

# Android Mobile Pentest 101

*© tsug0d, September 2018*

# Bài 9 – Hack đồ thiết

(Hoặc là mình đã quậy cuộc thi của công ty như nào)

Mục tiêu: =))

# Introduction

- Công ty mình tổ chức cuộc thi “chạy” để khuyến khích nhân viên đi nhiều hơn, win thì được 700k/tuần, 2 triệu/tháng, cơ mà lại tổ chức dựa trên 1 cái app của bên thứ 3, nên mình quyết định ngó lẹ qua cái app xem hack được hông, được luôn mới ghê 😊
- ...Đùa hoy, report rồi.

# Introduction

- App name: P\*\*\*\*
- Version: p5.9.2 (download from apkmonk)
- Goal: lên đỉn và lấy tiền 😊
- Icon:

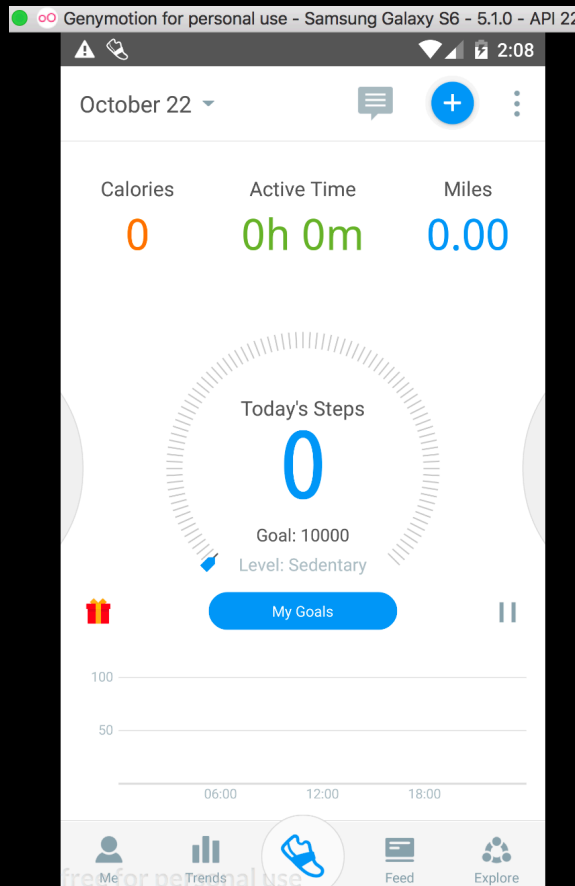


# Let's hack!

- Dynamic Analysis
- Static Analysis

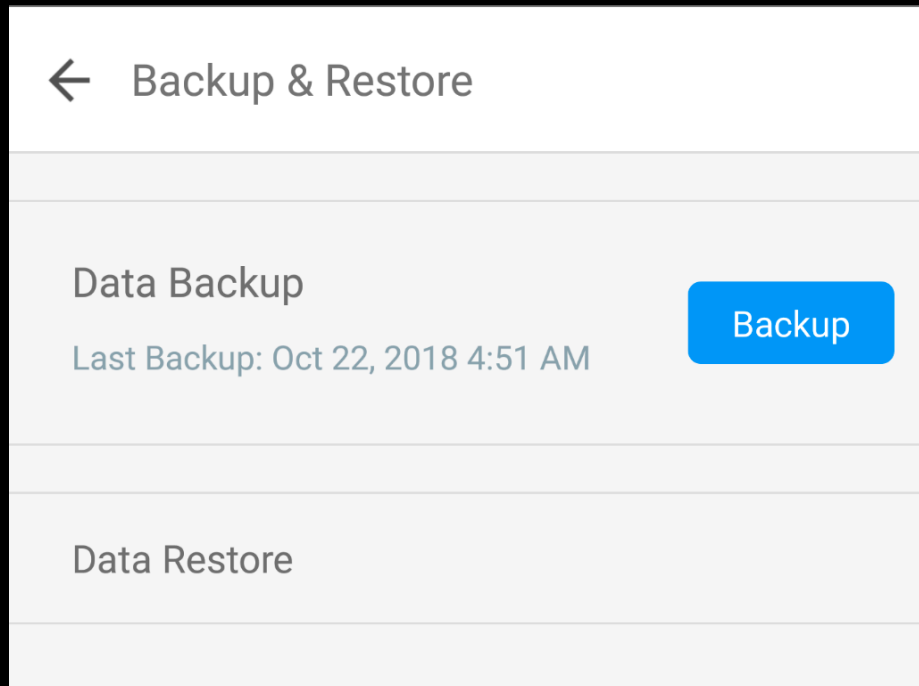
# Dynamic Analysis

- Chúng ta sẽ bắt đầu bằng phân tích động, **setup burp-suite để bắt hết request gửi lên** rồi phân tích
- Mở app lên, login bằng account mình ( account này sẽ lên top), app sẽ nhìn như vậy



# Dynamic Analysis

- Sử dụng quanh quanh, thấy chỉ có mỗi function `backup/restore` là có sinh request



- Xem thử request

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

Forward

Drop

Intercept is on

Action

Comment this item

Raw

Params

Headers

Hex

PUT /c5d143dfef96b3c751cl627745e56818b\_1540198509.zip HTTP/1.1  
Content-MD5: Vcf1ct+liDTSF1RXV87lrg==  
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/O en\_US TransferService/2.4.5  
aws-sdk-retry: 0/0  
Accept-Encoding: gzip, deflate  
aws-sdk-invocation-id: Od3fe942-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=76027fe55fe89f4f13fe3a295b5839c4b1637336ba8177afb4846aelc202f501  
Content-Length: 6725

Connection: close

1996;chunk-signature=55906d08caa4e653886e839bfd3576ef01cb8a36068d5547e5d7c12be3c9dc9c  
PK VM MDDData.db.json[mo 9...?z.Y]|o fgo3wqK eB (... \_ [...`M4lVQ ...Zv]~S.../?><W...[]->zuz...^'lwWW...p...?ooc)cp...eV...  
YyGoCw]<{G\$ \$ ,O--{VV ~~~~~W..... =76ânnn}oovw...-#...?xx<cO z,p'^}| -S... JA...ve[] j T5...5  
~~~g8@[]5â'. . red dots []... Q7?7\*??7....m 8Y:b .....<.....x-)zk[z...f.....swg... p= .. ?[]...Wd  
... n... } .....%yo~.....b... <-Z...}\nyN  
H:C O Z[] { @[]/ ~::~NK...4VO H:  
  
 x\_  
A A...sB ' ( B'...V Y| ) CCG1Bgzf \*Mo BCo o ( !... JFQ;[]'a ...Zoz{8/">D++2MAw-Z...KA...'aaGG\_-  
...) nn QQ+ eNG l... BA[l::4 FFO>jvvEb=u d gOB...YO + o v...yomllQQk;/...\$QOp+gt )V9  
0@c// \$ E  
>% sZoFFAA\*a qqtotetttt vGO..., vo :[]o2qq,%...'  
yfJeo[N ]o[m]\7[]j...v... i...> B[i li "4"B L6 | oog#gog#\$Fo500#...a[{...8j J+i yYoi -b30:[], ^  
coVo>Ta(C3Q NM] 9<... \*... Z:P(9.../\*! xx)~UodYY doed9:e ee 82&... ^...W...#\_3 qq  
6...iojqga... qggq...腦> ++)::G[j3[],wf / J]M...\$?S a, ++l... C }3s,wf / <+...π...fov"... e3Ne,,of /x{:cO Aaf, ,of / NrpOHYa4!!!!!( \_8AQ7?  
...AA Jo I:o KNH+]3...Log(m GGrh ....#VogTtWo]j/D o ggB[A] ( '阨(1\po Fo%f Dc33 ch8 u c z43 xLXI...A94a...'"M0l\_7...[] nn W 1p...  
nu lfz  
r""LC rM[...] / (<n+l...er Q[]Wwu黑Esi...10\*f...jdA]{}[! eoux[:@Ak\*kpr-x'Le...'' aa;; \$n=@+a 'l JJa  
gmEmE%E%\36^ E3&\*Km[q]...Pe6c&6c ...l h%VLV5yD De,8/Q('')JmEL[]}]...5ob  
U; l,b[L 51 4J... V3qgq(... X OMZ...sc eyYA[]O23%OOFF61 c'D'a'logSk LL  
..M irBB? 0US CoG(h...v...4...PB3...fJJ[]Jo x1 BEEr...ghHi&k...DoeReL +9 & PdAoLy6(  
fJJeOCEDDe IrF EA.....v2Yo'LomOd 22v&eI Nx & ol17@a&FG... HoXA...IX'+dm...-44/ i>[]32...>  
Cx×5en nj Bo I:\$= ccfn...\*AMoA 22vn&E[VH1...VR[R ] 55Cxlc C7Cb k;N3%n r;Boψ6NyX... ; e/p!-Sh\$. @((ζop^D[]H\$, gr@gq %R5R`W  
lg...if [] xyxyBOzzz9DC%/ AfCC: ×x2 F2 R Ye... }O...L  
=i X...2...!)MIIo...Qqdj2!'...ES...Q...%y: 8B^eb ::  
D...GS...D...x?...LR6Kxz...lLA...LYLP...EH'SE s6\_T\_S02...Q S...LS...Cox)<c8 \<br>Feuu...N1Ch004...D-y@V xxxXYyo-L s fo , 'g /70##f JFfo D Z- b3uo,o, f\* Mo frI...~#1  
B[o om [...]g  
Bisdd...rz luook ...) N4 0X...\h--eHx6...os9ggg| EtS9M...  
3FHox...K...&cy7zfje "... 00(Ioi ... #..."φfcmX  
^S\$...[Uo][U U ][...]... Uo? \*AO0x8Vi(" s"xAA...f...c':zfEt?-f馱EYEO20xi...rr...rf...f ...#BN8EMJAK 9VBFB M35...jOGOT ... =>zv r...\$f



# Dynamic Analysis

- Bự chà bá! Oh mà phần mở đầu là “PK”, nghĩa là ZIP file, như vậy lưu đồng này lại, extract ra xem thử

The screenshot shows a hex editor window with a 'Raw' tab selected. The hex data is displayed in a large font. A context menu is open over the hex data, listing various actions. The 'Copy to file' option is highlighted. The menu also includes options like 'Send to Spider', 'Do an active scan', 'Send to Intruder', 'Send to Repeater', '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', 'Paste from file', 'Save item', 'Don't intercept requests', 'Do intercept', 'Convert selection', 'URL-encode as you type', 'Cut', 'Copy', 'Paste', 'Message editor help', and '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
```

- Nội dung bên trong file MDData.db.json, steps kìa, vậy change nó rồi zip lại, paste vào burp là xong?

```
🍏 ~/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

- Không được, bởi vì server còn check hash key sinh ra từ content nữa, nên phải gen được cái key
- Khá khó (code nhiều quá), thôi làm phân tích tĩnh thử xem

# Static Analysis

- Quảng file apk vào MobSF

Icon



File Information

Name [REDACTED]

Size 28.3MB

MD5 3e665beaedc6fde82ff21496e21ac351

SHA1 515672722eabff91d0e81b88d1a2091c8ec55449

SHA256 d6b17c0521a79308e900d069b298301edac2031c1b4de57e98fbe347cffffdd43

App Information

Package Name [REDACTED]

Main Activity [REDACTED]

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

- Nhìn phần **code analysis**, cái này khá hay ho:

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

- Chúng ta sẽ ngó qua cái `sqlite3 databases`
- Nhớ bài phân tích tĩnh không, cài cái app, xài quanh quanh cho nó tạo thông tin trước

# Static Analysis

- Trong `/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` nhìn hứa hẹn đó, xem thử

# Static Analysis

- Chúng ta có thể thấy khá nhiều “Log” trong 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
```

- Suy nghĩ tí, ví dụ không vào mạng, app vẫn chạy, vẫn tính số bước đi thì dữ liệu này lưu ở đâu?
  - (Từ bước phân tích động) app gửi số bước đi, thời gian, vv... Lên server
- => Suy ra có cái gì đó lạ lạ ở databases rồi



# Static Analysis

- Kiểm tra bảng `minutelyActivityLog`

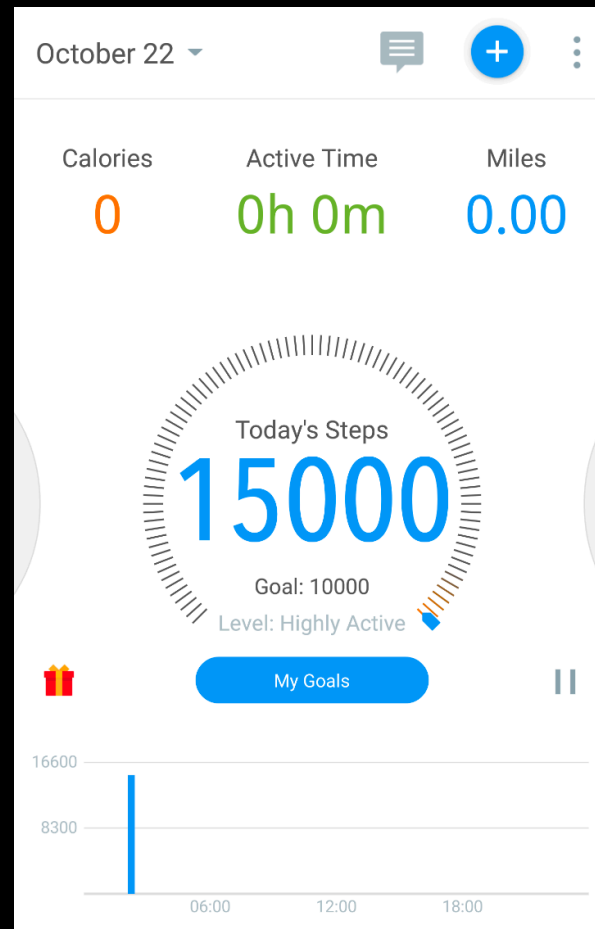
```
sqlite> .schema minutelyActivityLog
CREATE TABLE `minutelyActivityLog` (`Id` INTEGER PRIMARY KEY AUTOINCREMENT , `activetime` INTEGER , `activityType` INTEGER , `calories` FLOAT ,
`distanceInMeters` FLOAT , `endTime` INTEGER , `endTimeTimezoneOffset` INTEGER , `floors` INTEGER , `lastSeenStepCounterReading` 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` );
```

- Cột `steps`? Đổi thử xem!

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

# Static Analysis

- Tắt app, bật lại (hoặc click backup ngay sau khi đổi data trong database luôn)



# Static Analysis

- Click backup để lưu dữ liệu lên cloud
- Bật phone thiết lên, restore dữ liệu đó về, done (hình dưới là hack lâu rồi):



# Static Analysis

- Giờ thì chỉ cần chạy hết sức 1 ngày, lấy dữ liệu đó nhân 7 lên, đem đi show lấy tiền 😊



- Đùa hoy, report rồi, hỏi người ta có viết bài này được hông mới post đó 😊