ANDROID STATIC ANALYSIS REPORT

app_icon

TraKit (1.0)

File Name:	app-debug.apk
Package Name:	za.co.varsitycollege.st10204902.opsc7311poe
Scan Date:	Aug. 17, 2024, 10:07 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
2	9	1	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 9.98MB
MD5: f9948e0358724573863171115bf7eff3
SHA1: 1bf9bc184eb5214bf74d0e5caad387b6b3943b52
SHA256: 97ab80e81bfdec5353910f755c65a643428784ccf08e5155e14182846c578ea1

APP INFORMATION

App Name: TraKit
Package Name: za.co.varsitycollege.st10204902.opsc7311poe
Main Activity: za.co.varsitycollege.st10204902.opsc7311poe.views.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 14
Services: 1
Receivers: 1
Providers: 3
Exported Activities: 2
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-03-06 14:06:05+00:00
Valid To: 2054-02-27 14:06:05+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 988efe92ede32b68d45d7256a9991717
sha1: 7135cee6011ec42122f2a66a7a6d77d9f1bc8149
sha256: c7002899bbe80ae1e8bb66691f21932b4669351e9b000b20847716dc2d8420c5
sha512: 6c1336f69a981ccf59a6c7db5ac194728ab9a011e60f630075dae81cd1c445be97e0a14ee795a029867b7b689e5bd8fb5118c4851db336c4a425eeb0ff04a3b6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6a3e0d4c76c44976ce8a0474c7096d66933d7115d4956d4290b4ec5267e9b368
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
za.co.varsitycollege.st10204902.opsc7311poe.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></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>
<tr><td>classes3.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>
<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>
<tr><td>classes4.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>
<tr><td>classes6.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>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</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
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: **1** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.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.
5	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.
6	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: **0** | WARNING: **3** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/anychart/AnyChartView.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java defpackage/SettingsFragment$onViewCreated$3$1$1$1$1$1.java defpackage/SettingsFragment$onViewCreated$3$1$1$1$1$2.java defpackage/SettingsFragment$onViewCreated$5$1$1$1.java defpackage/SettingsFragment$onViewCreated$5$1$1$2.java defpackage/SettingsFragment$updateUser$1.java defpackage/SettingsFragment$updateUser$2.java za/co/varsitycollege/st10204902/opsc7311poe/ChartFragmentReportPage$setupProjectChips$2.java za/co/varsitycollege/st10204902/opsc7311poe/HomeFragment$onViewCreated$2$2.java za/co/varsitycollege/st10204902/opsc7311poe/HomeProjectsFragment$fetchDailyGoals$2.java za/co/varsitycollege/st10204902/opsc7311poe/HomeProjectsFragment$fetchProjects$1.java za/co/varsitycollege/st10204902/opsc7311poe/HomeProjectsFragment$fetchProjects$2.java za/co/varsitycollege/st10204902/opsc7311poe/HomeProjectsFragment$updateProgressBar$1$2.java za/co/varsitycollege/st10204902/opsc7311poe/HomeProjectsFragment.java za/co/varsitycollege/st10204902/opsc7311poe/HomeTasksFragment$fetchProjects$2.java za/co/varsitycollege/st10204902/opsc7311poe/classes/DBManager$deleteUserAccount$2.java za/co/varsitycollege/st10204902/opsc7311poe/classes/DBManager$deleteUserAccount$3.java za/co/varsitycollege/st10204902/opsc7311poe/classes/DBManager$getUserFromDatabase$1.java za/co/varsitycollege/st10204902/opsc7311poe/classes/DBManager.java za/co/varsitycollege/st10204902/opsc7311poe/views/CreateTaskActivity.java

za/co/varsitycollege/st10204902/opsc7311poe/views/MainActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java za/co/varsitycollege/st10204902/opsc7311poe/classes/User.java
3	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	com/anychart/AnyChartView.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	com/anychart/AnyChartView.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/24	android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET
Other Common Permissions	0/45	

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
github.com	ok	**IP:** 20.87.245.0 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.google.com	ok	**IP:** 142.251.216.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
static.anychart.com	ok	**IP:** 104.236.0.245 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
opsc7311-poe-9be77-default-rtdb.europe-west1.firebasedatabase.app	ok	**IP:** 34.107.226.223 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://opsc7311-poe-9be77-default-rtdb.europe-west1.firebasedatabase.app"
"google_api_key" : "AIzaSyCkCeZNut6A5_otUHk1a_RjBOcSsVTgWVo"
"google_crash_reporting_api_key" : "AIzaSyCkCeZNut6A5_otUHk1a_RjBOcSsVTgWVo"
"password" : "Password"
"username" : "Username"
115792089210356248762697446949407573529996955224135760342422259061068512044369
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
af60eb711bd85bc1e4d3e0a462e074eea428a8
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
36864200e0eaf5284d884a0e77d31646
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

POSSIBLE SECRETS
0df80e76aeca7dc40e01e876dca3542b
bae8e37fc83441b16034566b
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573530086143415290314195533631308867097853951

SCAN LOGS

Timestamp	Event	Error

2024-08-17 10:07:59	Generating Hashes	OK
2024-08-17 10:07:59	Extracting APK	OK
2024-08-17 10:07:59	Unzipping	OK
2024-08-17 10:07:59	Getting Hardcoded Certificates/Keystores	OK
2024-08-17 10:08:01	Parsing AndroidManifest.xml	OK
2024-08-17 10:08:01	Parsing APK with androguard	OK
2024-08-17 10:08:02	Extracting Manifest Data	OK
2024-08-17 10:08:02	Performing Static Analysis on: TraKit (za.co.varsitycollege.st10204902.opsc7311poe)	OK
2024-08-17 10:08:02	Fetching Details from Play Store: za.co.varsitycollege.st10204902.opsc7311poe	OK
2024-08-17 10:08:02	Manifest Analysis Started	OK
2024-08-17 10:08:02	Checking for Malware Permissions	OK

2024-08-17 10:08:02	Fetching icon path	OK
2024-08-17 10:08:02	Library Binary Analysis Started	OK
2024-08-17 10:08:02	Reading Code Signing Certificate	OK
2024-08-17 10:08:03	Running APKiD 2.1.5	OK
2024-08-17 10:08:10	Updating Trackers Database....	OK
2024-08-17 10:08:10	Detecting Trackers	OK
2024-08-17 10:08:12	Decompiling APK to Java with jadx	OK
2024-08-17 10:08:33	Converting DEX to Smali	OK
2024-08-17 10:08:33	Code Analysis Started on - java_source	OK
2024-08-17 10:10:05	Android SAST Completed	OK
2024-08-17 10:10:05	Android API Analysis Started	OK

2024-08-17 10:11:39	Android Permission Mapping Started	OK
2024-08-17 10:11:48	Android Permission Mapping Completed	OK
2024-08-17 10:11:49	Finished Code Analysis, Email and URL Extraction	OK
2024-08-17 10:11:49	Extracting String data from APK	OK
2024-08-17 10:11:49	Extracting String data from Code	OK
2024-08-17 10:11:49	Extracting String values and entropies from Code	OK
2024-08-17 10:11:51	Performing Malware check on extracted domains	OK
2024-08-17 10:11:53	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.