

Android Mobile Pentest 101

© tsug0d, September 2018

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:

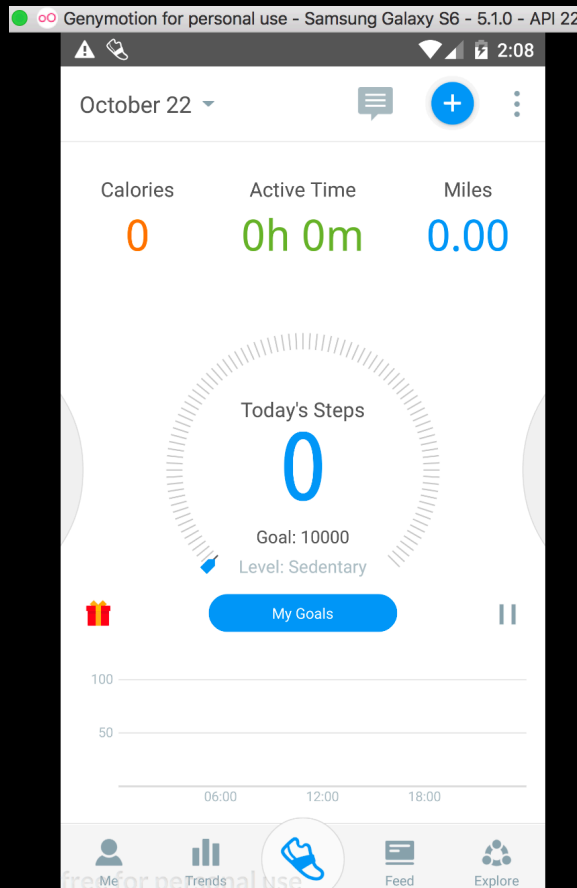


Let's hack!

- Dynamic Analysis
- Static Analysis

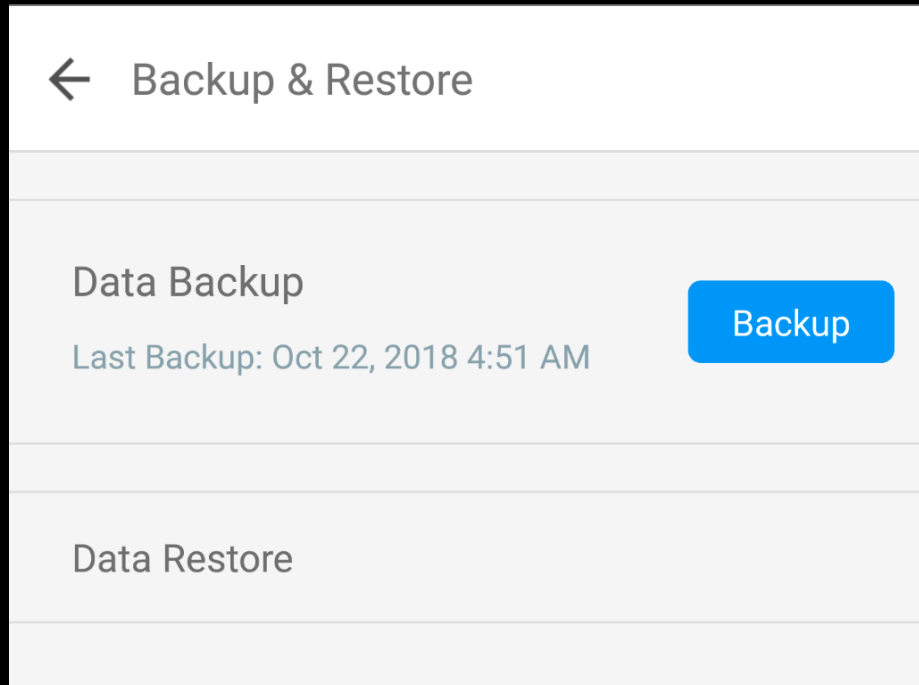
Dynamic Analysis

- 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



Dynamic Analysis

- Let see the request

InterceptHTTP historyWebSockets historyOptions

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

ForwardDropIntercept is onAction

Comment this item

RawParamsHeadersHex

```
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=76027fe55fe89f4f13fe3a295b5839c4b1637336ba8177afb4846a1c202f501
Content-Length: 6725
Connection: close

1996;chunk-signature=55906d08caa4e653886e839bfd3576ef01cb8a36068d5547e5d7c12be3c9dc9c
PK  VM MDData.db.jsonmo 9 /z#.Y|fg3wK b (2 [  S~?>W []~?zu?^1wWp?ooc}cp eV
YqoQw }<{G$  Oo- {V ~W  =76ânn]oovW~#?x<O xps^}| ~$ JAve[]7 j T5
[]~-=g8@[]5â".  []Q7*7?~?I m 8Y: b <x}zk[z fswg p= ?[]Wd
== n n i i  y~' b <2-Z\
H;C O Z [ {[]/ ~  NK4V H:
 x
A A sB ' ( B' V Y|)C G1Bzg}f *Mo B@ o ( ! J FQ; []^a Z z{8 / ">D + 2MAw~ Z KA  a G _
) n Q+ é Nj 1  A | l : 4 F O > j v b = u d g B o o Y + o v y m l Q k ; / $ Q p + g t ) V9
0 < / $ E
> % s Z F A a g t v G o , v O ; [] o 2 q , % '
y F [ N | o [ m ] \ 7 [ Z v v v f o f j > B { l i 4 " B L 6 [ o g # g g $ F 5 o # a { 8 j J + i Y i - b 3 0 : [ , ^
c V > T a ( c 3 Q N []  S <  Z : P 9 U o d Y d d d 9 : e 2 2 & ^ e W # _ 3 q
6 i o q q q q 腦 > + + ) : G [ 3 , w f / J J M S ? S a , + + l 1 o C [ 3 s , w f / < o + m f o v " e 3 N o , f / f 7 A a f , o f / N r p H Y a 4 l t ( 8 A Q 7
A A J : I o m K N H + j 3 o r h o o o # V o g T t W o j / D o q g B [ A ] ' 院 ( 1 p O F % % f D o 3 3 c h 8 > u z 4 3 x L X I A o 9 4 a o " M o 1 _ 7 o o o [] n W 1 p
nu l F z
r " L C r M [ o o / ( < u o + l o o o r Q | W U  Es i o o 1 0 * o o f ) d A | [ ! e 6 u x X : @ A k * p r - o x ' L o o " a ; $ n = @ + a ' 1 o o Ja
g o o m E % E % \ o o \ 3 6 ^ E 3 & * X o m q [ o P o 6 c & 6 c o o l 1 ^ o o o o o H u h % V L V 5 y D o , 8 / Q o ' ) J m E L [ o ] o 5 b
U ; 1 o , b [ L 5 1 o 4 J o o o ^ V o 3 q o o ( ^ X X O M Z o 5 s e Y A [ o o 2 3 % O o F 6 i c D a a o g $ k o L
o M o i r o B ? o 0 S o G ( h o o o o o 4 o o o o P B 3 o , f i J J J x 1 B E o & r o o o q H i o & k o D o r E o L o + 9 & e P D a o L y 6 ( o o
f o J o < C 8 o D o o I r F o E A o o o o v 2 V ' L o m o D 2 o v & e I N x & o o 1 7 o a & F g o o o o H o X a o o I X ' o + d o m o o o - o 4 / i o [ o 3 2 o > o o
C o x o 5 o n o n j B o I : o $ = o c f n o * A o o M o A o 2 2 o n & o E { V H i o o V R o | R o o 5 C x ! c C 7 o b k ; N o 3 % r ; B o o p o 6 N Y x o o ; e / p ! : $ h o . o @ ( o o o p o ^ D o [ o H o , g R ^ o q % + R 5 R ` o W o
l g o o f o [ o x y o o B o z o D c % / A | C o : o x o 2 F 2 o o R o Y o o o o } O o o o L
= i o ) X o o o 2 o o o o l o o o . ) o M o I o o o o B Q d j 2 ! " o o o o o o E S o o o Q o % y : o o 8 o o ^ o o o e b : :
D o o o o G S o o D o o o x ? o o o o L R 6 X o z o o o o o l 1 A o o o I o L Y b P o o o o Q H ' 5 E o s 6 T _ S O 2 o o Q S o o o ) L S o o o C o x ) < o 8 \ o o
P e o u o o o N l G h o 0 4 o o o o o o D - y @ V x o o o Y o y - L s o f o , ' g / 7 o o # o f J F o o D o Z - b 3 u o o , f * M o f r i o o o o ~ # 1
B [ o o m o o o [] g
B i s d o o o r z U o o k o o o ) N o 4 O X o o \ h o - e H x 6 o o o o o 9 o g o g | @ t S 9 M o o o
o 3 F H o x o o K o o o ) & o c y 7 z f j e o * o o [] o o i o I o i o # o " o f < m X
^ $ o é o o [ U o | U o o [ o o ) o U o ? o o o o x 8 V o o ( % " s o * z A o o { o o o o ' c o : z f E ? t - F 馱 o E Y o o 2 o o ~ o o r o o F f o o o f o o o o # o B N o 8 E M J a k 9 o o V B o M 3 5 o o o o j o G o o T o o o = o " ? v r o o $ o f
```


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

The screenshot shows a network traffic analysis tool with a 'Raw' tab selected. The data is displayed in hexadecimal. A context menu is open over the data, listing various actions. The data itself contains a 'PK' signature, which is a common header for ZIP files.

Action	Shortcut
Send to Spider	
Do an active scan	
Send to Intruder	⌘+^+I
Send to Repeater	⌘+^+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Request in browser	
Brida Custom 1	
Brida Custom 2	
Guess GET parameters	
Guess cookie parameters	
Guess headers!	
Guess body parameter	
Engagement tools	
Change request method	
Change body encoding	
Copy URL	
Copy as curl command	
Copy to file	
Paste from file	
Save item	
Don't intercept requests	
Do intercept	
Convert selection	
URL-encode as you type	
Cut	⌘+^+X
Copy	⌘+^+C
Paste	⌘+^+V
Message editor help	
Proxy interception help	

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","recordedForDateTmezoneOffset":"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","recordedForDateTmezoneOffset":"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","recordedForDateTmezone
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

Size

MD5

SHA1

SHA256

28.3MB

3e665beaedc6fde82ff21496e21ac351

515672722eabff91d0e81b88d1a2091c8ec55449

d6b17c0521a79308e900d069b298301edac2031c1b4de57e98fbe347cffffdd43

App Information

Package Name

Main Activity

Target SDK

Min SDK

Max SDK

Android Version Name

Android Version Code

26

16

p5.9.2

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.

high

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`

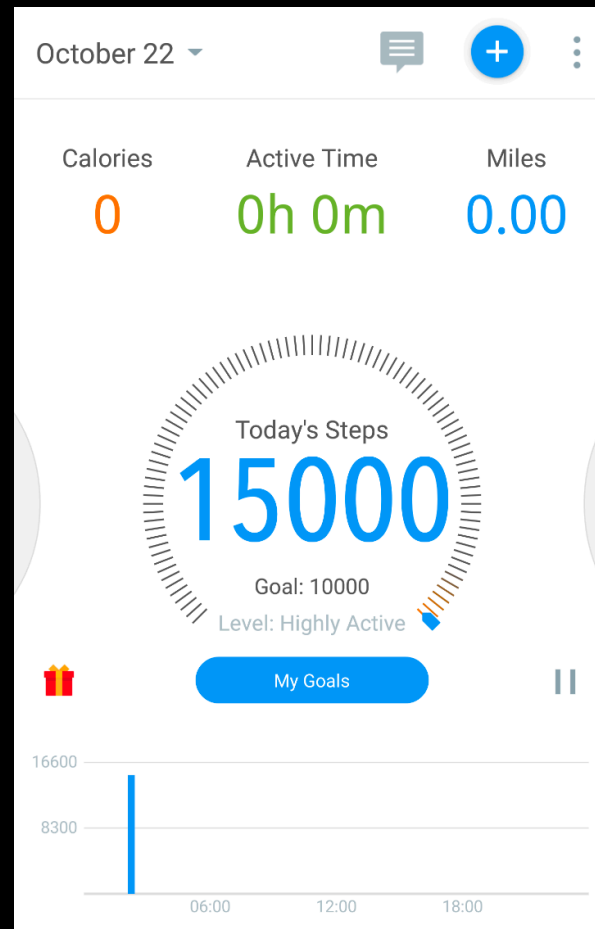
```
sqlite> .schema minutelyActivityLog
CREATE TABLE `minutelyActivityLog` (`Id` INTEGER PRIMARY KEY AUTOINCREMENT , `activetime` INTEGER , `activityType` INTEGER , `calories` FLOAT ,
`distanceInMeters` FLOAT , `endTime` INTEGER , `endTimeTimezoneOffset` INTEGER , `floors` INTEGER , `lastSeenStepCounterReading` INTEGER , `lastSeenStepCounterTimeStamp` INTEGER , `met` FLOAT , `payload` VARCHAR , `recordType` INTEGER , `recordedForDate` INTEGER , `recordedForDate`
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):



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...