ANDROID STATIC ANALYSIS REPORT

CSEAN

CYBER SECURITY EXPERTS
ASSOCIATION OF NIGERIA

Csean (1.0.0)

File Name:	app-release.apk
Package Name:	com.example.csean_mobile
Scan Date:	April 4, 2023, 6:26 a.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	1	2	1

FILE INFORMATION

File Name: app-release.apk
Size: 25.96MB
MD5: be450f98eeb466ebc757667fa7998be3
SHA1: fc4c38ccd8fdfd26400d95040c7d8ef04e0a66d1
SHA256: 5ac4b07a2664ac545eb6f6b61d5fdfb12db0c09dea788445aa1961091a088318

APP INFORMATION

App Name: Csean
Package Name: com.example.csean_mobile
Main Activity: com.example.csean_mobile.MainActivity
Target SDK: 30
Min SDK: 26
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 8
Services: 0
Receivers: 1
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=NG, ST=Lagos, L=Nigeria, O=infoscert, OU=csean, CN=csean
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-03-22 16:15:39+00:00
Valid To: 2050-08-07 16:15:39+00:00
Issuer: C=NG, ST=Lagos, L=Nigeria, O=infoscert, OU=csean, CN=csean
Serial Number: 0x7dbdfa4c
Hash Algorithm: sha256
md5: 5c077b56704cb106131757692ca4282d
sha1: 7f674f0ef8f8a37e38b6e57be624ab0e023bd0f7
sha256: c7eb0a2bbdf3e99bbc358b605c7479cc6b7fc36fc43cc26ddcd837d57bc6bc7b
sha512: 8e0171bbd9799634e0526826644ce35c09f13a2214a21a62da5a87ab7f29c6e6953c5600175f6d6c61ae50c76d5652baa1efdb7dfb018d0b77ca1800b680e18e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9c4302fb6e13d32b70a0c7c4f549ff5e03d01fd535a26a708beb62b1373cd8b1

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.example.csean_mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	a0/c.java b4/b.java com/mr/flutter/plugin/filepicker/c.java com/pichillilorenzo/flutter_inappwebview/Util.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InputAwareWebView.java io/flutter/plugins/imagepicker/a.java io/flutter/plugins/imagepicker/f.java io/flutter/plugins/webviewflutter/c.java io/flutter/plugins/webviewflutter/x1.java k3/d.java l3/b.java m0/a.java n0/e0.java s0/a.java s0/b.java t0/a.java t0/n.java t0/o.java t0/p.java u2/r.java u4/h.java v3/d0.java w4/a.java w4/b.java w4/c.java x/c.java y2/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	c2/b.java com/mr/flutter/plugin/filepicker/c.java l5/a.java l5/b.java m5/a.java y0/p1.java z1/o0.java
3	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/mr/flutter/plugin/filepicker/c.java u4/g.java u4/h.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/pichillilorenzo/flutter_inappwebview/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview/types/URLCredential.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a4/a.java
6	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	e2/a.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	y5/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/pichillilorenzo/flutter_inappwebview/credential_database/CredentialDatabaseHelper.java
9	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	co/paystack/flutterpaystack/AuthActivity.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libapp.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_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.
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
13	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
fonts.gstatic.com	ok	**IP:** 142.250.74.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ibm.com	ok	**IP:** 184.51.232.157 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
standard.paystack.co	ok	**IP:** 104.17.191.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
developer.apple.com	ok	**IP:** 17.253.39.201 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
i3.ytimg.com	ok	**IP:** 142.250.74.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
members.csean.org.ng	ok	**IP:** 104.21.49.94 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.paystack.co	ok	**IP:** 104.17.191.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
_supportfilemodel@335101832.fromjson _httpparser@13463476.responsepa _itemfile@331278803.fromjson _certificatemodel@343393679.fromjson _messagefile@321478361.fromjson _transactiondatafile@338097540.fromjson _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal _useraccountmodel@343393679.fromjson _link@14069316.fromrawpat _growablelist@0150898.withcapaci	

EMAIL	FILE
_growablelist@0150898._literal6	
subcategoryitemmodel@332337951.fromjson	
_blogfile@308328490.fromjson	
_receiveportimpl@1026248.fromrawrec	
_compressednode@746137193.single	
_colorfilter@15065589.mode	
_blogdatafile@307061076.fromjson	
_list@0150898._ofarray	
_timer@1026248.periodic	
_growablelist@0150898._literal2	
_bigintimpl@0150898.from	
_list@0150898.empty	
_itemdatafile@330411679.fromjson	
_subscriptionmodel@343393679.fromjson	
_directory@14069316.fromrawpat	
_paymentfile@323010841.fromjson	
_casterror@0150898._create	
_invocationmirror@0150898._withtype	
_forumfile@314427106.fromjson	
_chaptermodel@343393679.fromjson	
_rawsocket@14069316._writepipe	
_hashcollisionnode@746137193.fromcollis	
_categorymodel@309339553.fromjson	
_eventdatafile@310222375.fromjson	
_progressfile@325412391.fromjson	
_colorfilter@15065589.lineartosr	
_useraccountfile@342152561.fromjson	
progressrequestmodel@326454137.fromjson	
transactionfilemodel@340416292.fromjson	
_growablelist@0150898._literal1	
_uri@0150898.file	
_imagefilter@15065589.blur	
_sendermodel@322019563.fromjson	
_growablelist@0150898._literal4	
egisteredeventsmodel@329221958.fromjson	
_topicfile@336505675.fromjson	
_growablelist@0150898._ofgrowabl	
_growablelist@0150898.of	
_creatormodel@337357068.fromjson	
progresstrackermodel@326454137.fromjson	
nativesocket@14069316.pipe	

EMAIL	FILE
_cookie@13463476.fromsetcoo _supportfile@334266247.fromjson authenticationscheme@13463476.fromstring _list@0150898.of portparticipantmodel@335101832.fromjson _list@0150898.generate _profilemodel@343393679.fromjson steredeventsdatafile@327507047.fromjson _typeerror@0150898._create storationinformation@1137124995.fromserial _transactionfile@339445779.fromjson _list@0150898._ofgrowabl _paymentfilemodel@324362441.fromjson _inboxfile@317242154.fromjson _list@0150898._ofefficie _subcategorymodel@320227622.fromjson _growablelist@0150898._ofarray _growablelist@0150898._literal3 e@gmail.com _supportrepliesmodel@335101832.fromjson _growablelist@0150898._ofother _future@4048458.value _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe _messagefilemodel@322019563.fromjson _progressreportmodel@326454137.fromjson _list@0150898._ofother _bytebuffer@7027147._new _useraccountdatafile@341206965.fromjson ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _supportdatafile@333022651.fromjson _nativesocket@14069316.normal registeredeventsfile@328137207.fromjson _filestream@14069316.forstdin _colorfilter@15065589.srgbtoline _refereemodel@343393679.fromjson _uri@0150898.directory _authormodel@309339553.fromjson	lib/armeabi-v7a/libapp.so

EMAIL	FILE
rogressactivitymodel@326454137.fromjson _growablelist@0150898._literal8 _file@14069316.fromrawpat _eventfile@311501976.fromjson _categoryfile@319501040.fromjson _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _blogfilemodel@309339553.fromjson _future@4048458.zonevalue _growablelist@0150898._ofefficie _forumdatafile@313110784.fromjson earningcategorymodel@320227622.fromjson _future@4048458.immediatee	

Report Generated by - MobSF v3.6.4 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.