Android Mobile Pentest 101

Lecture 9 – Go to the real world

(Or how I ruined my company competition)

Goal: =))

Introduction

- My company host a “walk competition”, but based on the third party app, so... I decide to look at it to see if i can cheat ☺ And thats it!
- *...Just kidding, i reported to the vendor instead, but it still a good case to talk*

Introduction

- App name: P****
- Version: p5.9.2 (download from apkmonk)
- Goal: Go on top and win the company prize ☺
- Icon:

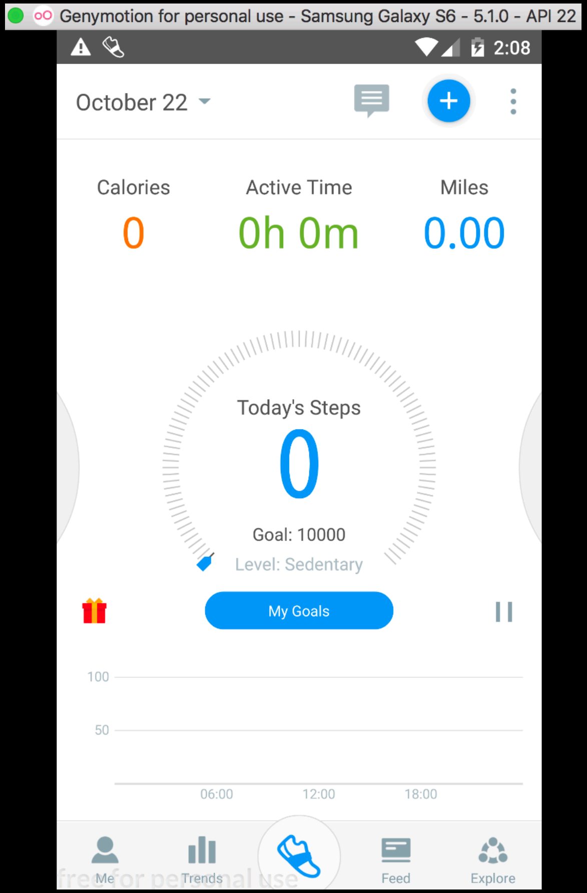
Let’s hack!

- Dynamic Analysis
- Static Analysis

Dynamic Analysis

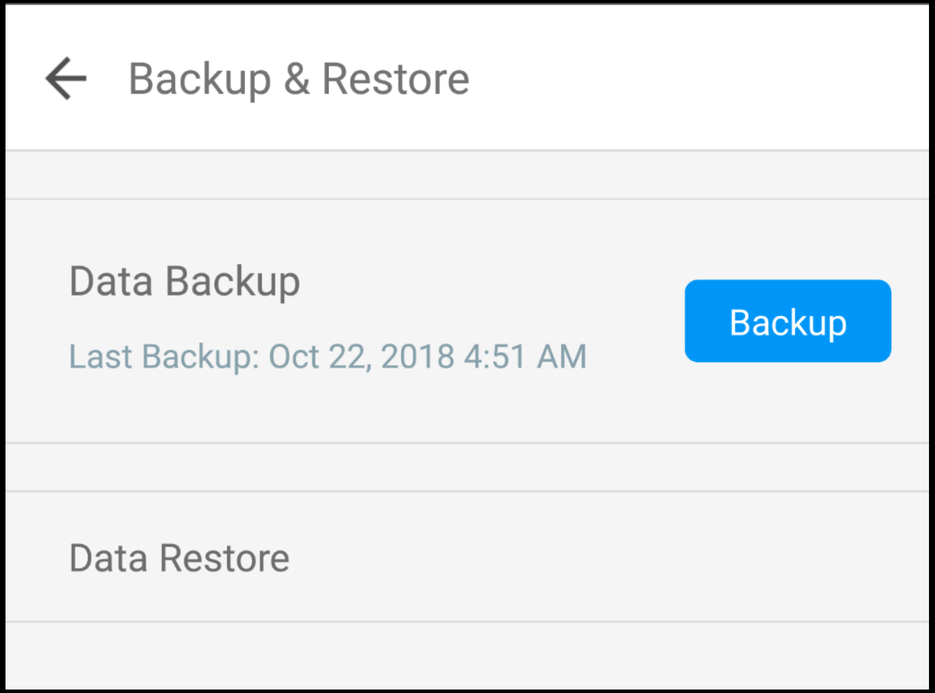
- So we start with dynamic analysis phase, in this phase, we setup burp-suite to intercept all the request then analyse

- Open app, use your account (we will let this account be on top) to login, the app look like this:



Dynamic Analysis

- Using around, the only function that generate a request is backup/restore function



Backup & Restore

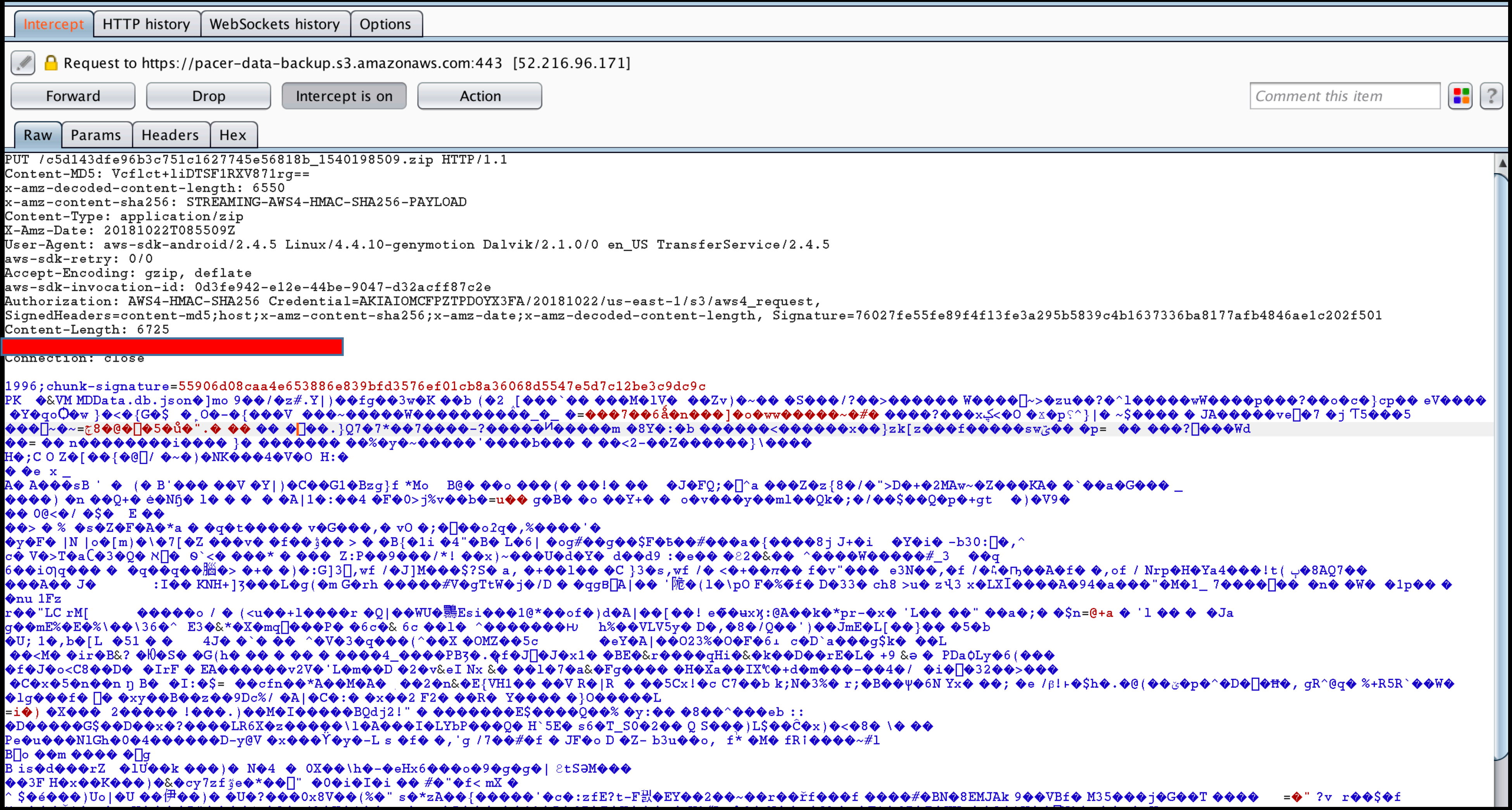
Data Backup

Last Backup: Oct 22, 2018 4:51 AM

Data Restore

Dynamic Analysis

- Let see the request



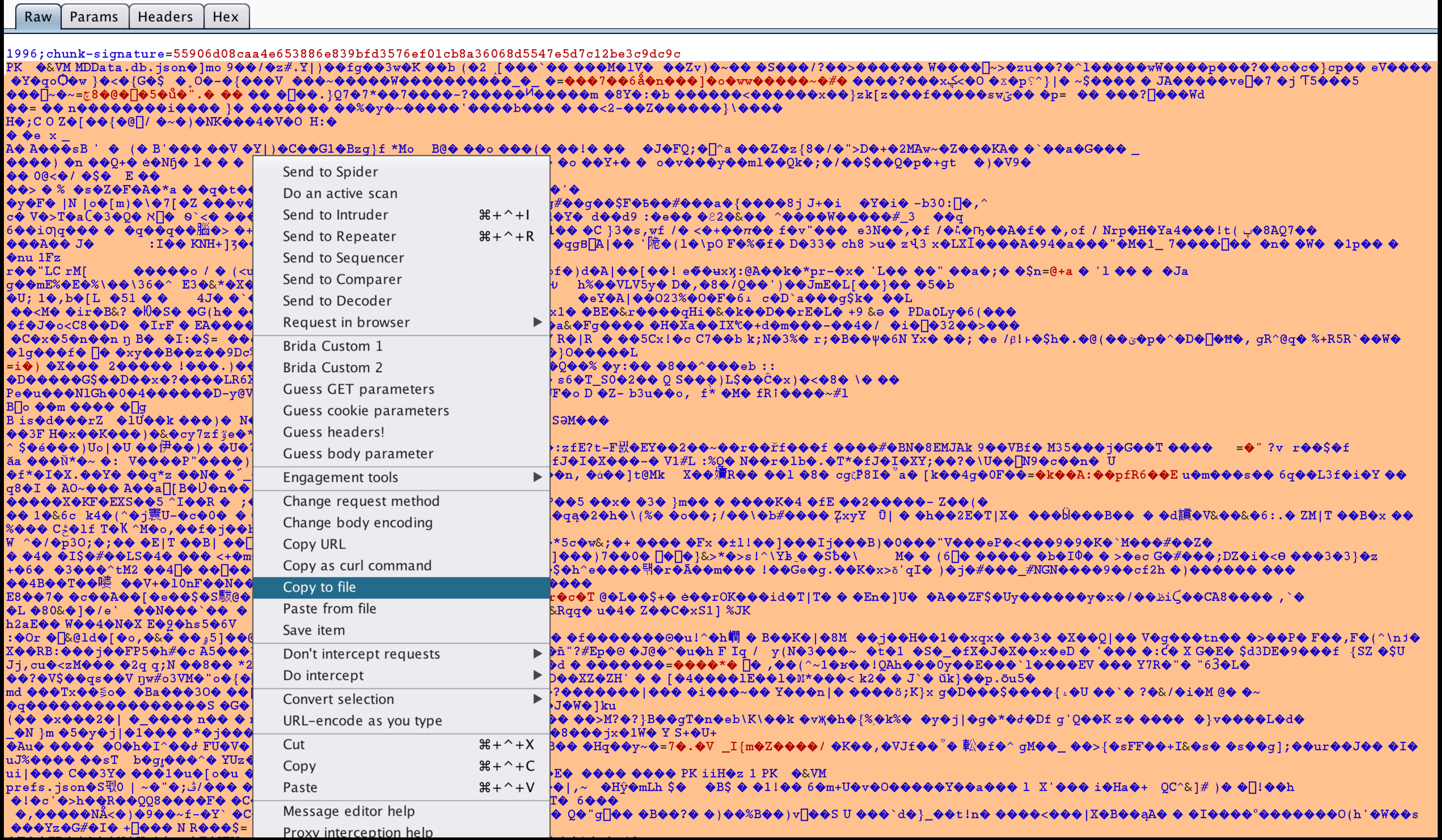
Request to https://pacer-data-backup.s3.amazonaws.com:443 [52.216.96.171]

```
PUT /c5d143dfe96b3c751c1627745e56818b_1540198509.zip HTTP/1.1
Content-MD5: Vcflct+liDTSF1RXV871rg==
x-amz-decoded-content-length: 6550
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD
Content-Type: application/zip
X-Amz-Date: 20181022T085509Z
User-Agent: aws-sdk-android/2.4.5 Linux/4.4.10-genymotion Dalvik/2.1.0/0 en_US TransferService/2.4.5
aws-sdk-retry: 0/0
Accept-Encoding: gzip, deflate
aws-sdk-invocation-id: 0d3fe942-e12e-44be-9047-d32acff87c2e
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOMCFPZTPDOYX3FA/20181022/us-east-1/s3/aws4_request,
SignedHeaders=content-md5;host;x-amz-content-sha256;x-amz-date;x-amz-decoded-content-length, Signature=76027fe55fe89f4f13fe3a295b5839c4b1637336ba8177afb4846ae1c202f501
Content-Length: 6725
[redacted]
Connection: close

1996;chunk-signature=55906d08caa4e653886e839bfd3576ef01cb8a36068d5547e5d7c12be3c9dc9c
PK  �&VM MDData.db.json�]mo 9��/�z#.Y|)��fg��3w�K ��b (�2 [���`�� ���M�1V� ��Zv)�~�� �S���/?��>
```

Dynamic Analysis

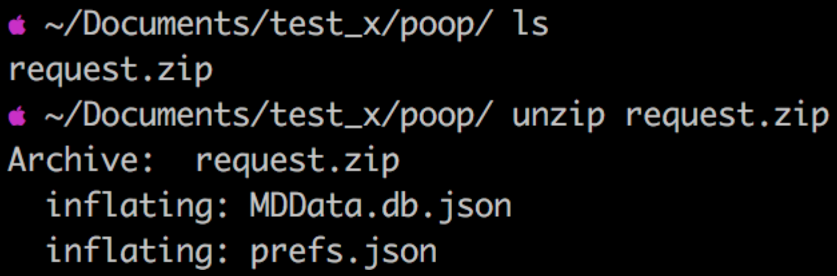
- Large! But, notice the header content of the request, you can see the “PK”, it’s a signature of ZIP file, so we saved the data and extract it to see what it is



```
1996;chunk-signature=55906d08caa4e653886e839bfd3576ef01cb8a36068d5547e5d7c12be3c9dc9c
```

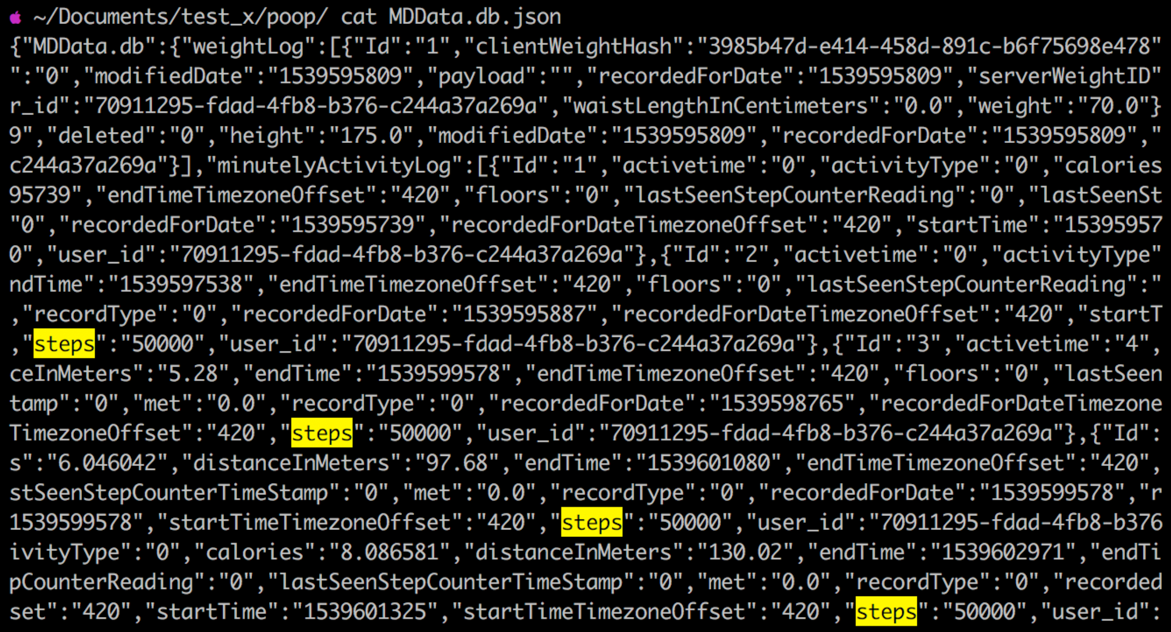
Dynamic Analysis

- Cool! Extracted.



```
~/Documents/test_x/poop/ ls
request.zip
~/Documents/test_x/poop/ unzip request.zip
Archive:  request.zip
  inflating: MDData.db.json
  inflating: prefs.json
```

- Inside it, we can see it sends the steps to server, so modify steps, zip it then paste to burp solve the problem?



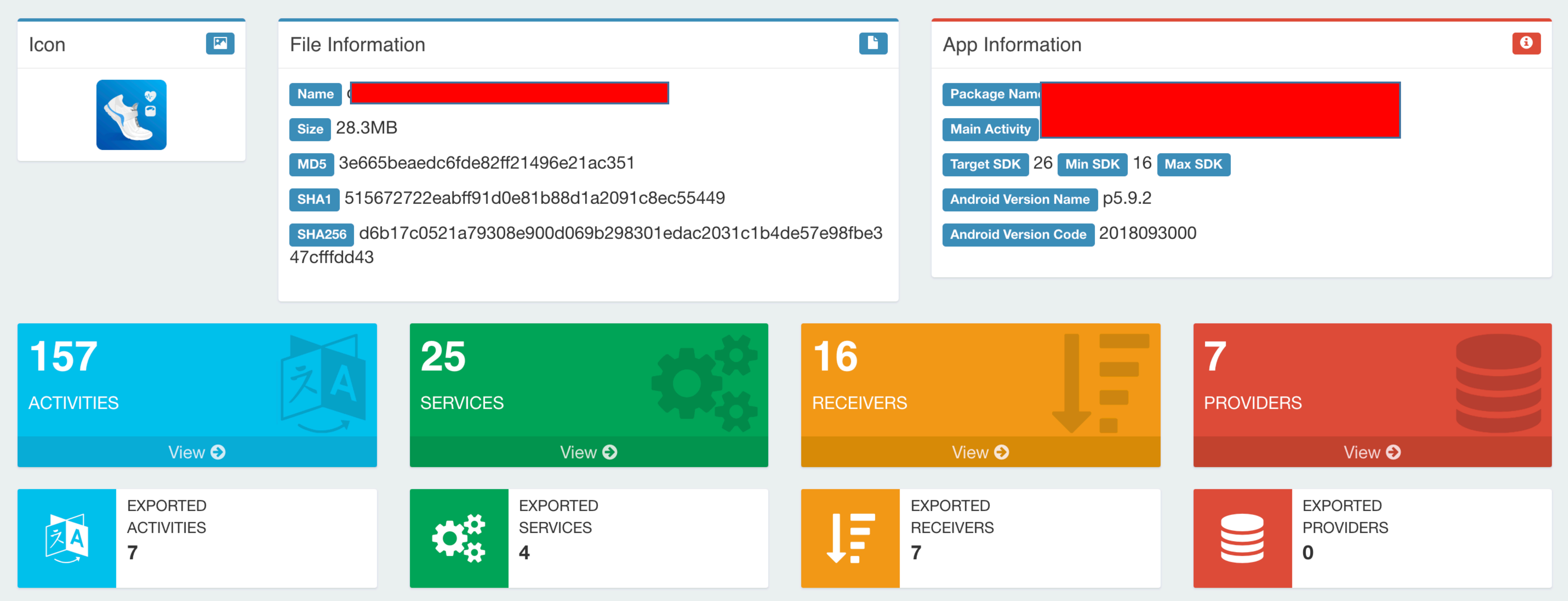
```
~/Documents/test_x/poop/ cat MDData.db.json
{"MDData.db":{"weightLog":[{"Id":"1","clientWeightHash":"3985b47d-e414-458d-891c-b6f75698e478"
":"0","modifiedDate":"1539595809","payload":"","recordedForDate":"1539595809","serverWeightID"
r_id":"70911295-fdad-4fb8-b376-c244a37a269a","waistLengthInCentimeters":"0.0","weight":"70.0"}
9","deleted":"0","height":"175.0","modifiedDate":"1539595809","recordedForDate":"1539595809","
c244a37a269a"}],"minutelyActivityLog":[{"Id":"1","activetime":"0","activityType":"0","calories
95739","endTimeTimezoneOffset":"420","floors":"0","lastSeenStepCounterReading":"0","lastSeenSt
"0","recordedForDate":"1539595739","recordedForDateTimezoneOffset":"420","startTime":"15395957
0","user_id":"70911295-fdad-4fb8-b376-c244a37a269a"},{"Id":"2","activetime":"0","activityType"
ndTime":"1539597538","endTimeTimezoneOffset":"420","floors":"0","lastSeenStepCounterReading":"
,"recordType":"0","recordedForDate":"1539595887","recordedForDateTimezoneOffset":"420","startT
,"steps":"50000","user_id":"70911295-fdad-4fb8-b376-c244a37a269a"},{"Id":"3","activetime":"4",
ceInMeters":"5.28","endTime":"1539599578","endTimeTimezoneOffset":"420","floors":"0","lastSeen
tamp":"0","met":"0.0","recordType":"0","recordedForDate":"1539598765","recordedForDateTimezone
TimezoneOffset":"420","steps":"50000","user_id":"70911295-fdad-4fb8-b376-c244a37a269a"},{"Id":
s":"6.046042","distanceInMeters":"97.68","endTime":"1539601080","endTimeTimezoneOffset":"420",
stSeenStepCounterTimeStamp":"0","met":"0.0","recordType":"0","recordedForDate":"1539599578","r
1539599578","startTimeTimezoneOffset":"420","steps":"50000","user_id":"70911295-fdad-4fb8-b376
ivityType":"0","calories":"8.086581","distanceInMeters":"130.02","endTime":"1539602971","endTi
pCounterReading":"0","lastSeenStepCounterTimeStamp":"0","met":"0.0","recordType":"0","recorded
set":"420","startTime":"1539601325","startTimeTimezoneOffset":"420","steps":"50000","user_id":
```

Dynamic Analysis

- No, the server check hash key based on data, so we have to generate a true key of it if we want to modify the content.
- Seems hard (because of the lots of code), we move to the static analysis phase!

Static Analysis

- To start, I drag the apk file to MobSF to do an automated static analysis



Icon

File Information

Name [redacted]

Size 28.3MB

MD5 3e665beaedc6fde82ff21496e21ac351

SHA1 515672722eabff91d0e81b88d1a2091c8ec55449

SHA256 d6b17c0521a79308e900d069b298301edac2031c1b4de57e98fbe347cfffdd43

App Information

Package Name [redacted]

Main Activity

Target SDK 26 Min SDK 16 Max SDK

Android Version Name p5.9.2

Android Version Code 2018093000

157 ACTIVITIES View

25 SERVICES View

16 RECEIVERS View

7 PROVIDERS View

EXPORTED ACTIVITIES 7

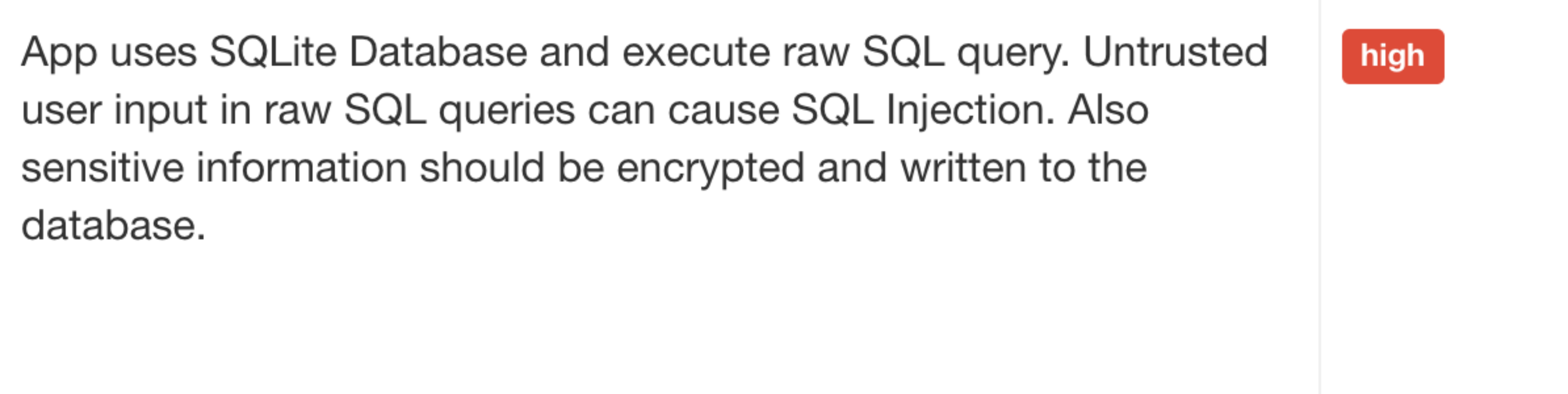
EXPORTED SERVICES 4

EXPORTED RECEIVERS 7

EXPORTED PROVIDERS 0

Static Analysis

- In the code analysis section, this point got my notice:



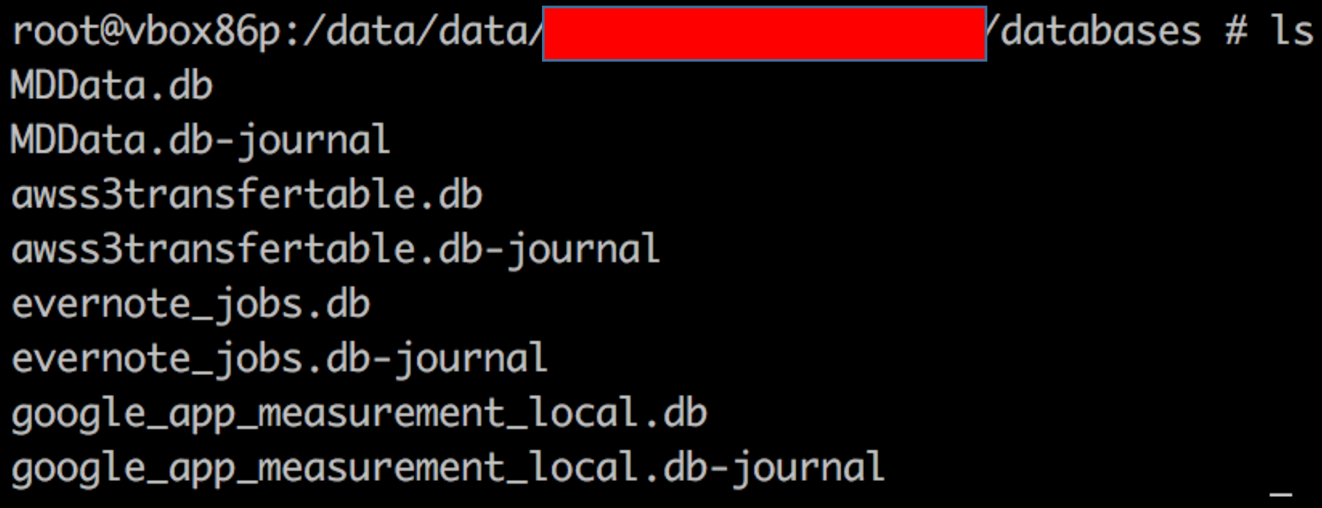
App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.

Static Analysis

- So, let take a look at the sqlite3 databases
- Remember the static analysis lecture? Let install the app, use it to generate some info, then check the database

Static Analysis

- In /data/data/cc.p****.androidapp/databases

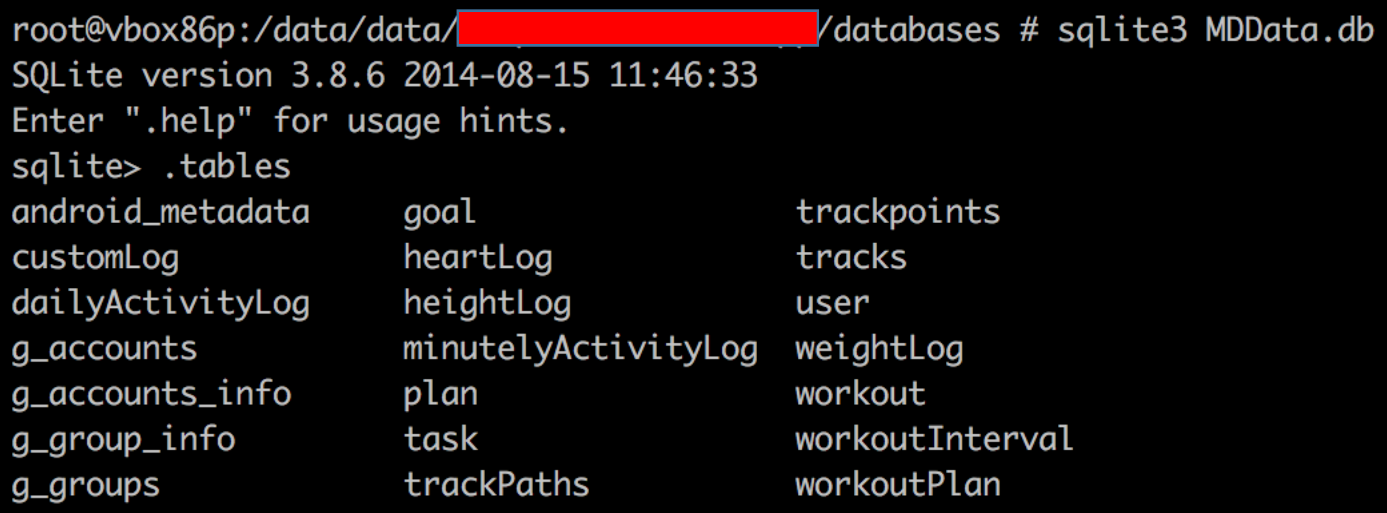


```
root@vbox86p:/data/data/[redacted]/databases # ls
MDData.db
MDData.db-journal
awss3transfertable.db
awss3transfertable.db-journal
evernote_jobs.db
evernote_jobs.db-journal
google_app_measurement_local.db
google_app_measurement_local.db-journal
```

- MDData.db look promising, let check it

Static Analysis

- We can see there are many “Log” based on table name



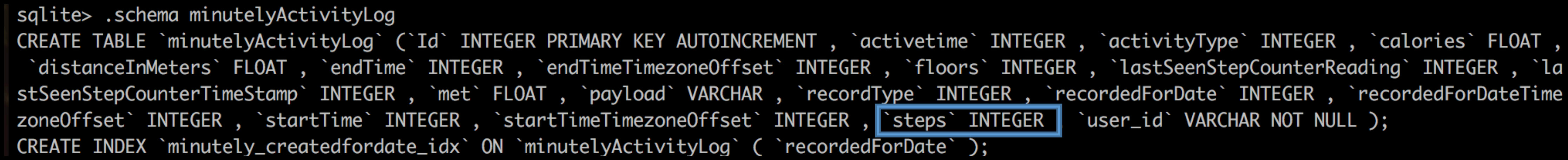
```
root@vbox86p:/data/data/[redacted]/databases # sqlite3 MDData.db
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
android_metadata     goal                 trackpoints
customLog            heartLog             tracks
dailyActivityLog     heightLog            user
g_accounts           minutelyActivityLog  weightLog
g_accounts_info      plan                 workout
g_group_info         task                 workoutInterval
g_groups             trackPaths           workoutPlan
```

- At this stage, let think a bit, We don’t connect to the internet and the app still running, the steps still counting, so how the app saved our step?
- (From the dynamic analysis phase) we can see it sends to server some information about steps, time, blah blah…

=> Absolutely the database is vulnerabled

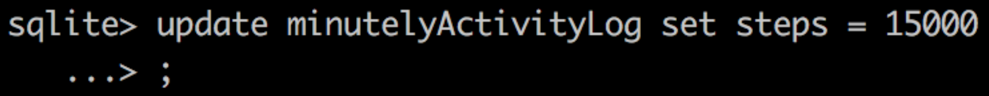
Static Analysis

- I decide to check table minutelyActivityLog



```
sqlite> .schema minutelyActivityLog
CREATE TABLE `minutelyActivityLog` (`Id` INTEGER PRIMARY KEY AUTOINCREMENT , `activetime` INTEGER , `activityType` INTEGER , `calories` FLOAT ,
 `distanceInMeters` FLOAT , `endTime` INTEGER , `endTimeTimezoneOffset` INTEGER , `floors` INTEGER , `lastSeenStepCounterReading` INTEGER , `la
stSeenStepCounterTimeStamp` INTEGER , `met` FLOAT , `payload` VARCHAR , `recordType` INTEGER , `recordedForDate` INTEGER , `recordedForDateTime
zoneOffset` INTEGER , `startTime` INTEGER , `startTimeTimezoneOffset` INTEGER , `steps` INTEGER , `user_id` VARCHAR NOT NULL );
CREATE INDEX `minutely_createdfordate_idx` ON `minutelyActivityLog` ( `recordedForDate` );
```

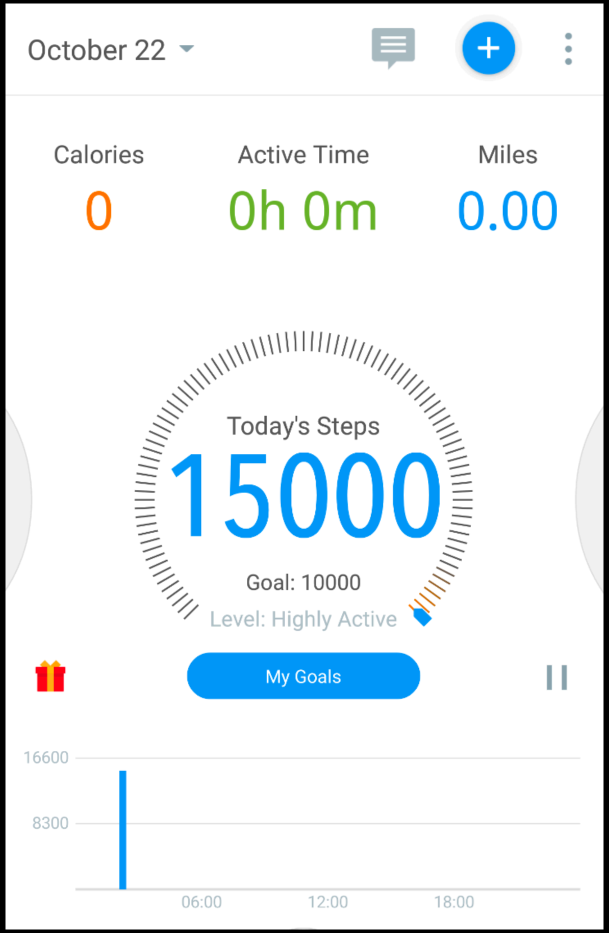
- Column steps? That it! Let change it



```
sqlite> update minutelyActivityLog set steps = 15000
   ...> ;
```

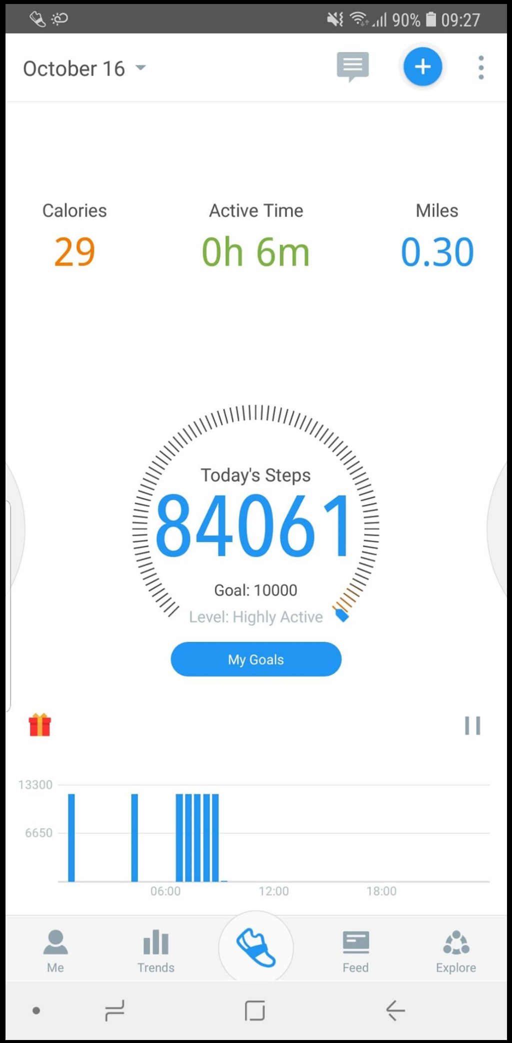
Static Analysis

- Quit app, re-open it (or just click backup after update steps in database immediately)



Static Analysis

- Click on backup function to save our value on cloud
- Come to real phone, click on restore, here the result (result of previous hack, not this time):



October 16

Calories 29

Active Time 0h 6m

Miles 0.30

Today's Steps 84061

Goal: 10000

Level: Highly Active

Static Analysis

- All I need is try hard running on one day, then x7 the result, then fake, ez win ☺

- Just kidding, reported to vendor, then ask them permission to write this lecture…