APP SCORES

Security Score **47/100**

Trackers Detection **4/432**

FILE INFORMATION

File Name RTC_Paiement-2.0.2.apk

Size 29.2MB

MD5 4fc1d615034fc3cf8633d1b51aa0f1b1

SHA1 8f684f2bd14bf35fbb7aa20170b7dd80ac5c45d7

SHA256 fab626c8126216f1bf3f1f47fe0219b8d2902a0c3932a25bd2d93084747a54fc

APP INFORMATION

App Name RTC Paiement

Package Name com.rtc.ticket

Main Activity fr.airweb.grandlac.ui.splash.SplashActivity

Target SDK 35 Min SDK 23 Max SDK

Android Version Name 2.0.2 Android Version Code 413

PLAYSTORE INFORMATION

Title RTC Nomade paiement

Score 3.25 Installs 100,000+ Price 0 Android Version Support Category Travel & Local Play Store URL com.rtc.ticket

Developer RTC : Réseau de transport de la Capitale, Developer ID RTC+:+R%C3%A9seau+de+transport+de+la+Capitale

Developer Address None

Developer Website https://www.rtcquebec.ca/

Developer Email _CentresdinformationduRTC@rtcquebec.ca

Release Date Jun 8, 2020 Privacy Policy Privacy link

Description

With the RTC Nomade paiement system, you can buy public transit tickets for Québec City’s public transit network, RTC, whenever and wherever you are.

- Create an account
- Buy transit tickets online and pay with your credit card
- Use the mobile app to activate your ticket before boarding the bus
- Pull up the eticket and present it to the driver when your board
- Use your eticket when you transfer onto another bus

The RTC Nomade payment system: fast, easy, and secure.

8 / 37

EXPORTED ACTIVITIES

View All

1 / 11

EXPORTED SERVICES

View All

2 / 6

EXPORTED RECEIVERS

View All

0 / 8

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-08 07:24:22+00:00
Valid To: 2050-06-08 07:24:22+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xdf10bf85828bb78606ca4e71114dc6666974d2a7
Hash Algorithm: sha256
md5: b2c4ee317d508b6d66e3a9a87e8b13f7
sha1: 2655d1b0268d67ed84448fee5dab048d1dfb86df
sha256: 5a52284ad3a3251b4987605fe702f70e31fcfd2a5d5e672794677d0c432199e2
sha512:
bdabc43beacf434ab942cad85864566c4b1802362fc37f6312f6d1b7724d748c074323095116c3dde6697572dce9fec60dee5f3ef7d1bae1d9298c2e8bf599a3
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 9765c73bdf823beceba1cb4c18df7f946c66c2fbeabe745eee5d59511858ed43
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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_CUSTOM_AUDIENCE	unknown	Unknown permission	Unknown permission from android reference	
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.	
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.	
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

Showing 1 to 10 of 20 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	

API	FILES
Dynamic Class and Dexloading	
Execute OS Command	
Get Android Advertising ID	
Get Installed Applications	

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.facebook.CustomTabActivity	**Schemes**: @string/ticket_fb_login_protocol_scheme://, @string/facebook_login_protocol_scheme://, fbconnect://, **Hosts:** cct.com.rtc.ticket,
com.google.firebase.auth.internal.GenericIdpActivity	**Schemes**: genericidp://, **Hosts:** firebase.auth, **Paths:** /,
com.google.firebase.auth.internal.RecaptchaActivity	**Schemes**: recaptcha://, **Hosts:** firebase.auth, **Paths:** /,

Showing 1 to 3 of 3 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	1	0	0

Search:

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.

Showing 1 to 2 of 2 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	11	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
4	**Activity** (fr.airweb.ticket.PrincipalActivity) 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.canhub.cropper.CropImageActivity) 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** (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.	
7	**Activity** (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
8	**Activity** (androidx.test.core.app.InstrumentationActivityInvoker$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	OPTIONS
9	**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.	
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.	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	7	2	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		
2	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		
3	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		
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
5	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		
6	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	K3/M.java K3/U.java S0/c.java	
7	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	R8/C2892c.java q4/b.java	
8	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2	F8/b.java io/jsonwebtoken/impl/security/EcSignatureAlgorithm.java io/jsonwebtoken/impl/security/RsaSignatureAlgorithm.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
9	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	**CWE:** CWE-295: Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	fr/airweb/grandlac/ui/payment/PaymentActivity.java fr/airweb/grandlac/ui/paymentmethods/PaymentMethodWebViewActivity.java	
10	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		

Showing 1 to 10 of 11 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table									

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Certificate/Key files hardcoded inside the app.	res/raw/td__public_key_preprod.pem res/raw/td__public_key_production.pem

Showing 1 to 1 of 1 entries

Previous 1 Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://ticket-universel.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1045157730205/namespaces/firebase:fetch?key=AIzaSyBnYtBFYRRipQC57z-GMSATXvLqfBji0uM. This is indicated by the response: {'state': 'NO_TEMPLATE'}

Showing 1 to 2 of 2 entries

Previous 1 Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous 1 Next

classes3.dex

Search:

FINDINGS	DETAILS
Compiler	r8

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 3 of 3 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	fr/airweb/grandlac/ui/camera/p003new/a.java
00002	Open the camera and take picture	camera	com/wonderkiln/camerakit/b.java
00003	Put the compressed bitmap data into JSON object	camera	f1/l.java
00004	Get filename and put it to JSON object	file collection	B2/C1294a.java p1/f.java x1/c.java
00009	Put data in cursor to JSON object	file	V1/Q.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	V1/F.java
00012	Read data and put it into a buffer stream	file	C1/C0672f.java
00013	Read file and put it into a stream	file	
00014	Read file into a stream and put it into a JSON object	file	
00015	Put buffer stream (data) to JSON object	file	V1/Q.java

Showing 1 to 10 of 40 entries

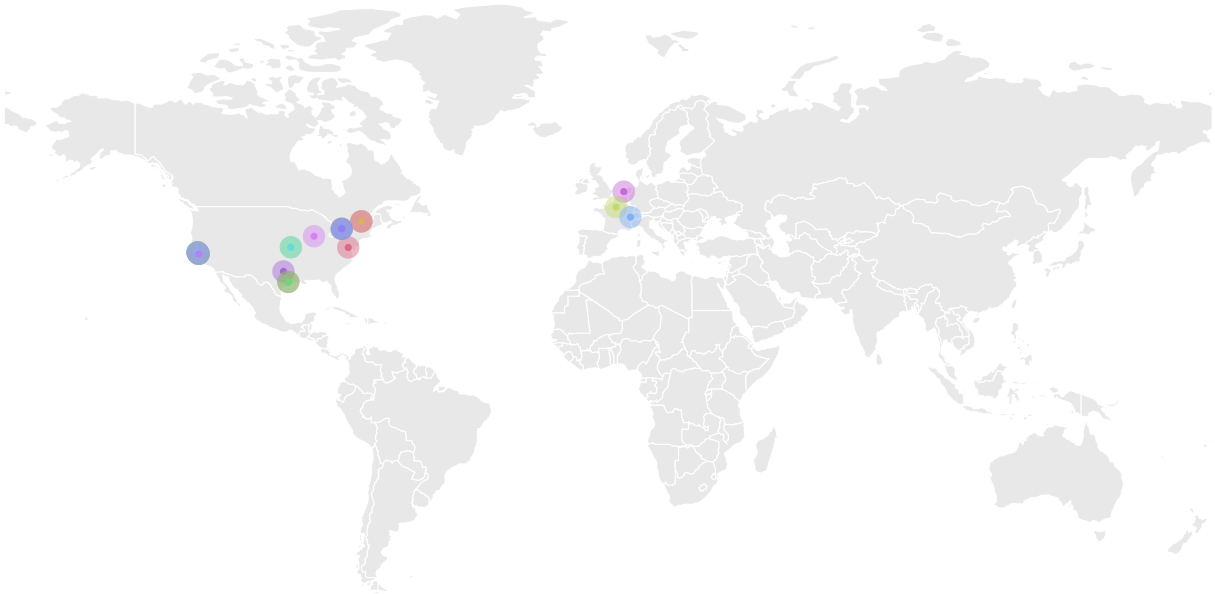
Previous 1 2 3 4 Next

ABUSED PERMISSIONS

Top Malware Permissions	9/25	Other Common Permissions	3/44
android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.WAKE_LOCK		android.permission.CHANGE_NETWORK_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
.facebook.com	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 142.250.31.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.surveymonkey.net	ok	**IP:** 13.225.196.34 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
catp-rtc.airweb.fr	ok	**IP:** 51.15.15.156 **Country:** Netherlands **Region:** Noord-Holland **City:** Haarlem **Latitude:** 52.380840 **Longitude:** 4.636830 **View:** Google Map
data.flurry.com	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.80.8 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
facebook.com	ok	**IP:** 31.13.80.36 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
form.typeform.com	ok	**IP:** 34.194.223.183 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
graph-video.s	ok	No Geolocation information available.

Showing 1 to 10 of 31 entries

Previous 1 2 3 4 Next

URLS

Search:

URL	FILE
data:image	g1/C2074e.java
file:///android_asset/	R6/AbstractC0868a.java
http://www.slf4j.org/codes.html#substitutelogger http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#version_mismatch http://www.slf4j.org/codes.html#unsuccessfulinit http://www.slf4j.org/codes.html#staticloggerbinder http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#loggernamemismatch	Ab/b.java
https://%s/%s/%s	r4/c.java

URL	FILE
https://.facebook.com https://facebook.com	V1/Q.java
https://accounts.google.com https://github.com https://phone.firebase https://twitter.com https://www.facebook.com	K2/j.java
https://accounts.google.com/o/oauth2/revoke?token=	X3/RunnableC3253f.java
https://api.surveymonkey.net/sdk/v1/respondents?api_key=	com/surveymonkey/surveymonkeyandroidsdk/loaders/GetRespondentTaskLoader.java
https://data.flurry.com/v1/flr.do	S2/B.java
https://developers.facebook.com/docs/android/getting-started https://developers.facebook.com/docs/android/getting-started/#client-access-token	V1/S.java

Showing 1 to 10 of 49 entries

Previous 1 2 3 4 5 Next

EMAILS

Search:

EMAIL	FILE
support@airweb.fr	Android String Resource

Showing 1 to 1 of 1 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

Showing 1 to 4 of 4 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **56** secrets

"biometric_secret_key_name" : "a1rw3BKeY|\|@mE"
"com.google.firebase.crashlytics.mapping_file_id" : "6feab716b38541fca3f80f8285e6dded"
"configuration_payment_api" : "MONERIS"
"configuration_survey_monkey_hash" : "undefined"
"firebase_database_url" : "https://ticket-universel.firebaseio.com"
"firebase_web_host" : "CHANGE-ME"
"google_android_map_api_key" : "AIzaSyB1Z__YdBE6G5W6PaT2qsS7bHdrByCSIvU"
"google_api_key" : "AIzaSyBnYtBFYRRipQC57z-GMSATXvLqfBji0uM"
"google_crash_reporting_api_key" : "AIzaSyBnYtBFYRRipQC57z-GMSATXvLqfBji0uM"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"pref_key_camerax_front_camera_target_resolution" : "cfctas"

"pref_key_camerax_rear_camera_target_resolution" : "crctas"
"push_airweb_secret_key" :
"88a69cP2FO60U3oSLwymfmvq7MSwmt1OXtl69nCXZy3r6a57MPwpMSUF52OCaMBAPh523LncGRuPV8m7khYeKP7ZqU1F0u0zlf3gKO651BetNLcg2BEawU6h4dn2zXpQ"
"ticket_facebook_client_token" : "fb96fc76ccf517c1a94f8bd5d5f442c2"
c64b7cd61a971e425d1d94e34726a8fd
1fe4854632aed8d5858f2c332c19cb97
uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
e26c4529c2a67ac8272637f646b2485e
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
cAajgxHlj7GTSEIzIYIQxmEloOSoJq7VOaxWHfv72QM=
UZJDjsNp1+4M5x9cbbdflB779y5YRBcV6Z6rBMLIrO4=
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
yNRK8AqsDET5pFSVQtJnscEJBbCYbZ
228acb26340b2d7160e32a3c1b32ee2f
470fa2b4ae81cd56ecbcda9735803434cec591fa
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
SVqWumuteCQHvVIaALrOZXuzVVVeS7f4FGxxu6V+es4=
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
8c9900064ed98b9c704a600146703313
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
031555375bffd76229d3bef40e6cc472
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
cc2751449a350f668590264ed76692694a80308a
aVs0XjIWLkydc11siwoS68B0RXfQOOnbfKzeEsXi9S0a8nJoR2RvOvSsMIBe
IAirwebWalletAlgorithmProtoV5ConfigOverrideRuleEffectType
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
5C09AA5E9EB4AED204229510BF75CB84
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028

291115057151
c56fb7d591ba6704df047fd98f535372fea00211
Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw=
9b8f518b086098de3d77736f9458a3d2f6f95a37
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

A STRINGS

From APK Resource

▶ Show all **1252** strings

From Code

▶ Show all **26615** strings

From Shared Objects

ACTIVITIES

▼ Showing all **37** activities
fr.airweb.ticket.PrincipalActivity
fr.airweb.grandlac.ui.document.adddocument.AddDocumentActivity
fr.airweb.grandlac.ui.document.viewer.DocumentViewerActivity
fr.airweb.grandlac.ui.camera.new.ImageHandlerActivity
com.canhub.cropper.CropImageActivity
fr.airweb.grandlac.ui.splash.SplashActivity
com.facebook.FacebookActivity
com.facebook.CustomTabActivity
fr.airweb.grandlac.service.login.phone.firebaseui.PhoneActivity
fr.airweb.grandlac.ui.camera.new.FaceCameraActivity
fr.airweb.grandlac.ui.payment.PaymentActivity

fr.airweb.grandlac.ui.paymentmethods.PaymentMethodWebViewActivity
fr.airweb.grandlac.ui.cgv.CGVActivity
com.surveymonkey.surveymonkeyandroidsdk.SMFeedbackActivity
fr.airweb.controlui.ui.TicketPresentationActivity
androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity
androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity
androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity
com.firebase.ui.auth.KickoffActivity
com.firebase.ui.auth.ui.idp.SingleSignInActivity
com.firebase.ui.auth.ui.credentials.CredentialSaveActivity
com.firebase.ui.auth.ui.email.RecoverPasswordActivity
com.firebase.ui.auth.ui.email.EmailActivity
com.firebase.ui.auth.ui.phone.PhoneActivity
com.firebase.ui.auth.ui.idp.WelcomeBackIdpPrompt
com.firebase.ui.auth.ui.email.WelcomeBackPasswordPrompt
com.firebase.ui.auth.ui.email.WelcomeBackEmailLinkPrompt
com.firebase.ui.auth.ui.email.EmailLinkCatcherActivity
com.firebase.ui.auth.ui.email.EmailLinkErrorRecoveryActivity
com.firebase.ui.auth.ui.idp.AuthMethodPickerActivity
com.google.mlkit.vision.codescanner.internal.GmsBarcodeScanningDelegateActivity
com.facebook.CustomTabMainActivity
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
com.google.firebase.auth.internal.GenericIdpActivity
com.google.firebase.auth.internal.RecaptchaActivity
com.google.android.gms.common.api.GoogleApiActivity
com.journeyapps.barcodescanner.CaptureActivity

SERVICES

▼ Showing all **11** services
fr.airweb.grandlac.push.MessagingHandlerService
com.google.mlkit.common.internal.MlKitComponentDiscoveryService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.auth.api.fallback.service.FirebaseAuthFallbackService
com.google.firebase.messaging.FirebaseMessagingService

com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
androidx.room.MultiInstanceInvalidationService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **6** receivers
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver
com.facebook.AuthenticationTokenManager$CurrentAuthenticationTokenChangedBroadcastReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
androidx.profileinstaller.ProfileInstallReceiver

PROVIDERS

▼ Showing all **8** providers
androidx.core.content.FileProvider
com.canhub.cropper.CropFileProvider
com.firebase.ui.auth.data.client.AuthUiInitProvider
com.google.mlkit.common.internal.MlKitInitProvider
com.google.firebase.provider.FirebaseInitProvider
com.facebook.internal.FacebookInitProvider
androidx.startup.InitializationProvider
com.flurry.android.agent.FlurryContentProvider

LIBRARIES

▼ Showing all **3** libraries

org.apache.http.legacy
androidx.window.extensions
androidx.window.sidecar

SBOM

▼ Showing all **78** Versioned Packages

androidx.activity:activity-ktx@1.8.0
androidx.activity:activity@1.8.0
androidx.annotation:annotation-experimental@1.3.0
androidx.appcompat:appcompat-resources@1.6.1
androidx.appcompat:appcompat@1.6.1
androidx.arch.core:core-runtime@dynamic
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.biometric:biometric@1.2.0-alpha04
androidx.browser:browser@1.3.0
androidx.camera:camera-camera2@1.1.0-alpha04
androidx.camera:camera-core@1.1.0-alpha04
androidx.camera:camera-lifecycle@1.1.0-alpha04
androidx.camera:camera-view@1.0.0-alpha24
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.9.0
androidx.core:core@1.9.0
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@8.7.3
androidx.documentfile:documentfile@1.0.1
androidx.drawerlayout:drawerlayout@1.1.1
androidx.dynamicanimation:dynamicanimation@1.0.0
androidx.emoji2:emoji2-views-helper@1.2.0
androidx.emoji2:emoji2@1.2.0
androidx.exifinterface:exifinterface@1.3.3
androidx.fragment:fragment-ktx@1.5.4
androidx.fragment:fragment@1.5.4
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0

androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-extensions@2.2.0
androidx.lifecycle:lifecycle-livedata-core-ktx@dynamic
androidx.lifecycle:lifecycle-livedata-core@dynamic
androidx.lifecycle:lifecycle-livedata@dynamic
androidx.lifecycle:lifecycle-process@dynamic
androidx.lifecycle:lifecycle-runtime-ktx@dynamic
androidx.lifecycle:lifecycle-runtime@dynamic
androidx.lifecycle:lifecycle-service@dynamic
androidx.lifecycle:lifecycle-viewmodel-ktx@dynamic
androidx.lifecycle:lifecycle-viewmodel-savedstate@dynamic
androidx.lifecycle:lifecycle-viewmodel@dynamic
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.navigation:navigation-common-ktx@2.5.3
androidx.navigation:navigation-common@2.5.3
androidx.navigation:navigation-fragment-ktx@2.5.3
androidx.navigation:navigation-fragment@2.5.3
androidx.navigation:navigation-runtime-ktx@2.5.3
androidx.navigation:navigation-runtime@2.5.3
androidx.navigation:navigation-ui-ktx@2.5.3
androidx.navigation:navigation-ui@2.5.3
androidx.print:print@1.0.0
androidx.profileinstaller:profileinstaller@1.3.0
androidx.recyclerview:recyclerview@1.1.0
androidx.room:room-runtime@2.5.0
androidx.room:room-rxjava2@2.5.0
androidx.savedstate:savedstate-ktx@1.2.1
androidx.savedstate:savedstate@1.2.1
androidx.slidingpanelayout:slidingpanelayout@1.2.0
androidx.sqlite:sqlite-framework@2.3.0
androidx.sqlite:sqlite@2.3.0
androidx.startup:startup-runtime@1.1.1
androidx.swiperefreshlayout:swiperefreshlayout@1.1.0
androidx.tracing:tracing@1.0.0
androidx.transition:transition@1.4.1

androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.1
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0
androidx.window:window@1.0.0
com.google.android.material:material@1.11.0
com.google.dagger:dagger@2.53
org.jetbrains.kotlinx:kotlinx-coroutines-android@1.6.4
org.jetbrains.kotlinx:kotlinx-coroutines-core@1.6.4

▶ Show all **696** Packages

FILES

▶ Show all **2750** files

Version v4.4.3