html	defpackage/ww.java
http://goo.gl/naFqQk	defpackage/g91.java
http://www.google-analytics.com https://ssl.google-analytics.com	defpackage/ya1.java
http://www.slf4j.org/codes.html#StaticLoggerBinder http://www.slf4j.org/codes.html#substituteLogger http://www.slf4j.org/codes.html#unsuccessfulInit http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#version_mismatch	defpackage/uu4.java
https://play.google.com/store/apps/details?id=	defpackage/xy.java
http://owncloud.org/ns	defpackage/n73.java
http://localhost	defpackage/p41.java
http://schemas.android.com/apk/res/android	defpackage/yb.java
https://app-measurement.com/a	defpackage/yx1.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	defpackage/o73.java
file:///android_asset/errors/connection_lost_after_login.html	defpackage/uw.java
http://goo.gl/8Rd3yj	defpackage/k91.java
http://owncloud.org/ns	defpackage/m73.java
file:///android_asset/errors/connection_lost_after_login.html	defpackage/zw.java
file:///android_asset/loader.html	defpackage/nw.java
https://firebase.google.com/support/privacy/init-options.	defpackage/xz2.java

URL	FILE
file:///android_asset/errors/connection_lost_after_login.html	defpackage/vw.java
https://emv3ds/challenge	defpackage/d2.java
https://errors.stripe.com/api/426/store/	defpackage/s.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	defpackage/b40.java
https://plus.google.com/	defpackage/eb0.java
https://play.google.com/store/apps/details?id=	defpackage/bu.java
www.googleapis.com/identitytoolkit/v3/relyingparty	defpackage/m41.java
www.google.com https://www.google.com https://goo.gl/NAOOOI. https://goo.gl/NAOOOI	defpackage/d82.java
https://digilocker.gov.in/public.php?service=files&t=	defpackage/g83.java
http://source.android.com/, http://source.android.com/compatibility) http://www.apache.org/licenses/ https://stripe.com/au-becs-dd-service-agreement/legal https://elibom.digitallocker.gov.in/index.php/apps/dashboard/api/1.0/partnerdashboard http://developers.facebook.com/policy/ https://digilocker-1032.firebaseio.com https://digilocker.gov.in) http://oauth2.authorization.server.org/paht/to/endporint/for/access/token http://oauth2.authorization.server.org/paht/to/endpoint/for/authorization https://play.google.com/store/apps/details?id=com.owncloud.android http://owncloud.com/mobile/help https://owncloud.com/mobile/new https://..	Android String Resource
https://utils.digitallocker.gov.in/api/v1/web/stage/default/digiDyNotification.json https://digilocker.gov.in/index.php https://digilocker.gov.in/public/reset/username https://digilocker.gov.in/public/reset_password?mobile https://digilocker.gov.in/public/reset_password https://digilocker.gov.in/public/reset_password/changepasswordOTP https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar?mobile https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar https://digilocker.gov.in/about_mob.html https://digilocker.gov.in/contact_mob.html https://digilocker.gov.in/faq_mob.html https://digilocker.gov.in/help.html https://digilocker.gov.in/help_signin.php https://digilocker.gov.in/help_signup.php	lib/armeabi-v7a/libnative-lib-DL.so
https://utils.digitallocker.gov.in/api/v1/web/stage/default/digiDyNotification.json https://digilocker.gov.in/index.php https://digilocker.gov.in/public/reset/username https://digilocker.gov.in/public/reset_password?mobile https://digilocker.gov.in/public/reset_password https://digilocker.gov.in/public/reset_password/changepasswordOTP https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar?mobile https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar https://digilocker.gov.in/about_mob.html https://digilocker.gov.in/contact_mob.html https://digilocker.gov.in/faq_mob.html https://digilocker.gov.in/help.html https://digilocker.gov.in/help_signin.php https://digilocker.gov.in/help_signup.php	lib/x86_64/libnative-lib-DL.so

URL	FILE
https://utils.digitallocker.gov.in/api/v1/web/stage/default/digiDyNotification.json https://digilocker.gov.in/index.php https://digilocker.gov.in/public/reset/username https://digilocker.gov.in/public/reset_password?mobile https://digilocker.gov.in/public/reset_password https://digilocker.gov.in/public/reset_password/changepasswordOTP https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar?mobile https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar https://digilocker.gov.in/about_mob.html https://digilocker.gov.in/contact_mob.html https://digilocker.gov.in/faq_mob.html https://digilocker.gov.in/help.html https://digilocker.gov.in/help_signin.php https://digilocker.gov.in/help_signup.php	lib/x86/libnative-lib-DL.so
https://utils.digitallocker.gov.in/api/v1/web/stage/default/digiDyNotification.json https://digilocker.gov.in/index.php https://digilocker.gov.in/public/reset/username https://digilocker.gov.in/public/reset_password?mobile https://digilocker.gov.in/public/reset_password https://digilocker.gov.in/public/reset_password/changepasswordOTP https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar?mobile https://digilocker.gov.in/public/reset_password/reset_pass_aadhaar https://digilocker.gov.in/about_mob.html https://digilocker.gov.in/contact_mob.html https://digilocker.gov.in/faq_mob.html https://digilocker.gov.in/help.html https://digilocker.gov.in/help_signin.php https://digilocker.gov.in/help_signup.php	lib/arm64-v8a/libnative-lib-DL.so

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://digilocker-1032.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@stripe.com	com/stripe/android/networking/StripeRequest.java
support@stripe.com	com/stripe/android/exception/APIConnectionException.java
support@digitallocker.gov	defpackage/ry.java
u0013android@android.com0 u0013android@android.com	defpackage/uc0.java
apps@owncloud.com	Android String Resource

TRACKERS

TRACKER	URL
Google Analytics	https://reports.exodus-privacy.eu.org/trackers/48

TRACKER	URL
Google CrashLytics	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"auth_fail_get_user_name" : "Your server is not returning a correct user id, please contact an administrator"
"auth_password" : "Password"
"auth_username" : "Username"
"esign_not_a_aadhaar_user" : "You are not authrized for eSigning your file. Please Link your aadhaar to digilocker account to avail this facility."
"forget_password" : "Forgot Password"
"forget_user_name" : "Forgot Username"
"google_api_key" : "AIzaSyAB_vvn04v8RgErmcnZ0Ocb4zd09-CrjLY"
"google_crash_reporting_api_key" : "AIzaSyAB_vvn04v8RgErmcnZ0Ocb4zd09-CrjLY"
"oauth2_client_secret" : ""
"refresh_list_key" : "refresh issued doc"
"saiftynet_key" : "AIzaSyDfCV6cgb-w8zAf2u4uRJUoHiTw4u1-vIg"
"saml_subject_token" : ""%1$s" has been shared with you"
"share_link_no_support_share_api" : "Sorry, sharing is not enabled on your server. Please contact your administrator."
"subject_token" : "%1$s shared "%2$s" with you"
"tooltip_password" : "Between 6-30 characters. Only hash(#), exclamation(!), asterisk(*), dollar($) and at the rate(@) are allowed as special characters."
"tooltip_username" : "Between 3-50 characters. Can contain only lowercase letters, numbers and special characters - dot(.), dash(-), underscore(_) and at the rate(@). Username c annot start with a special character."
"username" : "Username"
"auth_password" : "[redacted]"
"auth_username" : "[redacted]"
"username" : "[redacted]"
"auth_password" : "Mật khẩu"
"auth_username" : "Tên người dùng"

PLAYSTORE INFORMATION

Title: DigiLocker - a simple and secure document wallet

Score: 4.061808 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Productivity **Play Store URL:** com.digilocker.android

Developer Details: National eGovernance Division, Government of India, National+eGovernance+Division,+Government+of+India, Digital India Corporation, Government of India, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi - 110003, https://digilocker.gov.in/, support@digitallocker.gov.in,

Release Date: Feb 8, 2016 **Privacy Policy:** Privacy link

Description:

DigiLocker is a key initiative under Digital India, the Government of India's flagship program aimed at transforming India into a digitally empowered society and knowledge economy. Targeted at the idea of paperless governance, DigiLocker is a platform for issuance and verification of documents & certificates in a digital way, thus eliminating the use of physical documents. The DigiLocker website can be accessed at https://digitallocker.gov.in/. You can now access your documents and certificates from your DigiLocker on your mobile devices.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.2.4 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.