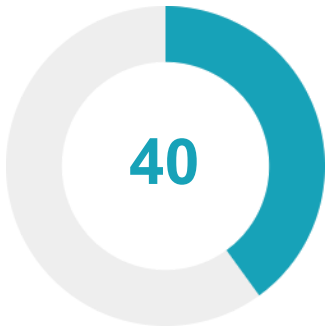
Security Score



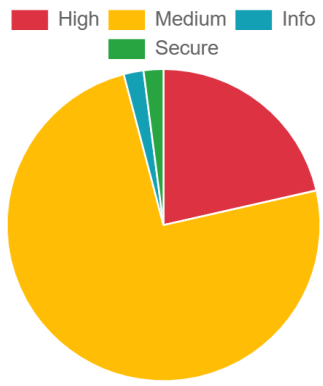
Security Score 40/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High
18

Medium
62

Info
2

Secure
2

Hotspot
1

high App can be installed on a vulnerable upatched Android version	MANIFEST
high Activity (com.instagram.mainactivity.MainActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.android.activity.MainTabActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.business.instantexperiences.ui.InstantExperiencesBrowserActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.url.UrlHandlerActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.url.UrlHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.bugreporter.BugReporterActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.canvas.CanvasActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.direct.share.handler.DirectShareHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.leadads.activity.LeadAdsActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.modal.PictureInPictureModalActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.settings.activity.NotificationSettingsHandlerActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Activity (com.instagram.settings.activity.NotificationSettingsHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.share.handleractivity.ShareHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.share.handleractivity.StoryShareHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity) is vulnerable to StrandHogg 2.0	MANIFEST
high Activity (com.instagram.video.videocall.activity.VideoCallActivity) is vulnerable to Android Task Hijacking/StrandHogg.	MANIFEST
high Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	CODE
medium Application vulnerable to Janus Vulnerability	CERTIFICATE
medium Certificate algorithm might be vulnerable to hash collision	CERTIFICATE
medium Activity (com.instagram.mainactivity.MainActivity) is not Protected.	MANIFEST
medium Activity-Alias (com.instagram.android.activity.MainTabActivity) is not Protected.	MANIFEST
medium Launch Mode of activity (com.instagram.business.instantexperiences.ui.InstantExperiencesBrowserActivity) is not standard.	MANIFEST
medium Launch Mode of activity (com.instagram.url.UrlHandlerActivity) is not standard.	MANIFEST
medium Activity (com.instagram.url.UrlHandlerActivity) is not Protected.	MANIFEST
medium Service (com.facebook.fbreact.autoupdater.ighttp.IgHttpUpdateGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Service (com.instagram.debug.memorydump.MemoryDumpTaskService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST

medium	Service (com.facebook.rti.push.service.FbnsService) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.facebook.rti.push.service.idsharing.FbnsSharingStateReceiver) is not Protected.	MANIFEST
medium	Content Provider (com.instagram.contentprovider.users.impl.IgLoggedInUsersContentProvider) is not Protected.	MANIFEST
medium	Content Provider (com.instagram.contentprovider.IgFaceEffectsProvider) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.instagram.launcherbadges.LauncherBadgesReceiver) is not Protected.	MANIFEST
medium	Service (com.instagram.util.offline.BackgroundWifiPrefetcherGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Content Provider (com.instagram.contentprovider.CurrentUserProvider) is not Protected.	MANIFEST
medium	Content Provider (com.instagram.contentprovider.FamilyAppsUserValuesProvider) is not Protected.	MANIFEST
medium	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.	MANIFEST
medium	Launch Mode of activity (com.instagram.bugreporter.BugReporterActivity) is not standard.	MANIFEST
medium	Launch Mode of activity (com.instagram.canvas.CanvasActivity) is not standard.	MANIFEST
medium	Broadcast Receiver (com.instagram.common.analytics.phoneid.InstagramPhoneIdRequestReceiver) is not Protected.	MANIFEST
medium	Content Provider (com.instagram.common.analytics.phoneid.InstagramPhoneIdProvider) is not Protected.	MANIFEST
medium	Service (com.instagram.direct.send.DirectMutationManagerGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Activity (com.instagram.direct.share.handler.DirectShareHandlerActivity) is not Protected.	MANIFEST
medium	Service (com.instagram.dogfood.selfupdate.SelfUpdateGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.instagram.install.InstallCampaignReceiver) is not Protected.	MANIFEST
medium	Launch Mode of activity (com.instagram.leadads.activity.LeadAdsActivity) is not standard.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Launch Mode of activity (com.instagram.modal.PictureInPictureModalActivity) is not standard.	MANIFEST
medium	Broadcast Receiver (com.instagram.notifications.push.GCMBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.instagram.notifications.push.ADMMessageHandler$Receiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.instagram.notifications.push.FbnsPushNotificationHandler$IgFbnsCallbackReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.instagram.pendingmedia.service.uploadretrypolicy.ConnectivityChangeReceiver) is not Protected.	MANIFEST

medium	Broadcast Receiver (com.instagram.push.InstagramAppUpgradeEventReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.instagram.push.fbns.FbnsInitBroadcastReceiver) is not Protected.	MANIFEST
medium	Launch Mode of activity (com.instagram.settings.activity.NotificationSettingsHandlerActivity) is not standard.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Launch Mode of activity (com.instagram.share.handleractivity.ShareHandlerActivity) is not standard.	MANIFEST
medium	Activity (com.instagram.share.handleractivity.ShareHandlerActivity) is not Protected.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Launch Mode of activity (com.instagram.share.handleractivity.StoryShareHandlerActivity) is not standard.	MANIFEST
medium	Activity (com.instagram.share.handleractivity.StoryShareHandlerActivity) is not Protected.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Launch Mode of activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity) is not standard.	MANIFEST
medium	Activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.instagram.store.PendingActionReceiver) is not Protected.	MANIFEST
medium	TaskAffinity is set for activity	MANIFEST
medium	Launch Mode of activity (com.instagram.video.videocall.activity.VideoCallActivity) is not standard.	MANIFEST
medium	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	The App uses an insecure Random Number Generator.	CODE
medium	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium	App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium	MD5 is a weak hash known to have hash collisions.	CODE
medium	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	CODE
medium	IP Address disclosure	CODE
medium	SHA-1 is a weak hash known to have hash collisions.	CODE
medium	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	CODE
medium	Application contains Privacy Trackers	TRACKERS
medium	This app may contain hardcoded secrets	SECRETS

info The App logs information. Sensitive information should never be logged. CODE

info This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. CODE

secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. CODE

secure This App may have root detection capabilities. CODE

hotspot Found 12 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for (No icon) (Instagram 74.0.0.21.99)