



## ANDROID STATIC ANALYSIS REPORT



 YsxLite (1.45)

File Name: yxslite.apk

Package Name: com.yxslite.cam

Scan Date: Oct. 28, 2024, 4:11 p.m.






App Security Score: 36/100 (HIGH RISK)

Grade:



Trackers Detection: 10/432

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
6	16	1	0	3

## FILE INFORMATION

**File Name:** ysxlite.apk

**Size:** 54.96MB

**MD5:** 434c3cd6a91b24380657e7852d5ea950

**SHA1:** b4ace169a5616dd9e381f86089f69543262b9dec

**SHA256:** 149b9467c8c28879a42c99fab9cc660ea54fb34da9cd314bda4e1de69b060be

## APP INFORMATION

**App Name:** YsxLite

**Package Name:** com.ysxlite.cam

**Main Activity:** com.ysxlite.cam.LauncherAty

**Target SDK:** 34

**Min SDK:** 21

**Max SDK:**

**Android Version Name:** 1.45

Android Version Code: 45

## APP COMPONENTS

Activities: 84

Services: 9

Receivers: 10

Providers: 9

Exported Activities: 2

Exported Services: 3

Exported Receivers: 2

Exported Providers: 0

## CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2023-09-13 05:54:36+00:00

Valid To: 2053-09-13 05:54:36+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xdc686c47c1f7146a14cf19ad199b62016f10e382

Hash Algorithm: sha256

md5: dc663c0f5bb4f26d367518a74bdd0448

sha1: 4bad58e28f5cd1049d54502d80aad83b26d09cc3

sha256: 5ab3740bdc2c7d7b8bcd6bcef350b6fe0d3130e081d3dff8413d2c04c47eb32d

sha512: 97ad9ec8e37abdf45ece1feaa5f3497b0f8ec673527108a87a3c6bb5b89e98acbe0692bcd3aa9c96e191d0622049c4ccdd0ee11e8491954ff23a11188cc2b618

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 0d818abb088a6eadd59b3a46b1718fd809b4b5384ba59278985c0b08d1138b65

Found 1 unique certificates

## ☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
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.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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
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.
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.



PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_AD SERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_AD SERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	unknown	Unknown permission	Unknown permission from android reference
com.yoxlite.cam.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
assets/audience_network.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check possible VM check
	Compiler	r8

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes4.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes5.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

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

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

## MANIFEST ANALYSIS

HIGH: 2 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Service (com.ilnk.IlnkService) 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.
5	Service (com.ilnk.utils.killSelfService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [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.
6	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]	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
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.
9	Activity (com.amazon.aps.ads.activity.ApsInterstitialActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.amazon.device.ads.DTBInterstitialActivity) 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.

## </> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/apm/insight/h/a.java com/applovin/exoplayer2/l/q.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/util/ContentLengthInputStream.java com/bykv/vk/opencv/component/video/api/f/c.java com/bykv/vk/opencv/preload/falconx/a/a.java com/bytedance/sdk/component/a/i.java com/bytedance/sdk/component/embeddapplog/PangleEncryptUtils.java com/bytedance/sdk/component/f/d/f.java com/bytedance/sdk/component/utis/HomeWatcherReceiver.java com/ilnk/utis/InkCmdEnc.java com/ilnk/utis/StringUtils.java com/ironsource/environment/c.java com/lzy/okgo/utis/OkLogger.java com/mbridge/msdk/dycreator/a/a.java com/mbridge/msdk/dycreator/e/g.java com/mbridge/msdk/e/a/v.java com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java com/mbridge/msdk/widget/FeedbackRadioGroup.java com/nicky/framework/utis/SIMCardMgr.java com/nicky/framework/utis/StringUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/zxing/common/PlatformSupport



NO	ISSUE	SEVERITY	STANDARDS	FILES
				Manager.java sg/bigo/ads/common/view/AutoNextLi nelinearLayout.java
2	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/applovin/exoplayer2/h/z.java com/ilnk/utlis/StringUtils.java com/mbridge/msdk/playercommon/ex oplayer2/source/ShuffleOrder.java com/nicky/framework/utlis/StringUtils.j ava sg/bigo/ads/common/utlis/k.java
3	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amazon/aps/ads/ApsConstants.jav a com/ilnk/bean/DevUserBean.java com/ilnk/bean/PushBean.java com/ilnk/constants/PushConfig.java com/ironsource/mediationsdk/adqualit y/AdQualityBridgeKt.java com/ironsource/mediationsdk/utlis/Iro nSourceConstants.java com/mbridge/msdk/foundation/downl oad/core/DownloadCommon.java com/vungle/ads/internal/Constants.jav a com/vungle/ads/internal/model/Cookie .java com/vungle/ads/internal/task/CleanupJ obKt.java com/ysxlite/cam/constants/PushConfig .java com/zxing/decode/Intents.java
4	<a href="#">Debug configuration enabled. Production builds must not be debuggable.</a>	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/bumptechnology/glide/BuildConfig.java com/bumptechnology/glide/gifdecoder/Build Config.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/bykv/vk/opencv/component/video/api/f/b.java com/bytedance/sdk/component/d/c/c/c.java com/bytedance/sdk/component/utis/e.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/applovin/mediation/adapters/amazonadmarketplace/BuildConfig.java com/applovin/mediation/adapters/bytedance/BuildConfig.java com/applovin/mediation/adapters/google/BuildConfig.java com/applovin/mediation/adapters/googleadmanager/BuildConfig.java com/applovin/mediation/adapters/ironsource/BuildConfig.java com/applovin/mediation/adapters/minintegral/BuildConfig.java com/bytedance/sdk/openadsdk/BuildConfig.java com/ilnk/bean/WifiSettingBean.java com/ilnk/constants/IlnkConstant.java com/jirbo/adcolony/BuildConfig.java com/vungle/mediation/BuildConfig.java
7	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/adcolony/sdk/d1.java com/applovin/impl/sdk/utis/StringUtils.java
8	<a href="#">The file or SharedPreferences is World Writable. Any App can write to the file</a>	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ironsource/environment/IronSourceSharedPreferencesUtilities.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	<a href="#">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.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/bykv/vk/opencv/component/video/a/b/b/d.java

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.VIBRATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	8/45	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, com.google.android.gms.permission.AD_ID

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.ysxlite.com	IP: 43.138.210.73 Country: China Region: Beijing City: Beijing
active.clewm.net	IP: 121.41.108.72 Country: China Region: Zhejiang City: Hangzhou

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	IP: 93.184.215.14 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
outcome-ssp.supersonicads.com	ok	<b>IP:</b> 18.173.205.28 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
www.ysxlite.com	ok	<b>IP:</b> 43.138.210.73 <b>Country:</b> China <b>Region:</b> Beijing <b>City:</b> Beijing <b>Latitude:</b> 39.907501 <b>Longitude:</b> 116.397232 <b>View:</b> <a href="#">Google Map</a>
github.com	ok	<b>IP:</b> 140.82.121.4 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
www.pangleglobal.com	ok	<b>IP:</b> 2.16.1.147 <b>Country:</b> Netherlands <b>Region:</b> Noord-Holland <b>City:</b> Amsterdam <b>Latitude:</b> 52.374031 <b>Longitude:</b> 4.889690 <b>View:</b> <a href="#">Google Map</a>
outcome-crash-report.supersonicads.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
adc-ad-assets.adtilt.com	ok	<b>IP:</b> 192.229.202.78 <b>Country:</b> United States of America <b>Region:</b> New Jersey <b>City:</b> Newark <b>Latitude:</b> 40.735661 <b>Longitude:</b> -74.172371 <b>View:</b> <a href="#">Google Map</a>
ssdk-sg.pangle.io	ok	<b>IP:</b> 212.77.167.240 <b>Country:</b> Germany <b>Region:</b> Bayern <b>City:</b> Regensburg <b>Latitude:</b> 49.014999 <b>Longitude:</b> 12.095560 <b>View:</b> <a href="#">Google Map</a>
outcome-arm-ext-med-ext.sonic-us.supersonicads.com	ok	No Geolocation information available.
ssdk-vd.pangle.io	ok	<b>IP:</b> 212.77.167.235 <b>Country:</b> Germany <b>Region:</b> Bayern <b>City:</b> Regensburg <b>Latitude:</b> 49.014999 <b>Longitude:</b> 12.095560 <b>View:</b> <a href="#">Google Map</a>
adc3-launch.adcolony.com	ok	<b>IP:</b> 34.36.45.50 <b>Country:</b> United States of America <b>Region:</b> Texas <b>City:</b> Houston <b>Latitude:</b> 29.941401 <b>Longitude:</b> -95.344498 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
lf3-cdn-tos.bytegoofy.com	ok	<b>IP:</b> 47.246.46.225 <b>Country:</b> Italy <b>Region:</b> Lombardia <b>City:</b> Milan <b>Latitude:</b> 45.464272 <b>Longitude:</b> 9.189510 <b>View:</b> <a href="#">Google Map</a>
active.clewm.net	ok	<b>IP:</b> 121.41.108.72 <b>Country:</b> China <b>Region:</b> Zhejiang <b>City:</b> Hangzhou <b>Latitude:</b> 30.293650 <b>Longitude:</b> 120.161423 <b>View:</b> <a href="#">Google Map</a>
p1.i-lnk.com	ok	<b>IP:</b> 174.129.34.188 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>

## TRACKERS

TRACKER	CATEGORIES	URL
AdColony	Advertisement	<a href="https://reports.exodus-privacy.eu.org/trackers/90">https://reports.exodus-privacy.eu.org/trackers/90</a>

TRACKER	CATEGORIES	URL
Amazon Advertisement		<a href="https://reports.exodus-privacy.eu.org/trackers/92">https://reports.exodus-privacy.eu.org/trackers/92</a>
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/72">https://reports.exodus-privacy.eu.org/trackers/72</a>
Facebook Ads	Advertisement	<a href="https://reports.exodus-privacy.eu.org/trackers/65">https://reports.exodus-privacy.eu.org/trackers/65</a>
Google AdMob	Advertisement	<a href="https://reports.exodus-privacy.eu.org/trackers/312">https://reports.exodus-privacy.eu.org/trackers/312</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>
IAB Open Measurement	Advertisement, Identification	<a href="https://reports.exodus-privacy.eu.org/trackers/328">https://reports.exodus-privacy.eu.org/trackers/328</a>
Mintegral	Advertisement, Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/200">https://reports.exodus-privacy.eu.org/trackers/200</a>
Pangle	Advertisement	<a href="https://reports.exodus-privacy.eu.org/trackers/363">https://reports.exodus-privacy.eu.org/trackers/363</a>
ironSource	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/146">https://reports.exodus-privacy.eu.org/trackers/146</a>

## HARDCODED SECRETS

POSSIBLE SECRETS
"dev_sleep_key" : "KeyDown"
"dev_wakeup_key" : "KeyDown"
"dyStrategy.privateAddress" : "privateAddress"



POSSIBLE SECRETS
"pppp_status_user_authenticated" : "Logged-in"
"pppp_status_user_authenticating" : "Authenticating"
"session_conn_p2p" : "P2P"
"session_conn_rly" : "Relay"
"str_password" : "Password"
"str_session" : "Session"
VXUYBRMamhge5PldHXwCUhQsvqUwyGaK
Q7EHaqXEYxiQEoilyqjopxzkHRhZVKtw
1PTlaN9o47ZvO5QWBq3tjVop340dHI6h
vVWBcEJQjEsfNalmzVe1r7miASaPIW1B
JnlGisJqZLjO7zfwdKKMw91nRUtlhmzE
oaymDZ7pAEcbNFhv7Y0pKv8En2RbSAw
exdb2ky9NstGP6elq11NgBzvOAGjRaxw
BXJhCJIGpStjQsMIN6w6cfyx8EdHGsbw
I8KF2ZVrYmk9QbzsZWIXvJRb7XPAUheH

POSSIBLE SECRETS
N6xF9rR52YV8YEOBA61RWKACjwLFpOaI
GOJ9oRRABJfcwjAA770tm42MgykpIS5Q
Mb83VhRFw0YfLpvsGxQ6UEzyZMUp7
9II84e7XMJCEHu7uA5OKUKZwzRXjipC4
wCPzQVRdLc9fuoZbbzdyTQMs65DUcW8k
FjwhSbR0Dqb1wEjXVBdpfUEyE2PwmXT5
1kYj9up9VehuFRcMC7DoHBWV3d6qFcAR
Un7ie3hNu6oSxsviCElGpaw70qJ7D3pr
6y0uOkezMm2TBG2XREAais4zy5M1tLxd
FDV889hBrMc5nJiB7wS69W2fLt8zA89o
v4tKPq3EceuOa5aRsmEiNo1tTprRM6C7
aad37172d5cdd94b403337275d1087b9619df33290
oK8ltqR6UoxvIOFM7x85SOaiyNHULhPY
iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAMAAAC6V+0/AAAAIVBMVEUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABt0UjBAAAAACnRSTIMAEExQVLL3Q0dLTtQgh4QAAAERJREFUeAFjIAWwsDLDKARg5ejkhlFwwMwB5MIoOGCCcJnQRNkhouxkizKyAblQCq8gphimkZhimI7H6U3MAMEMOplBAOSWA4VYaeadAAAAAEIFTkSuQmCC
yf08nX9dIZfcKypKRId4zDkH94BCZAU7

POSSIBLE SECRETS
------------------

PRV2czZbjjW7Ot8uajuxnRGNdIXO90ph
jpK43NGJIXCIE5ie7D0g7Fa1Rpa7kANX
WM0zVtm2JGvaa9vSTXp0h2YRnQYxQrEK
U1b0Njqb3LWazyJmLiNcKHMDagE8OpYs
Whp7rDnlG0MZliYb9hz51Us4d
les1EbCUxP4xgOdfeUltBKAu87PDHxqp
poMRnmB7rAFaE3bMUxI6O2dxmVQ0Moe
p5EAmOIUOepdn0ld4WtjwBc6P8vGfuC
W9Yqfcw4l1PfnAsasbj5MfnOF9oeiem1
stwUo5SqMIMCevvnzS9Ivu5YLcfkOLDd
f5IIXAtAKiBQqbeB00DIw30sTyOB6Nip
iVBORw0KGgoAAAAANSUhEUgAAABAAAAAQCAAAAAf8/9hAAAAAXNSR0IArs4c6QAAAHJRjYBjygBmHD0SA4puhchdxqMEpLayUAWn6BsSWOFXhkEDW7lxDDU5hkOYLQAyymWjNjFDjmiD0bSCWB+lrQPwBiPGBx0DJeCD+B9JINUcWF9BtpygQYYyhG0lwGrGFwVugSU5AfBylVWGmDmMaANyNFVTvpxwAAAAAEIFTkSuQmCC
L0nZjQMyNlt0WICmUM7oX7gpc1IDkDOo
Pl2vgN3HXqbbKxjZzIk4bg0eix12xhJu

POSSIBLE SECRETS
GuFhMY1Ngi3Kc2EktfHyZFCwamvVcTYP
n5EonvV2d0ynVphuWlfrU3PhJk0DBM6W
jWjWqJl6vm3EcSkucHo8Z2hc4QqQU5eN
kj80Vw1lOC47iRluFhEDeBzKcKjW1m8D
4d1rNabt9wBbosjplZDA5yWTcQ5bg7DE
o4JUIxa2QWu1MieYLvsMRT696KEqR
AQLjxK2FjjRwwoaJlN65VrZWNOsgzmXU
FcsNCE2HBjuao8xA2rTijTUxq38jGWif
a1b7a7ea69985aec39f305fb8b08309a0686940e
i1sqGOju2LE8Q92QQNgFTaNu0rUo1z4f
kQTCJlS50BSCbahTVqCDmy8LW1L9RVvG
vKITx3IWvQKkFLmjQGxCBjXBbaEzbyA1
IY1PhTJan2YjTy3m27KNizUeB7qtWqJm
r4XHqvELKUQNiUGngs8vqNM0Mk3b9MGe
qn8tosrMnBeOYh3nA69X7hpHPvfrKSD7

POSSIBLE SECRETS
BjImtcQqBka41jhChDLZKaESgBphWA9m
b7ab2f95043a05f760c84680
pTWsWF2qz8Xr2QvNaoeX4WQy7B5K1AFD
WI5YCVlpnY9sS2vUV4hGrIGwgmlaf2lo
QXuoBnzEZEqlDLe5TpAidegf9xy2rjp2
dru3glT9ekJ0g4QSSusKvICyYzfTBGaa
2VeddHnoq1PdFvEHeliEgk846BkmCK6O
zA4klKNJM0QxWDxEFTSTi5yKhMV68
EvQoHUIErOdPjfZNSaWf5ex2DDXDJXA1
hGyVADXG58acDgE3vJjwpiBKlvJlQGRP
eivXn7WqkaVyj2amCalRVsu1nM81zzOL
AjQwhKg0BmylW2zY2qnRPlrsdpwDD7xX
UwkWzl2MRtUAPiPmZ2pCt01Egbad
fQADRcl3z4I9sbyUvoxt9O6e4jXdGtKI
2B7qWnr6lboK1kzNzncdoP0B0brMv5Si

POSSIBLE SECRETS
xnB3F8eRzgUElZjXVWbAPI1tu19rGp71
Jjxe8gs2e3QRovgCjLhIxlujBEulNGa6
Kv65PDKGzQbP8opzJD3T0Bs4qFkMuEvW
bCA0WV7g9cnA4ltB5qqjp12FxZMghyDz
2QVULSr2cnp6GdJqIDXRW8b5XXXh3hMX
5xFyhJyAmXwpndJ9EoKqTFqqLI0O0t2g
WzMdgVuSy86surt8IbRNO89xVpYcFvZR
mmPym4lpWgK7OAi14ovsdO61E0NwpnnM
ndgFEZBTUbwthgxyC0k1ffQbXbGUnRaA
Fa9eXDyly4elyWfec912IKE0nqoR5HqV
UwpbEbRNI9IMKeij6uSiSZky6ATbVFhh
MZbjV39kBt4hAqLFGwVFLXITEV84r4gZ
rYxOc7Ypr1bQ7KOGmw9sN058kIB7gerB
BNF7ZQJYQPI9GTH2pfcSvMp6af8oi
kIaQKGqX2ZTqEjvfjkZOI1WwOBoH9uFY

POSSIBLE SECRETS
LRipwKypnEKMqg6PamR7G8YuQckBwe
a6e46478453c9aeaca5af624
XKBE22ujheelcTYagdBtfv4d5l35c1GL
B3EEABB8EE11C2BE770B684D95219ECB
zxcvbnmlkjhgfsaqrtwyuiopQWERTYUIOPASDFGHJKLZXCVBNM1234567890
dTodKdBY68fO6HNBSU3LN7qZJ4nOCEpk
9e896LaDKrRwUGEGxpikTCFLA2EDc0Ve
9jmWu3moBjPGR65ZxocrWcXRtVvlqMhB
Llt45BVzQE0ISVvxtilRjadurhGFSSrG
iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAAXNSR0IArs4c6QAAAMRjREFUWAljYBgFoyEw0kOAmYwAcAbqmQbEQkB8igz9FGnxB+r+BcT/gfgPEAsAMd0AsuUGB5yhm81Ai9AtvwUuk6KXAwaV5TcH0ufD03JGLAkjFOdrJgFKvcWSC8A4i9QPrnUX6DGHUB8Gp8BHEDJD0AMyma0wF+B5qKUHUxAgQEFsGCGOeIHkBEPxLSMAIAIEwToeZ+uOQDmulFHDOqQoGtlhCsk6FodY3ME3RskMEeAmmTbgTgXjJBKj4bAaAhQEglA28ZhUJU6FRwAAAAASUVORK5CYII=
iVBORw0KGgoAAAANSUhEUgAAAAwAAAAMCAQAAAD8fjRsAAAAVkiEQVR4AWMgBNgYjK8A8KJQBYK6GJ4zBDNEA0kO1EIPglFQsCK4TWqxBcGczBtDmQhAUuGBCRoChPmZPjF8B8JfoM5QADIQYUC5EowM1xGET6HNygAklo2DuA7sTMAAAAASUVORK5CYII=
1P4e8Svw6pgZkfS1AU7Ku11MIWhAZ0aY
KlezWCwDulS1StSn2NonTUsqgHFd0zlY
7iAt0ZQxlGPQ5tCLEuhHxDXKOxsROBn5

POSSIBLE SECRETS
A9eN1weHgCPL1SkQ3ZXjYtrHuOy08x6Y
xbTSMp8fvBEENljiQe5QRmpFAIAe0spq
sp7WuMlrQg67lklbNPhafgU9zVWwTylU
5zJBssfwfWeqrXRnFZsUzQPBIx8wM7U1
JEnYl3ig6b1G3QZnd7pVPdvwWtuLiuax
GcMaFESaYtqWHDueobHkP3OuSFimx
uaXBHv2Fpyp6t9CjlnldC1lJtF0IP5s0
8DkF2pCK7gEKj1aPHzeGQpXB8g2QomLh
xZfMamQuDxA6bTypucZ197RYNE4mvlcN
KEGdoxZZnAdDUnYCV96i9ePmYlw0nVcs
dsOpW9WfLYjghusiq4Ru5jQxxgYMnVUV
i2lfi3jYyaWanuhNA9EoVixSZwQkBGPJ
KhrHqa8env5LHobs7dTfjp4HGZPf1i5f
DP3a2sR6Ao5znMBkyRuDzqvSCPyaW43t
6rGRVoRQr925zwi8UOEHhi5JTPDCThCe



POSSIBLE SECRETS
DvSn6PhmC3i7LdpG0vBUuRZmjagS5as7
SocWgKvTrb27mU7I6HYZWtCOqe8vN7We
ErY0P3cLXtwrTQQ8AaevOJsLoOljf8Vw
ac6c0eb7d1dfb73d9e5cd82f
tZylzHWr5GKf5F95sWHTJWAqY8lomPh4
iVBORw0KGgoAAAAANSUhEUgAAABIAAAASCAQAAAD8x0bcAAAglEQVR4Ac3KtYECYRgA0UnxAqAALMI72fSrYf8M74jjKGZDOI3I4g36dDFAYXiQKkJH6ygDxMK/WFhoLhgYPGmwM5bhgAMvW1Hjo6FIqSw0MI5YiGEBIsnOWvuTAnNeLIg44QUdCJhi4IVkMmWiGCVJL89aaWTRqTPH9+C3vRpygZ9roDjp6hXFQAAAABJRU5ErkJggg==
5OO1eWJNP7Y3s5cQVhBQzuf4m1TAFPYu
7XnL499jY0auPeNFsvc8kwtFVWOKtFwM
7IyHNSQ2TJBMgpMVEgH3C5YFRcP1ce7U
bPkhSE8L0qTQU8qqVG5cBeS4akAeFCpX
dejWMVKCcsRHbrwAIECa6aRABNrvRLL1
QDtKUfo4Pv7jZ7qumv108KMzWf6HrSMn
XWwbNIOGXItiEE2sGKxxfB9q5IH48KSv
DtHbWGOE2Bmy5zeMr4BSgc5m3XVlvhqE
3kaHypjVzQjnFbgNDhrnWnyYOdOCg92b

POSSIBLE SECRETS
Xxl4rLnj16XDfkQUiM3437m5W6qonc5R
59L0PM8TZSDfga3AwgwmMzwLrxdyp45T
eS8IZAPFQFjEXoH0I8GlgHTr6fGbdCZa
1iDxwsFxF9YiCc2SPrS2klGyrj8KvyqU
tuFyi1rHy9z46G0g3HP9j8Pe4Wglo7s9
1AEGGiZtK9izNwxj0gdNwiRX4yxGSLbl
lPif8zo0BCGymIa9nsJJXRn9Vdfcrwfz
1RYqQKBI4tHo2l91LjIKc5yEyLaxvrL0
aVnA9Ux0owpYjW5hlcDkLBIQBKS6Kuco
AkiufmiMzZjvhyS77AiglOXb5e3YRP2V
ccCRkU4tjU1cPhlyS12s2rOBaxNg0sA2
Xt2DRLIKFdB95NslNvyqeyDnMxOOuDLx
p5lIOLlp1B1ZcinDN0X6ynPo7iUU6KYH
xulkP76phNp8oPrFkycOZ9oAWaaFvsfs
5HWyWxmgcaxBLo1LpD3PpaOljtbRMHJC

POSSIBLE SECRETS
LLxQm2Zb2cHXH3GFymsIhrLJVNNE7YVf
k9IbPcfog7a2vud71ZD1yiSptuKC
qcYJgrhXwk3F7gc49b8OJRulLZ0tc
fXviZ9AMoZT5h2KBZwjsITMVylobOTux
PumDfveAcRoz4mAMU1oiRh2I021HXL7u
qXEMgnv7Ct425I7In8PWxhOPFYVbEYpB
mcSvbra1TWIoRdhWTF80td7BovB7Z6D
u0FGaDlimXxXG0I3UqPLAtx16Sc8Y059
u680PltdmSCtrwUArgQMKOt5dGhFKyFy
XAoGi5mGaFQZFqWDdkVsCV3Av2NgJGYo
pR9Fkr1wWPG0d9ySETcIXHMYi8wcMIk0
9G2r59BoUI91An7yhO6AwIMh4F2sXT3r
Sw9TLHolawUN9KVNZQE03EMAiDKtc0hD
s90Sw2xfipZOULUf4YVvkqTv1ri2JEFZ
I5FSM6v9D3qkRXnarws6dVsmQqtQoJdF

POSSIBLE SECRETS
MDpcepjwzWMs517m4lh6aUQSJk
DwqRJ6bMYzXyiD2Eugn3dkRE0I23BFLv
EyZhmJMsuDDThnYHJcpUVdPGrs5jP
9PVJQ3IXsUcABNIhPZfYMIRDAFEvqeV3
eeDLrDiwzyZn1GaqUg9DZO06uYqn8isf
9xnRWvfnvAuFWSokCiPir6t5eweLHrnN
2vimyyNbMv6AohadWhJSDQSQPpWOARjH
8HaEwRmcLljD6jWZTmAaPx2QrUAiOCOo
18JvwLOKolmi3RAulpcsWcjyGiEhXJWG
W4gBMubxKiZM5LLivtLPs396PBqN8ReM
Y6chWCHiEHN0DdaKB8VVwwMQijKJ1yIC
YNAb6cApL15ElRgBdl6o6I27RW0RMDqg
THEbbJWzjj3eFDIXZnSzsYrmSmbq8w3u
UFa447OZZwRnjgAwYt6DCIQRKKYck
GEphX9PDUn8ir5euMldeMTZrm9gVIFzw



[illegible]

POSSIBLE SECRETS





POSSIBLE SECRETS
rwtSlkdLuH5KaJR0oY6wYi8G8Rc4X5Yb
BEVDZxUetTHXZyMQk8onv0fPj1ZBZ1Qa
uPGJEhgdW6Zw1Sj0ISecSmwhOYLW8VRR
8GKiNnUVprw3BQA7RRGITYk7sqsrZd2
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3
UISLjJpxihM79aLvihwYrwdsqCfo0Nro
ZnYv6Dz0eliuCYzsHLE25vrPVm9Ysg64
vBmFH1fuq9MEDYSajFcKFjMjxIndPyIT
JMyIsM6N3mQ5xBBSQqoIEfTakpln9APf
E7RgkNcVOxUPIMLAnYmg2qDI6nJpawyt
9oUH6lggskzj9KRnNq9fhlyXZqfLC7qm
dGfRjiYjSjpbYPiyGtO7b0cAlrZw4Mrv
0XKBrb3At6dwoT0wmD89VHK9vq2VdTUa
4ddrBoC1HSiu89JLzfXMV59B74qIm2xj
7CWVV5CGm74gAvba93StX50LTK78ikzM

POSSIBLE SECRETS
UVmnaLPTsQqsAUFvP4l9eFVdZ5Bnbi11
yCbh3JWABSPWXjzi8lqNfGSw4JUwRc1Z
fc6abssWsZoyWpr8fCHyT3ixVlnX2HG2
Z7tecEc8tS2JrzNmQM0R9CjEnjCb6ksC
MUUz2dKYtP7sZF6Tuk5kEGRgHEx452fj
el7YtyQobuGYp8qUnEWwGAo9eb5IMR8f
PPqjaOYWzYRlppBEr7ot7ueRFIAfsGXr
mZfo4fIlXHQscYR0BkWPKUfaL8c0bByk
1ad75ae72e05dcf4dadbd17a
LtGcJkDv8PpKzGxu4pknm0pyAahoAl9h
jDUjvWDGqsgivCcWfJbzlnhujFfNRoy6
Yb4G3rkI5nMioq4UjOOwWhO2qlazISB5
h73SRN04xx9GKM0Q116IBzLVfoAHdt6S
aJo4Pz0hsbQrFibFt4ypJbnLPuINPYvA
kvUI2sJVom05aD2rNLnp8ceY2vExoctW

POSSIBLE SECRETS
TZh0Sw2dsxVxMXdj340dFQnUzLECuqag
E1e7Uw5ci0LxHvCHKGZ7MMTImO0krz0e
UW9U9pyLqubavRm8Co8t1ARkgbl4JN3Q
DThvYGttjE9j20qDJ6yVSrG4WY8ID38s

## PLAYSTORE INFORMATION

**Title:** YsxLite

**Score:** 2.4257426 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** [com.ysxlite.cam](https://play.google.com/store/apps/details?id=com.ysxlite)

**Developer Details:** xiaowenyin2021, xiaowenyin2021, None, None, 25416287@qq.com,

**Release Date:** Sep 13, 2023 **Privacy Policy:** [Privacy link](#)

**Description:**

YsxLite is a virtual and exquisite network client software that is convenient and quick to bind network extensions, directly connect or access network extensions, and realize real-time observation, planning, alarm, real-time video/photography, local and remote video/photo transmission, deletion, download and sharing. , providing real-time image parameter settings, secure login and other control functions.

## SCAN LOGS

Timestamp	Event	Error
2024-10-28 16:11:22	Generating Hashes	OK

2024-10-28 16:11:22	Extracting APK	OK
2024-10-28 16:11:22	Unzipping	OK
2024-10-28 16:11:22	Getting Hardcoded Certificates/Keystores	OK
2024-10-28 16:11:31	Parsing AndroidManifest.xml	OK
2024-10-28 16:11:31	Parsing APK with androguard	OK
2024-10-28 16:11:31	Extracting Manifest Data	OK
2024-10-28 16:11:31	Performing Static Analysis on: YsxLite (com.ysxlite.cam)	OK
2024-10-28 16:11:31	Fetching Details from Play Store: com.ysxlite.cam	OK
2024-10-28 16:11:32	Manifest Analysis Started	OK
2024-10-28 16:11:32	Reading Network Security config from network_security_config.xml	OK
2024-10-28 16:11:32	Parsing Network Security config	OK

2024-10-28 16:11:32	Checking for Malware Permissions	OK
2024-10-28 16:11:32	Fetching icon path	OK
2024-10-28 16:11:32	Library Binary Analysis Started	OK
2024-10-28 16:11:32	Reading Code Signing Certificate	OK
2024-10-28 16:11:35	Running APKID 2.1.5	OK
2024-10-28 16:11:40	Updating Trackers Database....	OK
2024-10-28 16:11:40	Detecting Trackers	OK
2024-10-28 16:11:45	Decompiling APK to Java with jadx	OK
2024-10-28 16:14:08	Converting DEX to Smali	OK
2024-10-28 16:14:09	Code Analysis Started on - java_source	OK
2024-10-28 16:15:20	Android SAST Completed	OK

2024-10-28 16:15:20	Android API Analysis Started	OK
2024-10-28 16:15:27	Android Permission Mapping Started	OK
2024-10-28 16:16:16	Android Permission Mapping Completed	OK
2024-10-28 16:16:17	Finished Code Analysis, Email and URL Extraction	OK
2024-10-28 16:16:17	Extracting String data from APK	OK
2024-10-28 16:16:17	Extracting String data from Code	OK
2024-10-28 16:16:17	Extracting String values and entropies from Code	OK
2024-10-28 16:16:17	Performing Malware check on extracted domains	OK
2024-10-28 16:16:20	Saving to Database	OK

---

## Report Generated by - MobSF v4.1.0

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.

