MOBSF

ANDROID STATIC ANALYSIS REPORT

LOLC (2.30)

File Name:	LOLC.apk
Package Name:	com.fg.lolc
Scan Date:	Jan. 4, 2025, 11:50 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	16	4	3	3

FILE INFORMATION

File Name: LOLC.apk
Size: 14.06MB
MD5: f3e8af6965f48b43ae7340bf541f0ebd
SHA1: e2629407185c2e8e2b14645eca88a6342d6ef752
SHA256: 2a0ee82a48e0c424b48e9fc2e4780a3be8d6ec2d5d2f98a1b5f84bf021f25441

APP INFORMATION

App Name: LOLC
Package Name: com.fg.lolc
Main Activity: com.fg.lolc.feature.activity.SplashActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.30

Android Version Code: 76

APP COMPONENTS

Activities: 11
Services: 10
Receivers: 5
Providers: 2
Exported Activities: 3
Exported Services: 3
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: L=Colombo, O=FortunaGlobal, CN=LOLC App
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-04-03 13:14:38+00:00
Valid To: 2040-03-27 13:14:38+00:00
Issuer: L=Colombo, O=FortunaGlobal, CN=LOLC App
Serial Number: 0x2194daf6
Hash Algorithm: sha256
md5: 190ee54302eef28acb466860f5cb359c
sha1: 8c576df40b3724560ad461bb171eee0955598819
sha256: 3d7fc94eec632f8d9c85e9282a421d845c6875fc2ea9c2d9b1ff3152d6f0ad2e
sha512: 5442c7785c039b42c33e056e9fea21deca29fc95c69d3632e7821268a9a5e87b8f91d0f9976157144179fb5f73c6a062b09049a8a2cb8828e477346fa96db7ad
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bc13e024a9c736073ed536d0642e03563ef4b54f50b43900d9383364168db4ba
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.fg.lolc.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.fg.lolc.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes3.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.fg.lolc://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	https://lolcfinance.lk	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
2	https://lolcfinance.lk	info	Domain config is configured to trust bundled certs @raw/www_lolcfinance_2023_2024.
3	https://lolcfinance.lk	info	Domain config is configured to trust bundled certs @raw/www_lolcfinance_2024_2025.

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: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	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.
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	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.
4	Activity (com.google.android.gms.appinvite.PreviewActivity) 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.
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	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.

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.
7	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.
11	Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/chauthai/swipereveallayout/ViewBinderHelper.java com/fg/lolc/api/exception/LoginException.java com/fg/lolc/manager/JsonReader.java com/fg/lolc/manager/impl/AppPreferencesManager.java com/fg/lolc/model/common/UserData.java com/fg/lolc/model/request/AccountDetailEditRequest.java com/fg/lolc/model/request/EditBeneficiary

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/fg/lolc/model/request/EditBeneficiaryRequest.java com/fg/lolc/model/request/ExtendSessionTimeRequest.java com/fg/lolc/model/request/FirstTimeLoginRequest.java com/fg/lolc/model/request/ForgotPasswordRequest.java com/fg/lolc/model/request/FundTransferRequest.java com/fg/lolc/model/request/FundTransferRequestNew.java com/fg/lolc/model/request/LoginRequest.java com/fg/lolc/model/request/OtpLimitRequest.java com/fg/lolc/model/request/SavingPlannerSaveRequest.java com/fg/lolc/model/request/SchedulerDeleteRequest.java com/fg/lolc/model/request/SendOtpRequest.java com/fg/lolc/model/request/StandingOrdersFundTransferRequest.java com/fg/lolc/model/request/ThirdPartyFundTransferrequest.java com/fg/lolc/model/request/UpdateSavingPlannerRequest.java com/fg/lolc/model/request/UserLogoutItem.java com/fg/lolc/model/request/UserMessageRequest.java com/fg/lolc/model/request/ValidateOtpRequest.java com/fg/lolc/model/request/otp/OTPRequest.java com/fg/lolc/model/response/BankSchedulerFundTransfer.java com/fg/lolc/model/response/Daum.java com/fg/lolc/model/response/LoginResponse.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/fg/lolc/model/response/SavingPlannerSaveResponse.java com/fg/lolc/model/response/StandingOrdersViewList.java com/fg/lolc/model/response/User.java com/fg/lolc/model/response/UserLogoutResponse.java com/fg/lolc/model/response/UserMessageResponse.java com/fg/seylan/api/exception/ChangePasswordException.java com/fg/seylan/model/request/ChangePasswordRequest.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java
				com/base/app/api/service/ApiRouter.java com/base/app/api/service/BasicLoggerInteceptor.java com/fg/lolc/common/dialog/ProgressDialog.java com/fg/lolc/common/fragment/confirmation/ConfirmationFragment.java com/fg/lolc/common/fragment/success/SuccessFragment.java com/fg/lolc/feature/account/history/items/AccountHistoryItemFragment.java com/fg/lolc/feature/billpayment/payment/PaymentFragment.java com/fg/lolc/feature/fundtransfer/FundTransferFragment.java com/fg/lolc/feature/fundtransfer/scheduler/RegisteredSchedulersFragment.java com/fg/lolc/feature/login/socialmedia/SocialMediaDialog.java com/fg/lolc/feature/logout/LogoutDialog.java com/fg/lolc/feature/savingplaner/deatils/SavingPlannerDetailFragment$setListeners$7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/fg/lolc/feature/savingplaner/deatils/SavingPlannerDetailFragment.java com/fg/lolc/feature/savingplaner/viewall/SavingPlannerViewAllFragment.java com/fg/lolc/feature/savingplaner/viewall/SavingPlannerViewAllViewModel.java com/fg/lolc/feature/settings/accmanagement/AccManagementFragment.java com/fg/lolc/feature/settings/alertcontrol/AlertControlFragmentViewModel.java com/fg/lolc/feature/standingorders/StandingOrdersFragment$setListeners$11.java com/fg/lolc/feature/standingorders/viewall/StandingOrdersViewAllFragment.java com/fg/lolc/helper/common/AppSecurityHelper.java com/fg/lolc/helper/common/LoginChecksumHelper.java com/fg/lolc/helper/view/SessionTimeOutDialogHelper.java com/fg/lolc/util/Utils.java com/fg/tamil/Tamil.java com/github/paolorotolo/appintro/AppIntroBase.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java com/stericson/RootShell/RootShell.java com/stericson/RootShell/containers/RootClass.java com/stericson/RootTools/RootTools.java com/stericson/RootTools/internal/Installer.java com/stericson/RootTools/internal/RootToolsInternalMethods.java com/stericson/RootTools/internal/Runner.java com/wdullaer/materialdatetimepicker/date/DayPickerView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/wdullaer/materialdatetimepicker/time/AmPmCirclesView.java com/wdullaer/materialdatetimepicker/time/CircleView.java com/wdullaer/materialdatetimepicker/time/RadialPickerLayout.java com/wdullaer/materialdatetimepicker/time/RadialSelectorView.java com/wdullaer/materialdatetimepicker/time/RadialTextsView.java com/wdullaer/materialdatetimepicker/time/TimePickerDialog.java dagger/android/AndroidInjection.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/fg/lolc/model/request/LoginRequest.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/fg/lolc/feature/login/login/LoginFragment.java com/fg/lolc/helper/common/AppValidationHelper.java com/scottyab/rootbeer/RootBeer.java com/stericson/RootTools/SanityCheckRootTools.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/stericson/RootTools/internal/RootToolsInternalMethods.java
6	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/Const.java com/stericson/RootTools/internal/RootToolsInternalMethods.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/fg/lolc/api/service/DefaultClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/fg/lolc/helper/data/DataFormatHelper.java com/fg/lolc/helper/data/EncryptedDataFormatHelper.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/fg/lolc/manager/impl/AppPreferencesManager.java
10	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	at/favre/lib/bytes/Bytes.java at/favre/lib/bytes/BytesTransformers.java at/favre/lib/bytes/Util.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/stericson/RootTools/internal/Installer.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/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
2	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
3	arm64-v8a/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
4	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.	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
5	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
6	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
7	arm64-v8a/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
8	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.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/fg/lolc/helper/common/LoginChecksumHelper.java com/stericson/RootShell/execution/Shell.java com/stericson/RootTools/internal/Installer.java okio/Okio__JvmOkioKt.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/fg/lolc/feature/contactus/ContactUsFragment.java com/fg/lolc/feature/login/login/LoginFragment.java com/fg/lolc/feature/login/socialmedia/SocialMediaDialog.java com/stericson/RootTools/internal/RootToolsInternalMethods.java
00022	Open a file from given absolute path of the file	file	com/stericson/RootShell/containers/RootClass.java com/stericson/RootTools/internal/Remounter.java com/stericson/RootTools/internal/RootToolsInternalMethods.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/fg/lolc/feature/contactus/ContactUsFragment.java
00112	Get the date of the calendar event	collection calendar	com/fg/lolc/helper/data/DateFormatHelper.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/fg/lolc/helper/common/DeviceRegistrationHelper.java
00130	Get the current WIFI information	wifi collection	com/fg/lolc/helper/common/DeviceRegistrationHelper.java
00033	Query the IMEI number	collection	com/fg/lolc/helper/common/DeviceRegistrationHelper.java
00082	Get the current WiFi MAC address	collection wifi	com/fg/lolc/helper/common/DeviceRegistrationHelper.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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
www.seylanbank.lk	IP: 203.115.28.121 Country: Sri Lanka Region: Western Province City: Colombo

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
lk.linkedin.com	ok	**IP:** 13.107.246.45 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.tiktok.com	ok	**IP:** 2.21.20.151 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
www.google.com	ok	**IP:** 216.58.211.228 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
paolorotolo.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
www.youtube.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.lolcfinance.lk	ok	**IP:** 45.223.164.133 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.instagram.com	ok	**IP:** 157.240.205.174 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.seylanbank.lk	ok	**IP:** 203.115.28.121 **Country:** Sri Lanka **Region:** Western Province **City:** Colombo **Latitude:** 6.931940 **Longitude:** 79.847778 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
play.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.seylan.lk	ok	**IP:** 3.164.206.97 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

EMAILS

EMAIL	FILE
info@hnbfinance.lk	com/fg/lolc/config/AppConstant.java
this@loginfragment.requirecon this@loginfragment.requireact	com/fg/lolc/feature/login/login/LoginFragment.java
info@lolcfinance.com	com/base/app/config/Constants.java
example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"mdtp_deleted_key" : "%1$s□□□□□□□□"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"
"login_password" : "Password"
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
O3KEK4C8mMJ55X7+rKhyFI2gabDgFgd1qlmX9Na34/M=

POSSIBLE SECRETS
LLWEGIcMoDZoYXR7U5oWQiG0eqgHAi5y99iNxWUoUCrqQe4SBuROX6hcHHgPH+SM
cma5ZMQhKxelkLoCs6AZIf+jHy8LfWoLKTm3I25QQ7y8l7CIShnEfyEmDBtS6X1R
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
o4gCRP8pd3YBLYpyJe+pyrNh2wHBW5ZmIwpxvbEaiEk=
Ncqp5H+22w9W3L8txFxikPL++CvvT4UACmJT2y9HNWRLTaCz/GhnD086ih+pDclQ
123456789012345678901234567890123456
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
85aVi3SJCzURUruw80xwOCJlrH71CKBJVp0z1HeuVQI=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
gvEkKyx3YjkW3LmeffZWM+wAodTj/mcVSvq1iQ03Xm0=
vfxPDbj+Gh4UJloJgP7FDEw0pUJBChFkLoiSG9W3S+I=
cpk+vnXicdAmu6rqNpyRsH8Z9xFtWGhKh1PSt7R1wgo=
cXUR3QZnvsd8QFJrigAEcnhF5qRi6A1WjhzghuHtPIs=
kX7NAbLZCz/dSKM5Fw5tfFEDlfsFCqwNHFXHrnBBf44=

POSSIBLE SECRETS
zYGiKyXCQARtrMz4+R+cwjpghR9+uCtdZ+gYsXH0O9M=
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
PQ5SSaxTSuJzj647muMyUtZ+uYgTQgJ31c5fk186jfk=
dR638FFygwsrTt/QflyOMGvXjf1GSNZ7znIlrDruhqQ=
MmO0rCvC3l83tbAoIwnFF0x6ASHVe9zZRiunMzgf61w=
c6GziBvAtJVQl8145kYNIiXglYZwc9tWD7nqr7hLy/A=
Be4XNeKe48otW84OnyuJ3t3qbzO8QDmRqoj9GLjPbqCKHl4EjzEK31ZhyeIA63g7
gp0cIgUUdAIZbRXtUI5gQGevY7Ql5nC5BzKn6LnObLY=
sha256/BFz5FW3IdUD8XTY9n1WTrukCL54GhFzkoyXwUNK02yA=
fuI1JBLz73BbSdCY+eHqDP1u6baqogxj7PqSFpzZgrAG3XsVxk7kH3pFFSmoNQQw
fmyYtvp6GdfV8aXECqySf5usPZLp4lFIXsdmCOa6f3I=
Yt5XpSAtwgzkLrmXQYrSRr3fMYrlcB9+S6GNMxeM/YPVx9v5CKvi8nPmgPLSujhj
B3EEABB8EE11C2BE770B684D95219ECB
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
8HMIy/Wfi2fsqmlkEx1MOaO07gLN9KPbPeJd9GTSqvM=
AifE6OWHQ8zRmArdaoYy3/wDT3Tse3b0SsXzLMY2JhYTdkCeDJ1ty8MUlcSgr6P8
VN0mjb52HdSTqOivTj5aML5bEfMpu2JdQlvUopb/cybtBLaro7TgCOYdeQg7NyAj
nlNsfD0KfLAOzjZnsadcRaT7rHxwp4GC5EZVTVhnwe/pnADxonobSxOiLY3KGgZG
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
rw94Vrx/byjpqg0QbJ3qk6x9nbH4tHcDnVkhwVzqmY0=
b0nS9elqzY5/VJmQt0NlC62dB7yCaB6LeKUB+YXUuuDDycP369v3LvQySmqqDQ6y
Kl5uWPRlOPd31gHSoBTxQgFz93Wgsh3JQ5+syp0rqA1C1BUyIJ1EfI70uCpXJEXY
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
wflZ5ZrFWxKN35Rs/obkm9xcWW4uwhgDI7R93vb2gpXPjsYJYEKVt9jrMQOUQeAA
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19

POSSIBLE SECRETS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
Jr72ymQHv5OslUBKT3bZCPBk5tCtKWt432zERI2guaDk8CCuhfLPuPGiolFM9O2V
oClLCKzkLLWAqjtGJeQeLZr6xaB9RrnEuNDXspc7PYI=
aPsscg+Qxy0iqv59xAu19ukICD9tJAt4EQOJODpj5Ak49GynbXKvHyrrGvZ8bZTH
dn8+8pHjJ2wj5Gp1r/T7fEkOwzyz7KKq5AugUUrNOwEHnTcvhTP4W3g7fxLqTpFB
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

PLAYSTORE INFORMATION

Title: LOLC Realtime

Score: 2.3333333 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.fg.lolc

Developer Details: LOLC Finance PLC, LOLC+Finance+PLC, None, http://lankaorix.com/, lofin@lankaorix.com,

Release Date: Apr 3, 2015 **Privacy Policy:** Privacy link

Description:

LOLC Realtime, Enjoy Greater Convenience Do your financial transactions on the go with your Android mobile and enjoy a universe of financial facilities at your fingertip. Simply download the App to your Android Mobile and use the User ID and Password already issued to you for LOLC Realtime to do your financial transactions. If you do not have an account please visit http://www.lolcfinance.com/ to register online or visit your nearest LOLC branch and submit your details to create an online account. Inquire balancers, view account history transfer funds to an account with LOLC Finance PLC or any other commercial bank, pay your bills including leasing and gold loan payments manage your funds open other account, FD account creation and other main financial services. Financial modelling, locating our service points and ATM, information on interest rates currency details of our products and our latest promotional and offers, or contact us for any other matter. LOLC Realtime Enjoy Greater Convenience to all your financial needs. Call us on our 24 Hours Customer service Hotline +94115715555 for details on the activation and discover a whole new world of personalized virtual banking services today.

SCAN LOGS

Timestamp	Event	Error
2025-01-04 23:50:48	Generating Hashes	OK
2025-01-04 23:50:49	Extracting APK	OK
2025-01-04 23:50:49	Unzipping	OK
2025-01-04 23:50:49	Parsing APK with androguard	OK
2025-01-04 23:50:50	Extracting APK features using aapt/aapt2	OK
2025-01-04 23:50:51	Getting Hardcoded Certificates/Keystores	OK
2025-01-04 23:50:56	Parsing AndroidManifest.xml	OK
2025-01-04 23:50:56	Extracting Manifest Data	OK
2025-01-04 23:50:56	Manifest Analysis Started	OK

2025-01-04 23:50:56	Reading Network Security config from network_security_config.xml	OK
2025-01-04 23:50:56	Parsing Network Security config	OK
2025-01-04 23:50:56	Performing Static Analysis on: LOLC (com.fg.lolc)	OK
2025-01-04 23:50:56	Fetching Details from Play Store: com.fg.lolc	OK
2025-01-04 23:50:56	Checking for Malware Permissions	OK
2025-01-04 23:50:56	Fetching icon path	OK
2025-01-04 23:50:56	Library Binary Analysis Started	OK
2025-01-04 23:50:56	Analyzing apktool_out/lib/armeabi-v7a/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing apktool_out/lib/x86/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing apktool_out/lib/arm64-v8a/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing apktool_out/lib/x86_64/libtool-checker.so	OK

2025-01-04 23:50:56	Analyzing lib/armeabi-v7a/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing lib/x86/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing lib/arm64-v8a/libtool-checker.so	OK
2025-01-04 23:50:56	Analyzing lib/x86_64/libtool-checker.so	OK
2025-01-04 23:50:56	Reading Code Signing Certificate	OK
2025-01-04 23:50:57	Running APKiD 2.1.5	OK
2025-01-04 23:51:04	Detecting Trackers	OK
2025-01-04 23:51:12	Decompiling APK to Java with JADX	OK
2025-01-04 23:52:26	Converting DEX to Smali	OK
2025-01-04 23:52:26	Code Analysis Started on - java_source	OK

2025-01-04 23:52:32	Android SBOM Analysis Completed	OK
2025-01-04 23:52:47	Android SAST Completed	OK
2025-01-04 23:52:47	Android API Analysis Started	OK
2025-01-04 23:52:52	Android API Analysis Completed	OK
2025-01-04 23:52:53	Android Permission Mapping Started	OK
2025-01-04 23:53:01	Android Permission Mapping Completed	OK
2025-01-04 23:53:02	Android Behaviour Analysis Started	OK
2025-01-04 23:53:06	Android Behaviour Analysis Completed	OK
2025-01-04 23:53:06	Extracting Emails and URLs from Source Code	OK
2025-01-04 23:53:12	Email and URL Extraction Completed	OK

2025-01-04 23:53:12	Extracting String data from APK	OK
2025-01-04 23:53:13	Extracting String data from SO	OK
2025-01-04 23:53:13	Extracting String data from Code	OK
2025-01-04 23:53:13	Extracting String values and entropies from Code	OK
2025-01-04 23:53:26	Performing Malware check on extracted domains	OK
2025-01-04 23:53:27	Saving to Database	OK

Report Generated by - MobSF v4.2.9

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.