MOBSF

ANDROID STATIC ANALYSIS REPORT

Yuka (4.44)

File Name:	io.yuka.android_790.apk
Package Name:	io.yuka.android
Scan Date:	Sept. 1, 2025, 2:03 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	24	3	3	1

FILE INFORMATION

File Name: io.yuka.android_790.apk
Size: 83.25MB
MD5: f20eda25f65d229c985c878222e13b56
SHA1: 90089e99337c16e3e41f4295a271473828d61a54
SHA256: d3f747f705902b10d069c5640185e9708ae2750f0935fbe01ace388488597a55

APP INFORMATION

App Name: Yuka
Package Name: io.yuka.android
Main Activity: io.yuka.android.main.RootActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 4.44

Android Version Code: 790

APP COMPONENTS

Activities: 100
Services: 16
Receivers: 14
Providers: 11
Exported Activities: 7
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-05-25 09:48:00+00:00
Valid To: 2047-05-25 09:48:00+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x32be7a2335c7badcb39426b3dd177fd5ad1d73f2
Hash Algorithm: sha256
md5: 5066a2da27d3890eaf045101ea8b304e
sha1: a9626c847b9f10c48dab95e6ee162af007c8566f
sha256: a7e3c4a612680186937b02e7b89574d5fd62798b8cb668973992fa89f6198fcb
sha512: 5fb0fb514e4af7112ece190c15738b6c3a154268d4baf8b2acc342998119219eadf3f0239dfb2d14e11439acd32f0954324c90d1444a7375abd9acce8bcdbbb5
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ba75fb732731e9441738c53d87d881ff730b848cd6d416424e23099bc3790fae
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
io.yuka.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>f20eda25f65d229c985c878222e13b56.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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.BRAND check
Build.DEVICE check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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>r8 without marker (suspicious)</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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
io.yuka.android.main.RootActivity	Schemes: https://, http://, Hosts: app.yuka.io,
com.facebook.CustomTabActivity	Schemes: @string/facebook_login_protocol_scheme://, fbconnect://, Hosts: cct.io.yuka.android,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

ACTIVITY	INTENT
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 14 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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 (io.yuka.android.help.editproductthanks.HelpEditProductThanksActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (io.yuka.android.core.PushNotificationService) 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.
6	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.
8	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.google.firebase.auth.internal.RecaptchaActivity) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
12	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.
13	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (androidx.test.core.app.InstrumentationActivityInvoker$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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java mk/s5.java
				a5/h.java a9/e0$c.java a9/e0.java a9/p0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a9/q0.java a9/u.java aa/a.java ab/a.java ad/h.java ae/b.java ae/o.java af/g.java ah/h.java aj/c.java at/grabner/circleprogress/CircleProgressView.java aw/C0327c.java aw/C0330f.java aw/C0374m.java aw/C0390a0.java aw/C0392b0.java aw/C0416u.java aw/C0419x.java aw/C0420y.java aw/C0469a.java aw/ProductAndRecoFromScanLog.java aw/b0.java aw/d0.java aw/g.java aw/g0.java aw/k.java aw/x.java b5/d.java b8/e.java b8/f.java b8/k.java b8/l.java b8/n.java b8/o.java bc/h.java be/b.java bg/l.java bi/d0.java bq/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c5/a.java ca/j.java cb/b.java ci/a.java cj/a.java cj/l.java com/airbnb/lottie/LottieAnimationView.java com/bumptech/glide/b.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/engine/v.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/e.java com/bumptech/glide/load/resource/bitmap/e0.java com/bumptech/glide/load/resource/bitmap/p.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/t.java com/firebase/ui/auth/AuthUI$2.java com/firebase/ui/auth/AuthUI$5.java com/firebase/ui/auth/AuthUI$IdpConfig.java com/firebase/ui/auth/AuthUI.java com/firebase/ui/auth/data/remote/GoogleSignInHandler.java com/firebase/ui/auth/ui/credentials/CredentialSaveActivity.java com/firebase/ui/auth/ui/email/EmailLinkFragment$1.java com/firebase/ui/auth/util/CredentialUtils.java com/firebase/ui/auth/util/data/TaskFailureLo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gger.java com/firebase/ui/auth/viewmodel/ResourceObserver.java com/firebase/ui/auth/viewmodel/email/EmailProviderResponseHandler.java com/firebase/ui/auth/viewmodel/smartlock/SmartLockHandler.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/kennyc/bottomsheet/a.java com/mobsandgeeks/saripaar/Registry.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java com/scandit/datacapture/core/internal/module/source/o.java com/snapchat/djinni/NativeObjectManager.java com/theartofdev/edmodo/cropper/BitmapUtils.java com/theartofdev/edmodo/cropper/CropImageActivity.java com/theartofdev/edmodo/cropper/CropOverlayView.java d2/b.java db/h.java db/s.java db/t.java dq/ProductAndRecoFromScanLog.java ds/m.java e/d.java e8/h.java e9/c.java ei/a.java ei/b.java ei/c.java ei/i.java ep/g.java f1/d.java f3/g.java f5/b.java fe/a0.java fe/b0.java fe/c.java fe/c1.java fe/d0.java fe/f0.java fe/l0.java fe/l1.java fe/p0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	fe/r0.java fe/u6.java fe/w1.java fi/b.java fj/d.java fj/f.java fp/u.java g1/a.java g2/a.java g6/e.java gc/h.java gg/l2.java h1/x$a.java hb/d.java he/f.java he/n.java i0/a0.java id/p.java ij/e.java ij/f.java io/grpc/android/AndroidChannelBuilder.java io/grpc/internal/ManagedChannelImpl.java io/grpc/okhttp/internal/Platform.java io/yuka/android/core/nutritionFacts/NutritionFactsVerifier.java io/yuka/android/editProduct/EditProductActivityViewModel.java io/yuka/android/editProduct/camera/CameraXFragment.java io/yuka/android/editProduct/category/CategoryAdapter.java io/yuka/android/editProduct/deprecaded/EditProductManager.java io/yuka/android/editProduct/deprecaded/PhotoActivity.java io/yuka/android/editProduct/end/ThanksActivity.java io/yuka/android/firestore/CategorySuggestionService.java io/yuka/android/firestore/ChartFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/yuka/android/firestore/WritableFieldsCache.java io/yuka/android/help/HelpScanActivity.java io/yuka/android/help/editproductthanks/HelpEditProductThanksActivity.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java io/yuka/android/main/DeleteAccount.java io/yuka/android/main/RootActivity.java io/yuka/android/main/UserDisabled.java io/yuka/android/network/CategorySuggestionService.java io/yuka/android/network/WritableFieldsCache.java io/yuka/android/productdetails/NoGradeActivity.java io/yuka/android/scanner/ScanActivity.java io/yuka/android/scanner/ScanActivityViewModel.java io/yuka/android/search/c.java io/yuka/android/tools/CachedFileProvider.java io/yuka/android/tools/CustomExoPlayerVideoView.java io/yuka/android/tools/LockableBottomSheet.java io/yuka/android/tools/TouchZoomImageView.java io/yuka/android/yearinreview/c.java j7/a.java j8/a.java j9/c.java ja/a.java ja/d.java k0/d.java k1/e.java k2/c.java k5/n.java k7/b.java k8/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k8/g.java k8/g0.java k8/k0.java k8/u0.java k9/d0.java k9/y.java ke/g.java kh/b.java kj/f.java l/c.java l2/a.java l7/d.java l7/e.java l8/c.java l8/f.java l8/g0.java l8/m.java lh/e.java lp/b.java lr/a.java lx/b.java md/i.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java mk/b9.java mk/d4.java mk/j2.java mk/o8.java mk/ob.java mk/p3.java mk/ug.java mk/z3.java mx/a.java mx/c.java n7/b.java n7/j.java n7/l.java nb/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nb/d.java nb/f.java nb/h.java ne/r.java o7/c.java o7/e.java o8/l$c.java o8/l.java og/b.java oh/c.java org/slf4j/helpers/h.java org/tensorflow/lite/NativeInterpreterWrapper.java p2/m.java p8/e.java p8/f.java pg/c.java pub/devrel/easypermissions/a.java q1/c.java q7/i.java q7/k.java q9/a.java r7/e.java r7/i.java r8/a.java rb/a.java s7/a.java sa/g.java sf/r.java t7/c.java t7/d.java t7/f.java t7/s.java t7/t.java t8/f.java t8/i.java t8/l$a.java t8/l.java t9/a.java t9/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t9/c.java t9/d.java u0/d.java u4/n.java u6/c.java ua/a.java ub/a.java uc/a.java v7/m.java va/b.java va/c.java va/k.java va/r.java vb/a.java w4/o$e.java w4/o.java w4/r.java w4/u.java w4/y.java w8/a.java wa/d0.java wa/i0.java wa/j.java wa/m.java wa/n.java wa/n0.java wa/q.java wa/z.java x/o0.java x0/f.java x9/k.java xb/c.java xc/d.java y4/a.java yb/b.java yc/b.java yh/a.java yh/e.java z/s0.java z0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	a9/p0.java aw/C0462a.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	d6/g.java l8/d.java t8/l.java
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	k8/b.java k8/i0.java k8/j.java k8/l0.java k8/u0.java r8/j.java x8/b.java
				ah/g.java ai/b.java bn/o.java com/algolia/search/model/indexing/BatchOperation.java com/algolia/search/model/response/ResponseAPIKey.java com/algolia/search/model/response/creation/CreationAPIKey.java com/algolia/search/model/response/revision/RevisionAPIKey.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/firebase/ui/auth/IdpResponse.java com/firebase/ui/auth/ui/email/EmailLinkErrorRecoveryActivity.java
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/firebase/ui/auth/ui/phone/PhoneNumberVerificationHandler.java com/firebase/ui/auth/util/data/EmailLinkPersistenceManager.java com/scandit/datacapture/core/internal/module/capture/NativeRecognitionContextSettings.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/PickFirstLoadBalancerProvider.java io/grpc/internal/TransportFrameUtil.java io/jsonwebtoken/JwsHeader.java io/yuka/android/editProduct/category/SelectCategoryFragment.java io/yuka/android/editProduct/disclaimer/EditDisclaimerFragment.java io/yuka/android/editProduct/packaging/AddPackagingMaterialActivity.java io/yuka/android/editProduct/packaging/PackagingAdapter.java io/yuka/android/editProduct/packaging/PackagingViewModel.java kg/b.java m7/f.java n8/CloudBridgeCredentials.java oe/b.java of/b.java of/r.java p5/Preference.java pe/e.java pe/w.java pf/f.java pw/z0.java q2/a.java vq/SearchHistory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	a3/r.java a9/p0.java com/firebase/ui/auth/util/data/SessionUtils.java ei/c.java ht/a.java ht/b.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/PickFirstLeafLoadBalancer.java io/grpc/internal/PickFirstLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java jt/a.java sf/c0.java th/d.java u2/m1.java uw/e.java zj/c.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/theartofdev/edmodo/cropper/BitmapUtils.java com/theartofdev/edmodo/cropper/CropImageActivity.java io/yuka/android/editProduct/deprecaded/PhotoActivity.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java og/c.java w4/y.java z/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ig/z.java io/yuka/android/tools/Tools.java j9/a.java mk/x3.java og/b.java
11	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	b5/c.java ea/m0.java ea/v0.java nf/s2.java nf/s3.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	id/c.java md/v.java ne/i.java
13	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	aw/C0352a.java ds/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	a9/e0.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a9/a.java a9/e0.java a9/p0.java a9/q0.java a9/u0.java af/g.java aw/C0355b0.java aw/a1.java com/firebase/ui/auth/data/remote/FacebookSignInHandler.java ds/b0.java io/yuka/android/account/premiumstate/PremiumStateActivity.java io/yuka/android/brandcallout/BrandCallOutActivity.java io/yuka/android/editProduct/EditProductActivityViewModel.java io/yuka/android/editProduct/deprecaded/PhotoActivity.java io/yuka/android/editProduct/origins/CustomerServiceEmailIntroFragment.java io/yuka/android/editemail/EditEmailActivity.java io/yuka/android/help/FAQActivity.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java io/yuka/android/help/i.java io/yuka/android/main/RootActivity.java io/yuka/android/premium/PremiumActivity.java io/yuka/android/product/fragment/foodenvironment/FoodEnvironmentViewModel.java io/yuka/android/productdetails/ecofeatures/packagingdetail/d.java io/yuka/android/scanner/ScanActivity.java k9/c.java wa/k.java zf/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	a9/e0.java
00091	Retrieve data from broadcast	collection	a9/e0.java com/firebase/ui/auth/ui/email/EmailActivity.java io/yuka/android/main/RootActivity.java io/yuka/android/productdetails/product/ProductActivity.java k9/h0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	a9/e0.java
00191	Get messages in the SMS inbox	sms	a9/a.java a9/e0.java a9/p0.java aw/C0462a.java
00200	Query data from the contact list	collection contact	a9/e0.java
00187	Query a URI and check the result	collection sms calllog calendar	a9/e0.java
00201	Query data from the call log	collection calllog	a9/e0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	a9/e0.java o7/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	aw/C0360e.java aw/C0462a.java bt/i.java c9/k.java com/bumptech/glide/load/a.java d6/g.java d6/h.java ds/e.java g1/a.java gg/u2.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java io/yuka/android/editProduct/nutritionFacts/NutritionFactsPicAnalyzer.java io/yuka/android/editProduct/packaging/SortingInstructionPicViewModel.java k7/b.java l8/f.java ne/a0.java oe/f.java og/c.java se/e.java t7/f.java t8/l.java u8/j.java ue/a.java v1/l.java vg/k.java vg/q.java w4/y.java x8/a.java y4/b.java yw/q.java z/u.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	l8/f.java t8/l.java
00022	Open a file from given absolute path of the file	file	b5/d.java c5/a.java com/github/mikephil/charting/charts/Chart.java d6/g.java d6/h.java io/yuka/android/editProduct/deprecaded/PhotoActivity.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java kj/f.java mk/a9.java mk/g2.java mk/i3.java mk/s3.java mk/z2.java nk/c.java oe/f.java org/tensorflow/lite/b.java u5/q.java v1/l$h.java v1/l.java vg/a.java vg/c.java vg/e.java vg/h.java vg/j.java vg/k.java vg/t.java w4/y.java z/u.java
00004	Get filename and put it to JSON object	file collection	c9/c.java g9/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java r9/a.java
00163	Create new Socket and connecting to it	socket	io/grpc/android/UdsSocket.java io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java r9/a.java vg/g.java
00036	Get resource file from res/raw directory	reflection	a9/a.java a9/p0.java a9/q0.java aw/C0353a0.java aw/C0420y.java ds/a0.java io/yuka/android/help/enhancedemail/EnhancedEmailActivity.java io/yuka/android/scanner/ScanActivity.java io/yuka/android/tools/CustomExoPlayerVideoView.java wa/k.java
00096	Connect to a URL and set request method	command network	d6/b.java k8/b0$c.java n8/g.java pg/c.java r2/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a9/p0.java a9/q0.java aw/a1.java io/yuka/android/brandcallout/BrandCallOutActivity.java io/yuka/android/editemail/EditEmailActivity.java io/yuka/android/help/FAQActivity.java io/yuka/android/premium/PremiumActivity.java io/yuka/android/product/fragment/foodenvironment/FoodEnvironmentViewModel.java wa/k.java
00014	Read file into a stream and put it into a JSON object	file	c9/k.java oe/f.java og/c.java u8/j.java ue/a.java x8/a.java
00089	Connect to a URL and receive input stream from the server	command network	ae/o.java j9/c.java n8/g.java pg/c.java r2/i.java
00109	Connect to a URL and get the response code	network command	ae/o.java ja/d.java n8/g.java pg/c.java r2/i.java r9/b.java sa/f.java
00024	Write file after Base64 decoding	reflection file	u5/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00079	Hide the current app's icon	evasion	q5/p.java
00026	Method reflection	reflection	au/a.java au/b.java
00065	Get the country code of the SIM card provider	collection	aw/C0408m.java com/firebase/ui/auth/util/data/PhoneNumberUtils.java fp/m.java
00030	Connect to the remote server through the given URL	network	d6/b.java r2/i.java
00132	Query The ISO country code	telephony collection	p2/h0.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	h1/x.java
00094	Connect to a URL and read data from it	command network	r2/i.java re/a.java
00108	Read the input stream from given URL	network command	r2/i.java
00015	Put buffer stream (data) to JSON object	file	a9/p0.java
00078	Get the network operator name	collection telephony	a9/p0.java
00009	Put data in cursor to JSON object	file	a9/p0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	o2/a.java
00183	Get current camera parameters and change the setting.	camera	mk/ug.java
00125	Check if the given file path exist	file	io/yuka/android/editProduct/deprecaded/PhotoActivity.java
00005	Get absolute path of file and put it to JSON object	file	oe/f.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://yuca.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/844633789705/namespaces/firebase:fetch?key=AIzaSyBom1GwrWFqrH0zgjHiypC3DXTeAzgJ4Ak. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.CAMERA, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

DOMAIN	STATUS	GEOLOCATION
yuka.io	ok	**IP:** 46.101.146.164 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
help.yuka.io	ok	**IP:** 146.148.41.214 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
www.cotrep.fr	ok	**IP:** 4.233.56.168 **Country:** United States of America **Region:** Louisiana **City:** Monroe **Latitude:** 32.548328 **Longitude:** -92.045235 **View:** Google Map
www.inserm.fr	ok	**IP:** 51.158.55.228 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.fao.org	ok	**IP:** 104.18.10.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.epa.gov	ok	**IP:** 18.238.96.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
www.efsa.europa.eu	ok	**IP:** 18.238.109.97 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
us-central1-project-6706240203345572135.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firestore.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.who.int	ok	**IP:** 192.133.11.1 **Country:** United States of America **Region:** Massachusetts **City:** Lexington **Latitude:** 42.445580 **Longitude:** -71.236221 **View:** Google Map
clinicaltrials.gov	ok	**IP:** 34.107.134.59 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goodtoucan.com	ok	**IP:** 67.207.77.246 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.yuka.io	ok	**IP:** 76.76.21.21 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
tools.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
vapor.goodtoucan.com	ok	**IP:** 162.159.140.98 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.foodwatch.org	ok	**IP:** 62.113.231.137 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Paderborn **Latitude:** 51.719051 **Longitude:** 8.754390 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
oehha.ca.gov	ok	**IP:** 45.60.86.218 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clients3.google.com	ok	**IP:** 142.250.74.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.cir-safety.org	ok	**IP:** 209.126.25.193 **Country:** United States of America **Region:** Michigan **City:** Lansing **Latitude:** 42.733280 **Longitude:** -84.637764 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.cnrs.fr	ok	**IP:** 80.94.184.70 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.cspinet.org	ok	**IP:** 34.74.8.155 **Country:** United States of America **Region:** South Carolina **City:** North Charleston **Latitude:** 32.888561 **Longitude:** -80.007507 **View:** Google Map
res.cloudinary.com	ok	**IP:** 104.16.78.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ippocampoedizioni.it	ok	**IP:** 92.243.16.228 **Country:** France **Region:** Ile-de-France **City:** Saint-Denis **Latitude:** 48.933331 **Longitude:** 2.366670 **View:** Google Map
phone.firebase	ok	No Geolocation information available.
www.bfr.bund.de	ok	**IP:** 5.75.209.44 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.helpdocs.io	ok	**IP:** 146.148.41.214 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
www.iarc.who.int	ok	**IP:** 18.238.96.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
en.inrs.fr	ok	**IP:** 193.203.109.50 **Country:** France **Region:** Grand-Est **City:** Nancy **Latitude:** 48.683331 **Longitude:** 6.200000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
yuca.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.echa.europa.eu	ok	**IP:** 9.223.49.252 **Country:** United States of America **Region:** North Carolina **City:** Durham **Latitude:** 35.994701 **Longitude:** -78.896202 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.143 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.fda.gov	ok	**IP:** 23.53.145.191 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.anses.fr	ok	**IP:** 4.233.201.224 **Country:** United States of America **Region:** Louisiana **City:** Monroe **Latitude:** 32.548328 **Longitude:** -92.045235 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
maps-api.apple.com	ok	**IP:** 17.33.193.237 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
mlkit.googleapis.com	ok	**IP:** 216.58.207.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseappcheck.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.wwf.fr	ok	**IP:** 185.145.32.229 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
firebaseml.googleapis.com	ok	**IP:** 142.250.74.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ntp.niehs.nih.gov	ok	**IP:** 104.18.30.113 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ce84d4d7c.cloudimg.io	ok	**IP:** 23.206.188.208 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.industrialchemicals.gov.au	ok	**IP:** 23.62.226.169 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.iubenda.com	ok	**IP:** 38.32.110.58 **Country:** United States of America **Region:** Arizona **City:** Casa Grande **Latitude:** 32.879501 **Longitude:** -111.757347 **View:** Google Map
support.apple.com	ok	**IP:** 23.40.173.114 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.beuc.eu	ok	**IP:** 13.51.62.86 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
en.wikipedia.org	ok	**IP:** 198.35.26.96 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 142.250.74.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gu.de	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
health.ec.europa.eu	ok	**IP:** 18.155.173.100 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ineris.fr	ok	**IP:** 94.23.123.122 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	wa/y.java
copy@inbound.yuka	io/yuka/android/brandcallout/BrandCallOutViewModel.java
team@yuka.io	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Scandit	Analytics	https://reports.exodus-privacy.eu.org/trackers/84

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"_authorize" : "Allow"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"category_food_turkey" : "Turkeys"
"com.google.firebase.crashlytics.mapping_file_id" : "7d29f79960b44372976902fc97efc80f"
"firebase_database_url" : "https://yuca.firebaseio.com"
"firebase_web_host" : "CHANGE-ME"
"google_api_key" : "AIzaSyBom1GwrWFqrH0zgjHiypC3DXTeAzgJ4Ak"
"google_crash_reporting_api_key" : "AIzaSyBom1GwrWFqrH0zgjHiypC3DXTeAzgJ4Ak"
"turkey" : "turkey"

POSSIBLE SECRETS
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
af60eb711bd85bc1e4d3e0a462e074eea428a8
p+PEphJoAYaTewLnuJV01f1ieYuMtmiXOZL6ifYZj8s=
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c56fb7d591ba6704df047fd98f535372fea00211
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

POSSIBLE SECRETS
xBkDPNxUEiMRX5vPP2wqvCR4Grb8GZQqrKNyC0Y
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
xJXZd/zR0io4+XWtcwbtnyYutpO4NX7DhE3xBg4
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
82c62205f0ef0ea96608a8
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
cc2751449a350f668590264ed76692694a80308a
3071c8717539de5d5353f4c8cd59a032

POSSIBLE SECRETS
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a0784d7a4716f3feb4f64e7f4b39bf04
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Yuka - Food & Cosmetic Scanner

Score: 4.753136 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** io.yuka.android

Developer Details: Yuka App, 5638764101633798184, None, https://yuka.io, team@yuka.io,

Release Date: Dec 2, 2019 **Privacy Policy:** Privacy link

Description:

◆ 70 MILLION USERS ◆ Yuka scans food, beauty & personal care products to decipher their ingredients and evaluate their impact on your health. In a world of incomprehensible labels, Yuka provides clarity in one quick scan so you can make clear-sighted purchases. Yuka uses a simple color code to inform you of the product's impact on your health: excellent, good, mediocre, or poor. You can access a detailed info page for each product, to help you understand its grade. ◆ 3 MILLION FOOD PRODUCTS ◆ Every product is evaluated according to 3 objective criteria: nutritional value, additives, and the organic dimension of the product. ◆ 2 MILLION BEAUTY PRODUCTS ◆ The scoring method relies on analyzing all of the product's ingredients. Every ingredient is assigned a level of risk, based on current scientific research. ◆ BEST PRODUCT RECOMMENDATIONS ◆ For any product with a negative grade, Yuka will recommend in total independence a similar product that's better for your health

as an alternative. ◆ 100% INDEPENDENT ◆ Yuka is a 100% independent application. This means that product evaluations and recommendations are completely objective: no brand or manufacturer can influence them in one way or another. In addition, the application does not advertise. Find out more about our funding on our website. --- Terms of use: https://yuka-app.helpdocs.io/l/en/article/2a12869y56

SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:03:09	Generating Hashes	OK
2025-09-01 14:03:09	Extracting APK	OK
2025-09-01 14:03:09	Unzipping	OK
2025-09-01 14:03:10	Parsing APK with androguard	OK
2025-09-01 14:03:11	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:03:11	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 14:03:14	Parsing AndroidManifest.xml	OK
2025-09-01 14:03:14	Extracting Manifest Data	OK

2025-09-01 14:03:14	Manifest Analysis Started	OK
2025-09-01 14:03:14	Performing Static Analysis on: Yuka (io.yuka.android)	OK
2025-09-01 14:03:16	Fetching Details from Play Store: io.yuka.android	OK
2025-09-01 14:03:17	Checking for Malware Permissions	OK
2025-09-01 14:03:17	Fetching icon path	OK
2025-09-01 14:03:17	Library Binary Analysis Started	OK
2025-09-01 14:03:17	Reading Code Signing Certificate	OK
2025-09-01 14:03:18	Running APKiD 2.1.5	OK
2025-09-01 14:03:24	Detecting Trackers	OK
2025-09-01 14:03:29	Decompiling APK to Java with JADX	OK
2025-09-01 14:03:47	Decompiling with JADX failed, attempting on all DEX files	OK

2025-09-01 14:03:47	Decompiling classes6.dex with JADX	OK
2025-09-01 14:03:51	Decompiling classes2.dex with JADX	OK
2025-09-01 14:03:52	Decompiling classes4.dex with JADX	OK
2025-09-01 14:04:00	Decompiling classes.dex with JADX	OK
2025-09-01 14:04:08	Decompiling classes3.dex with JADX	OK
2025-09-01 14:04:17	Decompiling classes5.dex with JADX	OK
2025-09-01 14:04:22	Decompiling classes6.dex with JADX	OK
2025-09-01 14:04:26	Decompiling classes2.dex with JADX	OK
2025-09-01 14:04:27	Decompiling classes4.dex with JADX	OK
2025-09-01 14:04:36	Decompiling classes.dex with JADX	OK
2025-09-01 14:04:44	Decompiling classes3.dex with JADX	OK

2025-09-01 14:04:52	Decompiling classes5.dex with JADX	OK
2025-09-01 14:04:58	Converting DEX to Smali	OK
2025-09-01 14:04:58	Code Analysis Started on - java_source	OK
2025-09-01 14:05:05	Android SBOM Analysis Completed	OK
2025-09-01 14:05:14	Android SAST Completed	OK
2025-09-01 14:05:14	Android API Analysis Started	OK
2025-09-01 14:05:24	Android API Analysis Completed	OK
2025-09-01 14:05:24	Android Permission Mapping Started	OK
2025-09-01 14:05:31	Android Permission Mapping Completed	OK
2025-09-01 14:05:31	Android Behaviour Analysis Started	OK
2025-09-01 14:05:45	Android Behaviour Analysis Completed	OK

2025-09-01 14:05:45	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:05:51	Email and URL Extraction Completed	OK
2025-09-01 14:05:51	Extracting String data from APK	OK
2025-09-01 14:05:52	Extracting String data from Code	OK
2025-09-01 14:05:52	Extracting String values and entropies from Code	OK
2025-09-01 14:05:57	Performing Malware check on extracted domains	OK
2025-09-01 14:06:19	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.