MOBSF

ANDROID STATIC ANALYSIS REPORT

Instagram (357.0.0.0.90)

File Name:	Instagram_357.0.0.0.90_APKPure.apk
Package Name:	com.instagram.android
Scan Date:	Nov. 12, 2024, 8:46 a.m.

App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	100	2	3	1

FILE INFORMATION

File Name: Instagram_357.0.0.0.90_APKPure.apk
Size: 71.56MB
MD5: aad8cddd372fc8585bb242cbe8e56fa7
SHA1: b05c9a7109a3dbf6018f2a7bd8f76ccd6a2428bc
SHA256: b51fa3e82abc654bbb2060c5cec6687f202b5f74b5b11882e707ddc3f5d919e1

APP INFORMATION

App Name: Instagram
Package Name: com.instagram.android
Main Activity: com.instagram.lockscreen.LockScreenShortcutActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 357.0.0.0.90
Android Version Code: 375706983

APP COMPONENTS

Activities: 397
Services: 93
Receivers: 57
Providers: 14
Exported Activities: 39
Exported Services: 13
Exported Receivers: 17
Exported Providers: 10

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-08 01:41:31+00:00
Valid To: 2112-01-15 01:41:31+00:00
Issuer: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom

Serial Number: 0x4f31d2cb
Hash Algorithm: sha1
md5: f9cf2124dfaaccc45e7e3f739eca55ae
sha1: c56fb7d591ba6704df047fd98f535372fea00211
sha256: 5f3e50f435583c9ae626302a71f7340044087a7e2c60adacfc254205a993e305
sha512: a9b31009987e094fd2067d385056adfdb2cc4a272814a5982343335e639d064943e6025cbc7e36903f065c0e65bd99adab538dd0377c1404fa48b508970354a8
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: db2a9e7d36fb6915a995ee367d8971aca6f268c7b67e910b8431eeb636061c72
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
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.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.

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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
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.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.READ_BASIC_PHONE_STATE	normal	allows read-only access to basic phone state information.	Allows read only access to phone state with a non dangerous permission, including the information like cellular network type, software version.
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.instagram.direct.permission.PROTECTED_DEEPLINKING	unknown	Unknown permission	Unknown permission from android reference
com.instagram.direct.permission.DIRECT_APP_THREAD_STORE_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.facebook.services.identity.FEO2	unknown	Unknown permission	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.facebook.katana.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_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_ADSERVICES_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.CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS	normal	allows specifying candidate credential providers.	Allows specifying candidate credential providers to be queried in Credential Manager get flows, or to be preferred as a default in the Credential Manager create flows.
.permission.RECEIVE_ADM_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.amazon.device.messaging.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
com.instagram.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.MEDIA_PROJECTION	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.CAPTURE_VIDEO_OUTPUT	normal	allows capturing of video output.	Allows an application to capture video output.
com.instagram.android.permission.CROSS_PROCESS_BROADCAST_MANAGER	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
android.permission.FOREGROUND_SERVICE_CAMERA	normal	allows foreground services with camera use.	Allows a regular application to use Service.startForeground with the type "camera".
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
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.UPDATE_APP_BADGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

APKID ANALYSIS

<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes11.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes12.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</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></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.MANUFACTURER check
Build.BRAND check
SIM operator check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes9.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
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.instagram.android.activity.MainTabActivity	Schemes: instagram://, ig://, Hosts: mainfeed, story-camera, reels-camera, test-camera,
com.instagram.android.InternalLauncher	Schemes: instagram://, Hosts: mainfeed, story-camera, reels-camera, test-camera,
com.facebook.secure.deeplink.GlobalUriHandlerActivity	Schemes: instagram://, Hosts: ecp_checkout, ecp_e2e,

ACTIVITY	INTENT
com.instagram.url.UrlHandlerLauncherActivity	Schemes: http://, https://, instagram://, Hosts: instagram.com, www.instagram.com, applink.instagram.com, familycenter.instagram.com, aistudio.instagram.com, ig.me, active_promotions, ads_payments_prepay_payment_status, android, avatar, business_sign_up, business_profile_calling, call_settings, branded_content, branded_content_deal_creator_payout, branded_content_project, branded_content_ad, shops_directory, commerce, community_content, consent-launcher, cowatch, create_room, create_post, dogfooding_assistant, qr-code, suggested_reply, instant_reply, manage_folders, create_folder, responsive_guide, evergreen_safety_check_v2, welcome_message, quick_replies, explore, enter_promotion_payment, editprofile, edit_profile_bio, edit_profile_links, facebook_page_onboarding, inject, fundraiser, fb_profile_link, fb_story_tag_notification, fb_tag_notification, tag_mention_settings, fb_story_user_mention, guide, media, acredirect, inter_app/redirect, inter_app_redirect, open_access_application_enrollment, stories, stories_archive, open_access_profile_review_status, ads_product_page, product_display_page, professional_sign_up, promote, promote_high_performing_ad_upsell, music_selector, boost_with_reshared_media_not_delivering, professional_onboarding_checklist, professional_dashboard, profile, profile_shop, tag, location, user, fb_friends, fbpay_hub, bizwallet, bloks_native_hybrid_shell, shopping_seller_management_creator_media, products_for_you, reconsideration_products_for_you, firestarter_buyer_bootstrap, recommendations_in_explore_products, payments, shop_pay_did_finish, update_payment, bloks_order_receipt, hub_order_details, orders_hub, bwp_login, oauth_account_linking, step_up, business_order, follow_and_invite_friends, ig_payout_hub, ad_topics, insights, business_conversion, tv, igtv_profile, shopping_editorial, settings_payments, settings_theme, settings, settings_privacy, settings_account, settings_devoptions, ads_pay_now, fbe_app_store, ad_activity, ads_payments, fxim_name_changing_reminder, account_link_auth, smb_select_partner, smb_purchase_options, smb_edit_partner, smsrecovery, voting_info_center, create_shopping_tagged_post, shopping_home, shops_checkout, seller_screen_delegator, igtv_revshare_onboarding, reels_overlay_ads_onboarding, user_pay_onboarding, content_appreciation_management, subscriptions_management, subscriptions_claim_gift, subscriptions_ssc_invitation, creator_tools_value_props, creator_programs, open_creator_tool, open_collab_tools_settings, incentive_platform_management, incentive_platform_available_bonus, incentive_platform_progress_tracking, incentive_platform_xar_upsell, resume_payout_onboarding, product_eligibility, igtv_upload, product_composer, product_collection, open_xac, reels, reels_home, reels_share, reels_effect_page, reels_template_browser, audio, audio_page, business_spa_hub, pro2pro, pro2pro_framework, calendar_auth_success, calendar_auth_failure, calendar_auth_launch, discounts_interstitial, thread, msys_thread, seller_actions_bloks_app, creator_monetization_contact_support, creator_settings, creator_agent_suggested_replies, direct-thread, direct_message_options, shopping_guidance_router, technical_incident, bloks_leave_review, view_lead_details, aradscamera, ar_commerce, upload_contacts_settings, extbrowser, ar, embeds_opt_out_setting, payments_care_csat, recurring_notification, payments_payout_support, redirect_to_app, in_app_webview, trustly_authentication, map, shopping_creator_shop_management, injected_feed_unit_products, discovery_home, messaging_hub, tyi, care, transfer_your_information, collection, manage_qa_private_reply, survey, view_all_lead_opportunities, view_all_leads, fan_club, icebreakers, group_profile_creation, two_factor_setting, post_follow_ty, p2m, p2m_payout_settings, nft_collection_details, nft_collectible_details, nft_collection_listing, mediakit, languages_settings, content_language_settings, app_language_setting, accountquality, view_lead_gen_guidance_hub, direct_prompt_camera, camera_feed, security_checkup, hacked, view_lead_opportunity_details, wearable_pivot_page_url, wearables_pivot_page, wearables_sharing, ads_consent_growth_url, reels_trends, your_activity, news, share, live_camera, direct-inbox, direct_thread_deletion, create_creator_subscriber_chat, birthday_effects_settings, birthday_visibility_settings, event, event_rsvp, events_discovery, opal_profile, opal_content, add_school, birthday_center, blocking_list, hide_likes, hidden_words, account_status, settings_security, download_your_information, follower_milestone_share_to_story, achievements_hub, achievements_detail_bottom_sheet, reels_chaining, settings_2, nido, settings_elevation, channel, fb_channel, superlative, meta_pro_engagement, direct_agents, direct_ugc_ai_agent_bot, note_viewer, direct-notes, note_prompt_responses, aud_preloads, open_mbs_hub, trending_audio_list, camera_modal, direct_spotlight_submission, featured_channels, open_ig_x_posting_setting_page, new_collab_collection, meta_verified, hallpass_members, hallpass_participants, direct_create_group, qp_interstitial, saved, search, live_location, pinned_location, run_bloks_action, wonderwall, wonderwall_activity, encryptedbackups, friend_map, friend_map_location_shared, friend_map_audience_settings, story_camera, reels_lane, fb_profile_with_cta_banner, unvetteddevicelogin, whatsapp, permissions_invitation, p2b_thread_event_async_controller, direct_meta_ai_thread, p2b_thread_event_bloks_controller, broadcastchannelcontrols, preferred_businesses, burner, billingwizard, open_to_collab_surface, ugc_persona_ai_home, parental_access_education, quick_snap_details, story_template_discovery_surface, permissions_management, direct_privacy_feature_bundle_upsell, security_alerts_settings, security_alerts_feeds, edit_collaborators, gen_ai_accounts, gen_ai_bot_all_subscriptions, gen_ai_bot_single_subscription, myprofilecard, profilecard, link-spotify-from-audio-browser, permissions_removed_accounts, mifu_carousel, direct_account_theme_picker, ify_carousel, ify_recipe_selector, zero_extrig, ad_slider,

ACTIVITY	INTENT
	signals_playground, messaging_ad_inspiration, creators_inspiration, creator_activation_trial, remix_pivot_page, ad_preferences, launch_emoji_pong, teen_creator_bespoke,
com.instagram.url.InstagramHelpDeeplinkAliasActivity	Schemes: http://, https://, Hosts: help.instagram.com, about.instagram.com, privacycenter.instagram.com,
com.instagram.url.InstagramShortenDeeplinkAliasActivity	Schemes: http://, https://, Hosts: instagr.am, m.instagram.com,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.instagram.android,
com.spotify.sdk.android.auth.browser.RedirectUriReceiverActivity	Schemes: instagram://, Hosts: spotify-login-callback,

NETWORK SECURITY

HIGH: **4** | WARNING: **1** | INFO: **1** | SECURE: **2**

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.
3	*	high	Base config is configured to trust user installed certificates.
4	*	high	Base config is configured to bypass certificate pinning.

NO	SCOPE	SEVERITY	DESCRIPTION
5	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com meta.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
6	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com meta.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	info	Certificate pinning expires on 2025-11-06. After this date pinning will be disabled. [Pin: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Digest: SHA-256,Pin: ICGRfpgmOUXIWcQ/HXPLQTkFPEFPoDyjvH7ohhQpjzs= Digest: SHA-256,Pin: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= Digest: SHA-256,Pin: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU= Digest: SHA-256,Pin: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E= Digest: SHA-256,Pin: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= Digest: SHA-256,Pin: uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256,Pin: Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw= Digest: SHA-256,Pin: ape1HIIZ6T5d7GS61YBs3rD4NVvkfnVwELcCRW4Bqv0= Digest: SHA-256,Pin: oC+voZLIy4HLE0FVT5wFtxzKKokLDRKY1oNkfJYe+98= Digest: SHA-256,Pin: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: aCdH+LpiG4fN07wpXtXKvOciocDANj0daLOJKNJ4fx4= Digest: SHA-256,Pin: rn+WLLnmp9v3uDP7GPqbcaiRdd+UnCMrap73yz3yu/w= Digest: SHA-256,Pin: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= Digest: SHA-256,Pin: diGVwiVYbubAI3RW4hB9xU8e/CH2GnkuvVFZE8zmgzI= Digest: SHA-256,Pin: q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ= Digest: SHA-256]

NO	SCOPE	SEVERITY	DESCRIPTION
7	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
8	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. []

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **96** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/fb_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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.instagram.mainactivity.LauncherActivity) 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	Activity (com.instagram.mainactivity.InstagramMainActivity) 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.
6	Activity-Alias (com.instagram.android.activity.MainTabActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity-Alias (com.instagram.android.InternalLauncher) is not Protected. [android:exported=true]	warning	An Activity-Alias 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.instagram.url.UrlHandlerActivity) 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	Activity (com.instagram.url.UrlHandlerLauncherActivity) 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-Alias (com.instagram.url.InstagramHelpDeeplinkAliasActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity-Alias (com.instagram.url.InstagramShortenDeeplinkAliasActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (com.facebook.CustomTabActivity) 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.
13	Service (com.facebook.rti.push.service.FbnsService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Content Provider (com.instagram.contentprovider.users.impl.IgLoggedInUsersContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (com.instagram.launcherbadges.LauncherBadgesReceiver) is not Protected. [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.
16	Content Provider (com.instagram.contentprovider.DeferredCurrentUserProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Content Provider (com.instagram.barcelona.feed.crossapp.contentprovider.ThreadsContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Content Provider (com.instagram.contentprovider.AsyncFamilyAppsUserValuesProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
19	Content Provider (com.instagram.liteprovider.FirstPartyUserValuesLiteProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Content Provider (com.instagram.liteprovider.v2.FirstPartyUserValuesLiteProviderV2) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
21	Content Provider (com.instagram.contentprovider.InstallReferrerProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Content Provider (com.instagram.whatsapp.foabackuptoken.FoaBackupTokenProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Content Provider (com.instagram.common.analytics.fdidlite.AsyncInstagramFDIDLiteProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
24	Service (com.meta.trusteddevice.service.TrustedDeviceFoundationServiceImpl) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Activity (com.instagram.urlhandlers.boostresharedmedianotdelivering.BoostResharedMediaNotDeliveringUrlHandlerActivity) 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.
26	Activity (com.instagram.urlhandlers.musicselector.MusicSelectorUrlHandlerActivity) 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.
27	Broadcast Receiver (com.instagram.common.analytics.phoneid.InstagramPhoneIdRequestReceiver) is not Protected. [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.
28	Content Provider (com.instagram.common.analytics.phoneid.AsyncInstagramPhoneIdProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
29	Service (com.instagram.direct.stella.StellaDirectMessagingService) 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.
30	Service (com.instagram.fbpay.w3c.ipc.IsReadyToPayServiceImpl) 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.
31	Service (com.fbpay.w3c.ipc.AutofillKeyFetchServiceImpl) 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.
32	Activity (com.instagram.fbpay.w3c.views.PaymentActivity) 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.
33	Activity (com.spotify.sdk.android.auth.browser.RedirectUriReceiverActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
34	Broadcast Receiver (com.instagram.notifications.push.ADMMessageHandler$Receiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.device.messaging.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.
35	Service (com.facebook.analytics2.logger.GooglePlayUploadService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
36	Service (com.facebook.pushlite.PushLiteGCMJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
37	Broadcast Receiver (com.instagram.publisher.CopypastaConnectivityChangeReceiver) is not Protected. [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.
38	TaskAffinity is set for activity (com.instagram.share.handleractivity.ShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
39	Activity (com.instagram.share.handleractivity.ShareHandlerActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
40	TaskAffinity is set for activity (com.instagram.share.handleractivity.ShareHandlerActivityMultipleFeedAlias)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
41	Activity-Alias (com.instagram.share.handleractivity.ShareHandlerActivityMultipleFeedAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
42	TaskAffinity is set for activity (com.instagram.share.handleractivity.StoryShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
43	Activity (com.instagram.share.handleractivity.StoryShareHandlerActivity) 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.
44	TaskAffinity is set for activity (com.instagram.share.handleractivity.ReelShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
45	Activity (com.instagram.share.handleractivity.ReelShareHandlerActivity) 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.
46	TaskAffinity is set for activity (com.instagram.share.handleractivity.MultiStoryShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
47	Activity (com.instagram.share.handleractivity.MultiStoryShareHandlerActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
48	TaskAffinity is set for activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
49	Activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity) 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.
50	TaskAffinity is set for activity (com.instagram.share.handleractivity.ClipsShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
51	Activity (com.instagram.share.handleractivity.ClipsShareHandlerActivity) 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.
52	TaskAffinity is set for activity (com.instagram.share.handleractivity.ClipsMusicShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
53	Activity (com.instagram.share.handleractivity.ClipsMusicShareHandlerActivity) 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.
54	TaskAffinity is set for activity (com.instagram.share.handleractivity.ClipsThreadShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
55	Activity (com.instagram.share.handleractivity.ClipsThreadShareHandlerActivity) 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.
56	Activity (com.instagram.lockscreen.LockScreenCameraCaptureActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
57	Broadcast Receiver (com.instagram.pendingmedia.service.debug.DebugCommandsReceiver) is not Protected. [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.
58	Broadcast Receiver (com.instagram.push.InstagramAppUpgradeEventReceiver) is not Protected. [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.
59	Broadcast Receiver (com.instagram.push.FbnsInitBroadcastReceiver) is not Protected. [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.
60	Broadcast Receiver (com.facebook.oxygen.preloads.sdk.firstparty.managedappcache.IsManagedAppReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.facebook.appmanager.ACCESS [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.
61	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.
62	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.
63	Activity (com.instagram.bloks.extensions.plugins.bkigactionwarequestotp.BloksWhatsAppCodeReceiverActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
64	Broadcast Receiver (com.instagram.bloks.extensions.plugins.bkigactionwarequestotp.BloksWhatsAppCodeReceiver) is not Protected. [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.
65	Activity (com.instagram.direct.stella.permission.StellaPermissionActivity) 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.
66	Activity (com.instagram.settings.activity.NotificationSettingsHandlerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.instagram.android.permission.SYSTEM_ONLY protectionLevel: signatureOrSystem [android:exported=true]	info	An Activity is found to be exported, but is protected by a permission. However, the protection level of the permission is set to signatureOrSystem. It is recommended that signature level is used instead. Signature level should suffice for most purposes, and does not depend on where the applications are installed on the device.
67	Broadcast Receiver (com.instagram.notifications.push.fbns.IgPushSdkFbnsReceiverShim) is not Protected. [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.
68	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.
69	TaskAffinity is set for activity (com.instagram.acp.igacpsecuritykey.IGACPSecurityKeySignInActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
70	Broadcast Receiver (com.instagram.appcomponentmanager.IgAppComponentReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
71	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.
72	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.
73	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
74	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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.
75	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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.
76	TaskAffinity is set for activity (com.instagram.direct.share.handler.DirectShareHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
77	Activity (com.instagram.direct.share.handler.DirectShareHandlerActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
78	Activity-Alias (com.instagram.direct.share.handler.DirectShareHandlerActivityInterop) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
79	TaskAffinity is set for activity (com.instagram.direct.share.handler.DirectExternalMediaShareActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
80	Activity (com.instagram.direct.share.handler.DirectExternalMediaShareActivity) 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.
81	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityPhoto) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
82	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityPhotoInterop) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
83	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityVideo) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
84	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityVideoInterop) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
85	Activity (com.instagram.direct.share.handler.DirectMultipleExternalMediaShareActivity) 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.
86	Activity-Alias (com.instagram.direct.share.handler.DirectMultipleExternalMediaShareActivityInterop) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
87	Activity-Alias (com.instagram.direct.share.handler.DirectMultipleExternalMediaShareActivityMultiMediaFromMWA) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
88	Service (com.instagram.direct.share.choosertarget.DirectChooserTargetService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CHOOSER_TARGET_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.
89	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.AppComponentManagerTestingReceiver) is not Protected. [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.
90	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.FirstEnableStageTestReceiver) is not Protected. [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.
91	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.SecondEnableStageTestReceiver) is not Protected. [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.
92	Service (com.instagram.notifications.push.fcm.IgFirebaseMessagingService) 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.
93	Service (com.instagram.notifications.push.fcm.GetFCMTokenAndRegisterWithServerGCMService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
94	TaskAffinity is set for activity (com.instagram.rtc.activity.RtcCallActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
95	TaskAffinity is set for activity (com.instagram.rtc.activity.RtcCallIntentHandlerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
96	Service (androidx.sharetarget.ChooserTargetServiceCompat) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CHOOSER_TARGET_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.
97	Activity-Alias (com.facebook.secure.packagefinder.PackageFinderActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
98	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	arm64-v8a/libsuperpack-jni.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.	True info The binary has the following fortified functions: ['__strlen_chk', '__fwrite_chk', '__memcpy_chk', '__strncpy_chk', '__fgets_chk', '__strchr_chk', '__fread_chk', '__write_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libforce_dlopen.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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/liblinkerutils.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	arm64-v8a/libandroidx.graphics.path.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	arm64-v8a/libarcore_sdk_jni.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	arm64-v8a/libunwindstack_binary.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	$ORIGIN/./__unwindstack_binary-binary__shared_libs_symlink_tree:$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['__write_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libc++_shared.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.	True info The binary has the following fortified functions: ['__read_chk', '__vsnprintf_chk', '__fwrite_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libdistract.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libbreakpad_cpp_helper.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
10	arm64-v8a/libfbunwindstack.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.	$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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
11	arm64-v8a/libbreakpad.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__write_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libandroid_aware_dlopen.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
13	arm64-v8a/libsigmux.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
14	arm64-v8a/libsuperpack-jni.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.	True info The binary has the following fortified functions: ['__strlen_chk', '__fwrite_chk', '__memcpy_chk', '__strncpy_chk', '__fgets_chk', '__strchr_chk', '__fread_chk', '__write_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libforce_dlopen.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
16	arm64-v8a/liblinkerutils.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
17	arm64-v8a/libandroidx.graphics.path.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
18	arm64-v8a/libarcore_sdk_jni.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
19	arm64-v8a/libunwindstack_binary.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	$ORIGIN/./__unwindstack_binary-binary__shared_libs_symlink_tree:$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['__write_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libc++_shared.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.	True info The binary has the following fortified functions: ['__read_chk', '__vsnprintf_chk', '__fwrite_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/libdistract.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libbreakpad_cpp_helper.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.	False high This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
23	arm64-v8a/libfbunwindstack.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.	$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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
24	arm64-v8a/libbreakpad.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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__write_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	arm64-v8a/libandroid_aware_dlopen.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
26	arm64-v8a/libsigmux.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

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://api-480944848731659155 5-410575.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/390017741467/namespaces/firebase:fetch?key=AIzaSyA61fjQCSE2EqQMc_lX6XVYhKBXWh9MD3k. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	12/45	com.google.android.gms.permission.AD_ID, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.BLUETOOTH, android.permission.MODIFY_AUDIO_SETTINGS, com.android.launcher.permission.INSTALL_SHORTCUT, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.CHANGE_NETWORK_STATE, android.permission.CALL_PHONE, android.permission.BLUETOOTH_ADMIN, android.permission.CHANGE_WIFI_STATE

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
m.instagram.com	ok	**IP:** 157.240.192.174 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.087840 **Longitude:** 80.278473 **View:** Google Map
www.instagram.com	ok	**IP:** 157.240.192.174 **Country:** India **Region:** Tamil Nadu **City:** Chennai **Latitude:** 13.087840 **Longitude:** 80.278473 **View:** Google Map
api-480944848731659155 5-410575.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Notifications		https://reports.exodus-privacy.eu.org/trackers/68
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyA61fjQCSE2EqQMc_lX6XVYhKBXWh9MD3k"
"firebase_database_url" : "https://api-480944848731659155 5-410575.firebaseio.com"

PLAYSTORE INFORMATION

Title: Instagram

Score: 3.9972253 **Installs:** 5,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** com.instagram.android

Developer Details: Instagram, Instagram, Facebook, Inc. 1601 Willow Rd Menlo Park, CA 94025 United States, http://help.instagram.com/, android-support@instagram.com,

Release Date: Apr 3, 2012 **Privacy Policy:** Privacy link

Description:

Little moments lead to big friendships. Share yours on Instagram. —From Meta Connect with friends, find other fans, and see what people around you are up to and into. Explore your interests and post what's going on, from your daily moments to life's highlights. Share what you're up to and into on Insta®. - Keep up with friends on the fly with Stories and Notes that disappear after 24 hours. - Start group chats and share unfiltered moments with your Close Friends. - Share memories from recent events or trips in Feed. - Turn your life into a movie and discover short, entertaining videos on Instagram with Reels. - Customize your posts with exclusive templates, music, stickers and filters. Dive into your interests. - Watch videos from your favorite Creators and discover new content that's personalized to your interests. - Get inspired by photos and videos from new accounts in Explore. - Discover brands and small businesses, and shop products that are relevant to your personal style. Some Instagram features may not be available in your country or region. Terms and Policies - https://help.instagram.com/581066165581870 Consumer Health Privacy Policy: https://privacycenter.instagram.com/policies/health Learn how we're working to help keep our communities safe across Meta technologies at the Instagram Safety Center: https://about.instagram.com/safety

SCAN LOGS

Timestamp	Event	Error
2024-11-25 17:59:46	Generating Hashes	OK
2024-11-25 17:59:47	Extracting APK	OK
2024-11-25 17:59:47	Unzipping	OK
2024-11-25 17:59:53	Getting Hardcoded Certificates/Keystores	OK

2024-11-25 17:59:54	Parsing AndroidManifest.xml	OK
2024-11-25 17:59:54	Parsing APK with androguard	OK
2024-11-25 18:00:18	Extracting Manifest Data	OK
2024-11-25 18:00:18	Performing Static Analysis on: Instagram (com.instagram.android)	OK
2024-11-25 18:00:18	Fetching Details from Play Store: com.instagram.android	OK
2024-11-25 18:00:19	Manifest Analysis Started	OK
2024-11-25 18:00:19	Reading Network Security config from fb_network_security_config.xml	OK
2024-11-25 18:00:19	Parsing Network Security config	OK
2024-11-25 18:00:19	Checking for Malware Permissions	OK
2024-11-25 18:00:19	Fetching icon path	OK
2024-11-25 18:00:19	Library Binary Analysis Started	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libsuperpack-jni.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libforce_dlopen.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/liblinkerutils.so	OK

2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libarcore_sdk_jni.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libunwindstack_binary.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libdistract.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libbreakpad_cpp_helper.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libfbunwindstack.so	OK
2024-11-25 18:00:19	Analyzing apktool_out/lib/arm64-v8a/libbreakpad.so	OK
2024-11-25 18:00:20	Analyzing apktool_out/lib/arm64-v8a/libandroid_aware_dlopen.so	OK
2024-11-25 18:00:20	Analyzing apktool_out/lib/arm64-v8a/libsigmux.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libsuperpack-jni.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libforce_dlopen.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/liblinkerutils.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	OK

2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libarcore_sdk_jni.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libunwindstack_binary.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libdistract.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libbreakpad_cpp_helper.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libfbunwindstack.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libbreakpad.so	OK
2024-11-25 18:00:20	Analyzing lib/arm64-v8a/libandroid_aware_dlopen.so	OK
2024-11-25 18:00:21	Analyzing lib/arm64-v8a/libsigmux.so	OK
2024-11-25 18:00:22	Reading Code Signing Certificate	OK
2024-11-25 18:00:25	Running APKiD 2.1.5	OK
2024-11-25 18:01:00	Detecting Trackers	OK
2024-11-25 18:01:39	Decompiling APK to Java with jadx	OK
2024-11-25 18:05:05	Converting DEX to Smali	OK

2024-11-25 18:05:06	Code Analysis Started on - java_source	OK
2024-11-25 18:05:18	Android SAST Completed	OK
2024-11-25 18:05:18	Android API Analysis Started	OK
2024-11-25 18:06:20	Android Permission Mapping Started	OK
2024-11-25 18:06:23	Android Permission Mapping Completed	OK
2024-11-25 18:06:23	Email and URL Extraction Completed	OK
2024-11-25 18:06:23	Android Behaviour Analysis Started	OK
2024-11-25 18:06:24	Android Behaviour Analysis Completed	OK
2024-11-25 18:06:24	Extracting String data from APK	OK
2024-11-25 18:06:24	Extracting String data from SO	OK
2024-11-25 18:06:24	Extracting String data from Code	OK
2024-11-25 18:06:24	Extracting String values and entropies from Code	OK
2024-11-25 18:06:26	Performing Malware check on extracted domains	OK
2024-11-25 18:06:29	Saving to Database	OK

Report Generated by - MobSF v4.1.8

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.