

FILE INFORMATION

File Name Homeless Resources-Shelter App_2.0.11_APKPure.xapk

Size 7.04MB

MD5 fef5c6f07d6528452c72c3fbc394547c

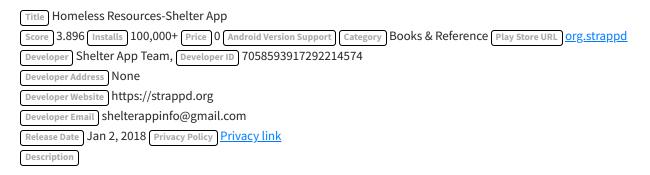
SHA1 45e3e5faa76a5c109664ce7c90d8ec18ded914e8

SHA256 5095d27e868042a3ec014c0189ab0eb1bb422c1409a1721246eaa5656760b4e2



| App Name ShelterApp |
|---|
| Package Name org.strappd |
| Main Activity org.strappd.MainActivity |
| Target SDK 33 Min SDK 21 Max SDK |
| Android Version Name 2.0.11 Android Version Code 2001 |

▶ PLAYSTORE INFORMATION



Shelter App, Inc. is an All-volunteer Non-Profit Organization that helps Homeless and At-risk Youth connect to services using a mobile app where they can find Food, Shelter, Health, Resources and Work. Our Shelter App(formerly Strappd) has resources for Youth across US and resources for everyone in Colorado and in following Counties/Cities: Los Angeles County, King County(Seattle), Multnomah County(Portland), Orange County, San Bernardino County, Riverside County, San Francisco County, Santa Clara County(San Jose), Alameda County(Oakland), San Diego County and El Paso County.

Shelter App is an AI Powered Chatbot that connects at-risk youth to services like Youth Drop-in Centers, Homeless & Run Away Youth Shelters, LGBT Advocacy and Support Groups, After School Programs, Crisis or Hot lines, Food Banks, Soup Kitchens, Food Pantries, Transitional Housing, Domestic Violence Shelters, Pet Shelters, Rent/Utility Assistance, Affordable Housing Options, Free or Low-cost Medical & Dental Clinics, Mental Health Centers, HIV/STI Testing Centers, Syringe Exchange Programs, Clothing Resources, Free Legal clinics, Hygiene Services, Showers, Restrooms, Homeless and Low-income Family Resources, Education & Employment Assistance Services, Job Training Programs, Life Skills Training, Mentorship & many more resources for Homeless and People in Need.

App Users can switch from List View to Map View and can filter services that are just open from the side menu. Users can click on any service to get details like contact info, transit directions and schedule for that service. Flag button on Home Screen will help you connect to the App Admin or Service Provider for that resource. Users can click on Kudos button to show appreciation for the services they like. If you want to mark any service for future reference, click on the star icon in service detail page to add them to My Favorites.

If you are doing community service and interested in listing your service, you can add/manage a service by signing up in the app. You can also update the number of beds available for shelters that you manage. All details entered by the service providers will take some time to get approved before getting published in the app. If you have any questions or see information that is not up to date, please report changes using Give Feedback in side menu.

Download our app to find Homeless resources close to you.

3/7

EXPORTED ACTIVITIES

View All

3/5

EXPORTED RECEIVERS

2/7

XPORTED SERVICES

View All 🛡

0 / 4

EXPORTED PROVIDERS

View All 😃

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: 2018-01-02 18:54:22+00:00 Valid To: 2048-01-02 18:54:22+00:00

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

Serial Number: 0x828baf26effd4a58bb47bef2216bdd662f7036ab

Hash Algorithm: sha256

md5: 55cf27a5728da62d79f01713ea9ecd91

sha1: d7e774ab51fcd541789ae2ec429a38abf28bfe02

sha256: efeec86b51841e83d6ea5be3389b6f51f6f3bd1ea700c8b16246258d13dd304b

sha512:

55f89c6eb3c070280cb4ca8a022f67e5fd3489db8c1f910e8c8102261184dfa01e133f1d56fe23dc845e94c5a32588892cda439626a15ad7d1107d2b46c295ba

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 1337545d829fe3911f83199cfeda413e4a41e16b5c2753d6a2c04b42b5a234be

Found 1 unique certificates

≡APPLICATION PERMISSIONS

| Search: | | |
|---------|--|--|

| PERMISSION | STATUS \$ | INFO ♣ | DESCRIPTION | CODE MAPPINGS |
|---|-----------|------------------------------------|--|------------------|
| 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. | |
| 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.INTERNET | normal | full Internet access | Allows an application to create network sockets. | |
| android.permission.READ_APP_BADGE | normal | show app notification | Allows an application to show app icon badges. | |
| android.permission.RECEIVE_BOOT_COMPLETED | normal | automatically start at boot | Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running. | |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. | |

| PERMISSION | STATUS • | INFO ♦ | DESCRIPTION | CODE MAPPINGS |
|---|-----------|--|---|------------------|
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. | |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. | |

Showing 1 to 10 of 27 entries

| Previous | 1 | <u>2</u> | <u>3</u> | Next |
|----------|---|----------|----------|------|
| | | | | |

ANDROID API

Search:

| API • | FILES \$ |
|-----------------------------------|----------|
| Android Notifications | |
| Base64 Decode | |
| Base64 Encode | |
| Crypto | |
| Get Installed Applications | |
| Get Network Interface information | |
| Get Phone Number | |
| Get Running App Processes | |

| 24, 7:12 PM | | | | Static Ana | aiysis | | | | | |
|-------------------------------|-----------|------------|-----------|-------------------|--------------------|-------------------------------------|----------------|---------------------|----------|----------|
| API | | | | | | * | FILES | | | ♦ |
| Get System Service | | | | | | | | | | |
| Get WiFi Details | | | | | | | | | | |
| Showing 1 to 10 of 26 entries | es | | | | | | | | | |
| | | | | | | | <u>Previou</u> | <u>s</u> 1 <u>2</u> | <u>3</u> | Next |
| | | | | | | | | | | |
| ■ BROWSABLE ACTIVITIE | 5 | | | | | | Search: | | | |
| | | | | | | | Jearen. | | | |
| ACTIVITY | | | | * | INTENT | | | | | * |
| com.facebook.CustomTa | bActivity | | | | | s: fbconnect://, ct.org.strappd, | | | | |
| org.strappd.MainActivity | | | | | Scheme Hosts: A | s : shelter://, uth, | | | | |
| Showing 1 to 2 of 2 entries | | | | | | | | | | |
| | | | | | | | | <u>Previous</u> | 1 | Next |
| | | | | | | | | | | |
| △ NETWORK SECURITY | | | | | | | | | | |
| | | | | | | | Search: | | | |
| NO - | SCOPE | ≜ ▼ | SEVERITY | | * | DESCRIPTION | | | | \$ |
| | | | No data a | vailable in table | | | | | | |

Showing 0 to 0 of 0 entries

| <u>Previous</u> | <u>Next</u> |
|-----------------|-------------|
| | |

<u>Previous</u>

□ CERTIFICATE ANALYSIS

| HIGH 0 | | WARNING 1 | | INFO 1 | | |
|---|-------------|--|------------------------|-----------|---------|----|
| | | | | | Search: | |
| TITLE \$ | SEVERITY \$ | DESCRIPTION | | | | \$ |
| Application vulnerable to Janus Vulnerability | warning | Application is signed with v1 only with v1 signature schem vulnerable. | _ | • | • | |
| Signed Application | info | Application is signed with a c | code signing certifica | te | | |
| Showing 1 to 2 of 2 entries | | | | | | |

Q MANIFEST ANALYSIS

| HIGH | WARNING | INFO | SUPPRESSED |
|------|---------|------|------------|
| 1 | 8 | 0 | 0 |
| | | | Search: |

| NO ♦ | ISSUE | SEVERITY \$ | DESCRIPTION | OPTIONS |
|-------------|---|-------------|--|---------|
| 1 | App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21] | high | This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates. | |
| 2 | Activity (com.facebook.react.devsupport.DevSettingsActivity) 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. | |
| 3 | Activity (com.facebook.FacebookActivity) 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. | |
| 4 | Service (io.invertase.firebase.messaging.RNFirebaseMessagingService) is not Protected. [android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. | |
| 5 | Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. | |
| 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 | OPTIONS |
|-------------|---|----------|--|---------|
| 7 | 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. | |
| 8 | 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. | |

| NO ♦ | ISSUE \$ | SEVERITY \$ | DESCRIPTION | OPTIONS \$ |
|-------------|---|-------------|--|------------|
| 9 | Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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. | |

Showing 1 to 9 of 9 entries

Previous 1 Next

</> CODE ANALYSIS

| HIGH | WARNING | INFO | SECURE | SUPPRESSED | |
|------|---------|------|--------|------------|--|
| 0 | 5 | 1 | 0 | 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 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 | com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java | |
| 3 | 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/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/FileUtil.java com/reactnativecommunity/webview/RNCWebViewModule.java | |
| 4 | 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 | | |

| NO ♦ | ISSUE ♦ | SEVERITY • | STANDARDS \$ | FILES \$ | OPTIONS \$ |
|-------------|---|------------|--|-----------------------------------|------------|
| 5 | 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 | | |
| 6 | Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. | warning | CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG- PLATFORM-7 | bolts/WebViewAppLinkResolver.java | |

Showing 1 to 6 of 6 entries

Previous 1 Next

M SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

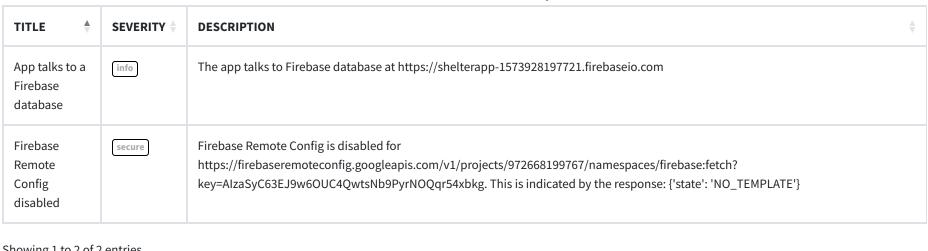
| | | | | | | | | Search: | |
|----------------------------|------------------|-------|-------|-----------------|-------|---------|---------|---------|---------------------|
| NO * | SHARED OBJECT | NX \$ | PIE * | STACK CANARY | RELRO | RPATH • | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
| No data available in table | | | | | | | | | |

Showing 0 to 0 of 0 entries

<u>Previous</u> <u>Next</u>

■ NIAP ANALYSIS v1.3

| | | | | | | | Search: | | |
|----------------------------|----------------------------|----------|-------------|----------------------|---------|-------|-------------|-----------------|-------------|
| NO \$ | IDENTIFIER | * | REQUIREMENT | \$ | FEATURE | \$ | DESCRIPTION | | * |
| No data available in table | | | | | | | | | |
| Showing 0 to 0 of 0 |) entries | | | | | | | | |
| | | | | | | | | <u>Previous</u> | Next |
| | | | | | | | | | |
| FILE ANALYSIS | | | | | | | | | |
| | | | | | | | Search: | | |
| NO | A V | ISSUE | | | A V | FILES | | | Å |
| | | | No data | a available in table | | | | | |
| Showing 0 to 0 of 0 |) entries | | | | | | | | |
| | | | | | | | | Previous | <u>Next</u> |
| | | | | | | | | | |
| FIREBASE DATA | FIREBASE DATABASE ANALYSIS | | | | | | | | |
| | | | | | | | Search: | | |



Showing 1 to 2 of 2 entries

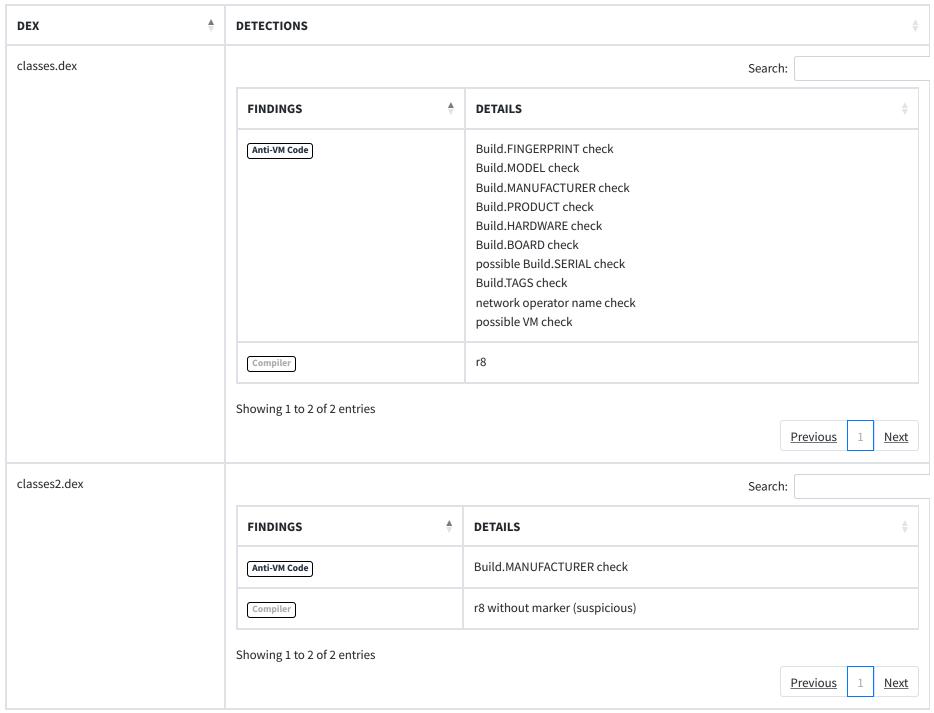


⊘ MALWARE LOOKUP



MAPKID ANALYSIS

| arch: | Searc |
|-------|-------|
| arch: | Searc |



| <u>Previous</u> | 1 | <u>Next</u> | |
|-----------------|---|-------------|--|
| | | | |

BEHAVIOUR ANALYSIS

Search:

| RULE ID 🌲 | BEHAVIOUR . | LABEL \$ | FILES \$ |
|-----------|---|------------------------|---|
| 00001 | Initialize bitmap object and compress data (e.g. JPEG) into bitmap object | camera | com/airbnb/android/react/maps/ImageUtil.java |
| 00009 | Put data in cursor to JSON object | file | com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java |
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | me/leolin/shortcutbadger/impl/SamsungHomeBadger.java |
| 00013 | Read file and put it into a stream | file | |
| 00022 | Open a file from given absolute path of the file | file | |
| 00030 | Connect to the remote server through the given URL | network | bolts/WebViewAppLinkResolver.java io/invertase/firebase/notifications/DisplayNotificationTask.java |
| 00036 | Get resource file from res/raw directory | reflection | |
| 00038 | Query the phone number | collection | com/learnium/RNDeviceInfo/RNDeviceModule.java |
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | bolts/AppLinkNavigation.java |
| 00062 | Query WiFi information and WiFi Mac Address | wifi collection | com/learnium/RNDeviceInfo/RNDeviceModule.java |

Showing 1 to 10 of 30 entries

Previous 1 2 3 Next

SERVER LOCATIONS



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

DOMAIN

COUNTRY/REGION

No data available in table

Showing 0 to 0 of 0 entries

<u>Previous</u> <u>Next</u>

Q DOMAIN MALWARE CHECK

| DOMAIN . | STATUS . | GEOLOCATION \$ |
|---|----------|--|
| api.shelter.app | ok | IP: 44.227.24.210 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| shelterapp-1573928197721.firebaseio.com | ok | IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map |

Showing 1 to 2 of 2 entries

| <u>Previous</u> | 1 | <u>Next</u> |
|-----------------|---|-------------|
| | | |

URLS

| Search: | | |
|---------|--|--|

| URL | * | FILE | * |
|---|---|------------------------------|---|
| https://api.shelter.app https://api.shelter.app/auth/instagram/callback https://api.shelter.app/files | | org/strappd/BuildConfig.java | |

| URL . | FILE \$ |
|---|-----------------------------------|
| https://api.shelter.app https://api.shelter.app/auth/instagram/callback https://shelterapp-1573928197721.firebaseio.com https://api.shelter.app/files | Android String Resource |
| javascript:boltswebviewapplinkresolverresult.setvalue((function() | bolts/WebViewAppLinkResolver.java |

Showing 1 to 3 of 3 entries

| <u>Previous</u> | 1 | <u>Next</u> |
|-----------------|---|-------------|
| | | |

EMAILS

ATRACKERS

Search:

| TRACKER NAME | CATEGORIES | URL \$ |
|---------------------------|----------------|---|
| Facebook Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/66 |
| Facebook Login | Identification | https://reports.exodus-privacy.eu.org/trackers/67 |
| Facebook Places | | https://reports.exodus-privacy.eu.org/trackers/69 |
| Facebook Share | | https://reports.exodus-privacy.eu.org/trackers/70 |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |

Showing 1 to 5 of 5 entries

Previous

Next

<u>ous</u> 1

POSSIBLE HARDCODED SECRETS

▼ Showing all **20** secrets

"FCM_TOKEN": "@fcmToken_shelter"

"GOOGLE_MAPS_APIKEY": "AlzaSyDg2iZZy3zugO2Uo-brrUcfRv6khyQSoKo"

"INSTAGRAM_APP_SECRET": "2e6309f18710a8f2b14acbcf3e000545"

"TWITTER_COMSUMER_KEY": "GkOT1u6XJjPt5eQOWsQOiBTdS"

"TWITTER_CONSUMER_SECRET": "z9OpBbQHCEtLEvyHP9tyZuFx03Xr1mSn8dQDfkX5l3tj1hUW1U"

"WWW_MOBILE_API_URL": "https://api.shelter.app"

"firebase_database_url": "https://shelterapp-1573928197721.firebaseio.com"

"google_api_key": "AlzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg"

"google_crash_reporting_api_key": "AlzaSyC63EJ9w6OUC4QwtsNb9PyrNOQqr54xbkg"

cc2751449a350f668590264ed76692694a80308a

5e8f16062ea3cd2c4a0d547876baa6f38cabf625

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

z9OpBbQHCEtLEvyHP9tyZuFx03Xr1mSn8dQDfkX5l3tj1hUW1U

9b8f518b086098de3d77736f9458a3d2f6f95a37

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

B3EEABB8EE11C2BE770B684D95219ECB

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

2e6309f18710a8f2b14acbcf3e000545

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

A STRINGS

From APK Resource

► Show all **137** strings

From Code

► Show all **13691** strings

From Shared Objects

AE ACTIVITIES

▼ Showing all **7** activities

org.strappd.MainActivity

com.facebook.react.devsupport.DevSettingsActivity

com.facebook.FacebookActivity

com.facebook.CustomTabMainActivity

com.facebook.CustomTabActivity

com.google.android.gms.auth.api.signin.internal.SignInHubActivity

com.google.android.gms.common.api.GoogleApiActivity

Ф° SERVICES

▼ Showing all **7** services

io.invertase.firebase.messaging.RNFirebaseMessagingService
io.invertase.firebase.messaging.RNFirebaseBackgroundMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService



▼ Showing all **5** receivers

com.learnium.RNDeviceInfo.RNDeviceReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver
com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver

PROVIDERS

▼ Showing all **4** providers

com.imagepicker.FileProvider
com.reactnativecommunity.webview.RNCWebViewFileProvider
com.google.firebase.provider.FirebaseInitProvider
com.facebook.internal.FacebookInitProvider

\$LIBRARIES

▼ Showing all **1** libraries org.apache.http.legacy

SBOM

▼ Showing all **30** Versioned Packages androidx.appcompat:appcompat@1.0.2 androidx.arch.core:core-runtime@2.0.0 androidx.asynclayoutinflater:asynclayoutinflater@1.0.0 androidx.browser:browser@1.0.0 androidx.cardview:cardview@1.0.0 androidx.coordinatorlayout:coordinatorlayout@1.0.0 androidx.core:core@1.1.0-rc01 androidx.cursoradapter:cursoradapter@1.0.0 androidx.customview:customview@1.0.0

and roid x. document file: document file @ 1.0.0

androidx.drawerlayout:drawerlayout@1.0.0

androidx.fragment:fragment@1.0.0

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-livedata-core@2.0.0

androidx.lifecycle:lifecycle-livedata@2.0.0

androidx.lifecycle:lifecycle-runtime@2.0.0

androidx.lifecycle:lifecycle-viewmodel@2.0.0

androidx.loader:loader@1.0.0

androidx.localbroadcastmanager:localbroadcastmanager@1.0.0

androidx.media:media@1.0.0

androidx.print:print@1.0.0

androidx.slidingpanelayout:slidingpanelayout@1.0.0

androidx.swiperefreshlayout:swiperefreshlayout@1.1.0-alpha02

androidx.vectordrawable:vectordrawable-animated@1.0.0

androidx.vectordrawable:vectordrawable@1.0.1

androidx.versionedparcelable:versionedparcelable@1.1.0-rc01

androidx.viewpager:viewpager@1.0.0

▼ Showing all 22 Packages

bolts

co.apptailor.googlesignin

com.AlexanderZaytsev.RNI18n

com.agontuk.RNFusedLocation

com.airbnb.android.react.maps

com.imagepicker

com.learnium.RNDeviceInfo

com.lugg.ReactNativeConfig

com.oblador.vectoricons

com.reactnativecommunity.asyncstorage

com.reactnativecommunity.webview

com.swmansion.gesturehandler

im.shimo.react.cookie

io.invertase.firebase

javax.annotation

javax.inject

me.leolin.shortcutbadger okio org.devio.rn.splashscreen org.intellij.lang.annotations org.jetbrains.annotations org.strappd

FILES

► Show all **391** files

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

Version v4.2.5