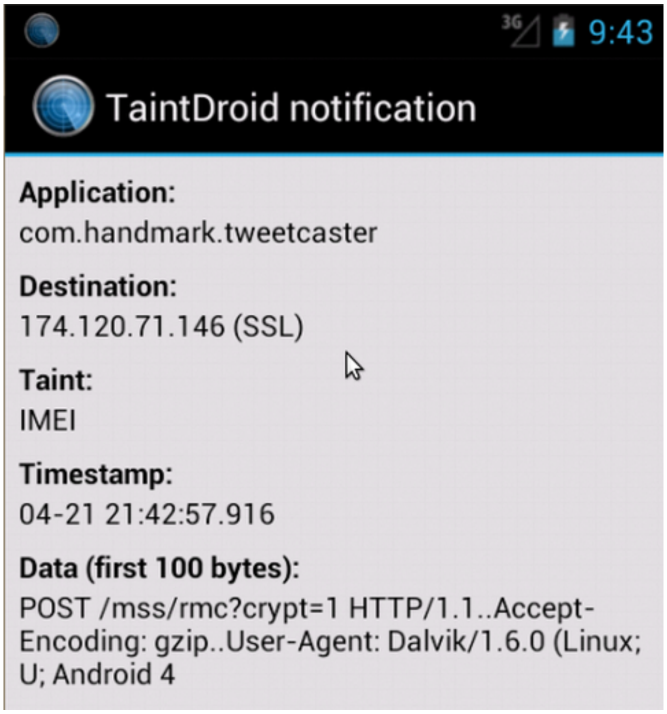
Report of
Android Developer Security Checklist
Avoiding OWASP Mobile Top 10 Risks

Yucheng Liu, Eby John

Application List

Tweetcaster

(https://play.google.com/store/apps/details?id=com.handmark.tweetcaster&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5oYW5kbWFyay50d2VldGNhc3RlciJd)

- Send IMEI to specific IP address(174.120.71.146)
    - ○ 

TaintDroid notification

Application:
com.handmark.tweetcaster

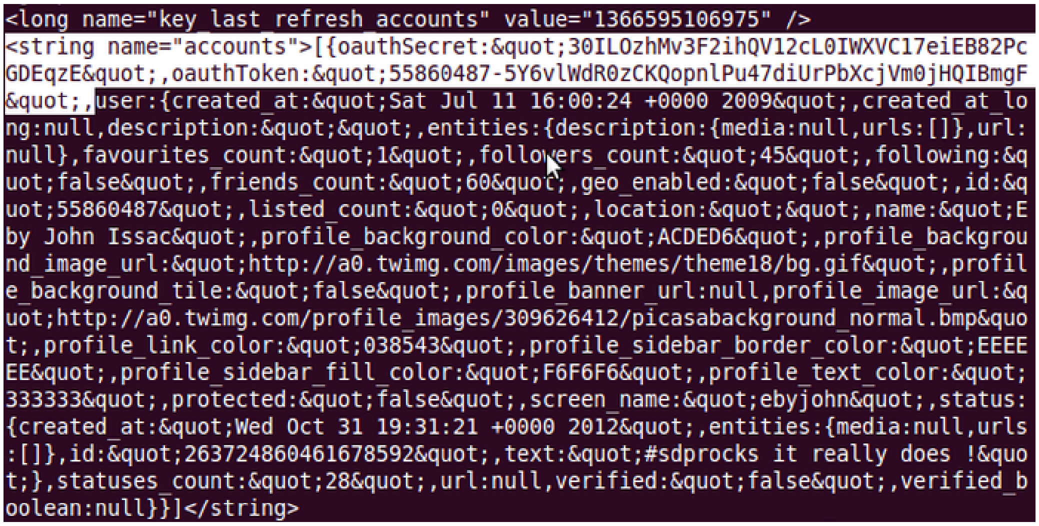
Destination:
174.120.71.146 (SSL)

Taint:
IMEI

Timestamp:
04-21 21:42:57.916

Data (first 100 bytes):
POST /mss/rmc?crypt=1 HTTP/1.1..Accept-Encoding: gzip..User-Agent: Dalvik/1.6.0 (Linux; U; Android 4

- Disclosure in the com.handmark.tweetcaster_preference.xml not encrypted

- ○ 

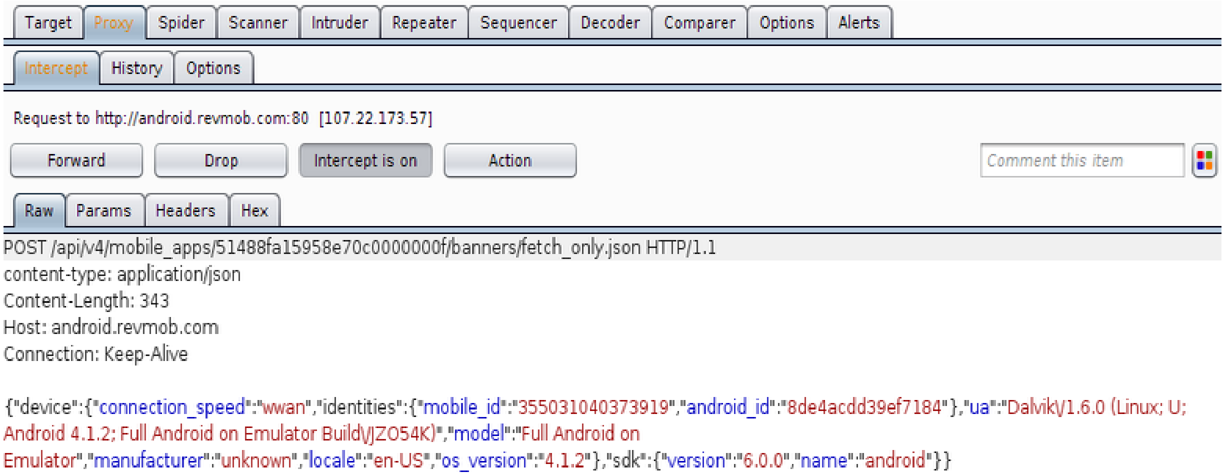
```
<long name="key_last_refresh_accounts" value="1366595106975" />
<string name="accounts">[{oauthSecret:&quot;30ILOzhMv3F2ihQV12cL0IWXVC17eiEB82Pc
GDEqzE&quot;,oauthToken:&quot;55860487-5Y6vlWdR0zCKQopnlPu47diUrPbXcjVm0jHQIBmgF
&quot;,user:{created_at:&quot;Sat Jul 11 16:00:24 +0000 2009&quot;,created_at_lo
ng:null,description:&quot;&quot;,entities:{description:{media:null,urls:[]},url:
null},favourites_count:&quot;1&quot;,followers_count:&quot;45&quot;,following:&q
uot;false&quot;,friends_count:&quot;60&quot;,geo_enabled:&quot;false&quot;,id:&q
uot;55860487&quot;,listed_count:&quot;0&quot;,location:&quot;&quot;,name:&quot;E
by John Issac&quot;,profile_background_color:&quot;ACDED6&quot;,profile_backgrou
nd_image_url:&quot;http://a0.twimg.com/images/themes/theme18/bg.gif&quot;,profil
e_background_tile:&quot;false&quot;,profile_banner_url:null,profile_image_url:&q
uot;http://a0.twimg.com/profile_images/309626412/picasabackground_normal.bmp&quo
t;,profile_link_color:&quot;038543&quot;,profile_sidebar_border_color:&quot;EEEE
EE&quot;,profile_sidebar_fill_color:&quot;F6F6F6&quot;,profile_text_color:&quot;
333333&quot;,protected:&quot;false&quot;,screen_name:&quot;ebyjohn&quot;,status:
{created_at:&quot;Wed Oct 31 19:31:21 +0000 2012&quot;,entities:{media:null,urls
:[]},id:&quot;263724860461678592&quot;,text:&quot;#sdprocks it really does !&quo
t;},statuses_count:&quot;28&quot;,url:null,verified:&quot;false&quot;,verified_b
oolean:null}}]</string>
```

- adlib onelouder
- No access to SDcard
- Install ad https://ads.appia.com/installAd.jsp which might cause some vulnerability if it doesnot check the data from server side

----

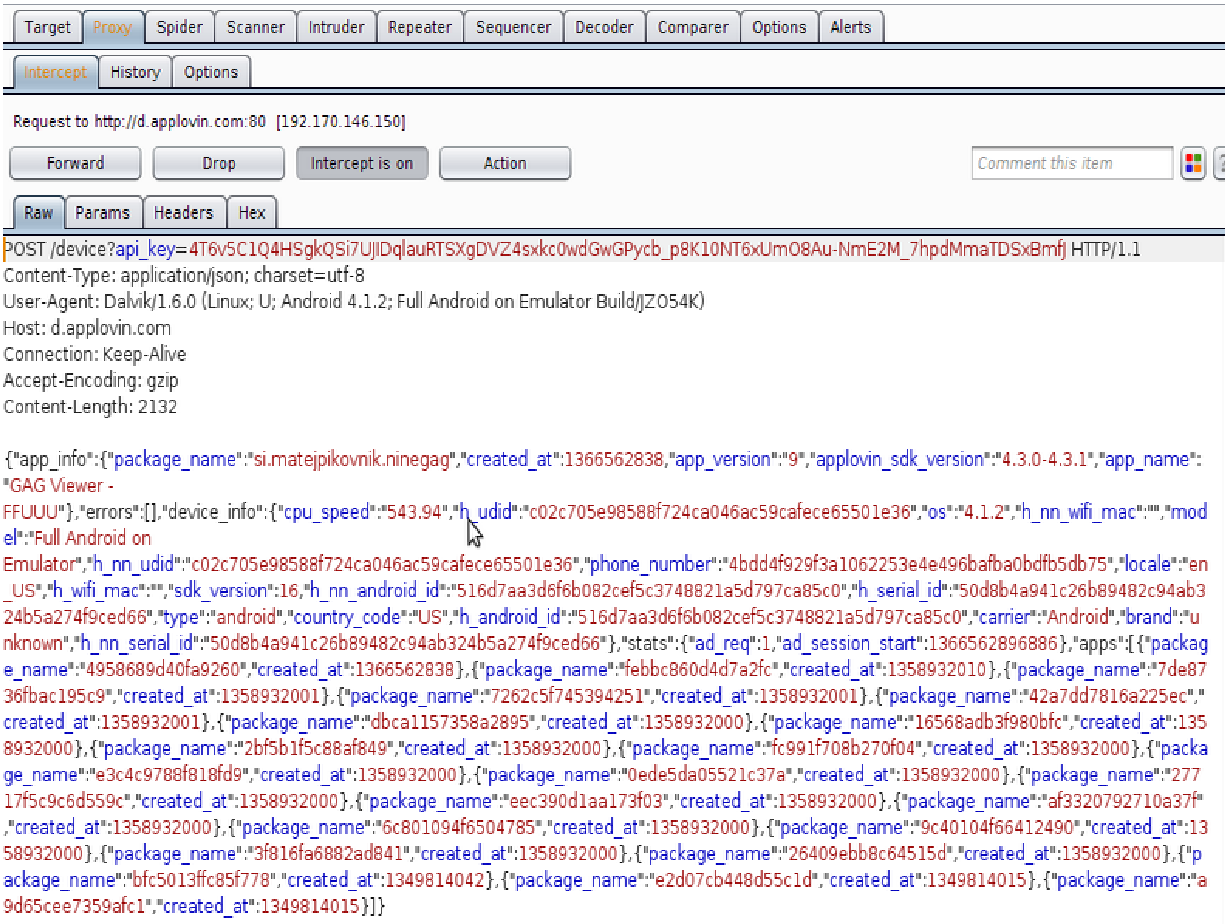
Gag Viewer

[(https://play.google.com/store/apps/details?id=si.matejpikovnik.ninegag&feature=search_result#?t=W251bGwsMSwyLDEsInNpLm1hdGVqcGlrb3ZuaWsubmluZWdhZyJd)](https://play.google.com/store/apps/details?id=si.matejpikovnik.ninegag&feature=search_result#?t=W251bGwsMSwyLDEsInNpLm1hdGVqcGlrb3ZuaWsubmluZWdhZyJd)



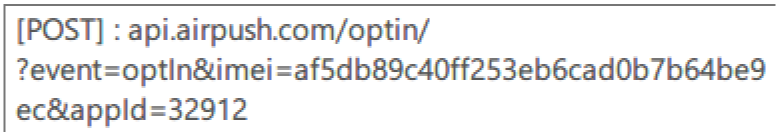
Request to http://android.revmob.com:80 [107.22.173.57]

```
POST /api/v4/mobile_apps/51488fa15958e70c0000000f/banners/fetch_only.json HTTP/1.1
content-type: application/json
Content-Length: 343
Host: android.revmob.com
Connection: Keep-Alive

{"device":{"connection_speed":"wwan","identities":{"mobile_id":"355031040373919","android_id":"8de4acdd39ef7184"},"ua":"Dalvik/1.6.0 (Linux; U;
Android 4.1.2; Full Android on Emulator Build/JZO54K)","model":"Full Android on
Emulator","manufacturer":"unknown","locale":"en-US","os_version":"4.1.2"},"sdk":{"version":"6.0.0","name":"android"}}
```

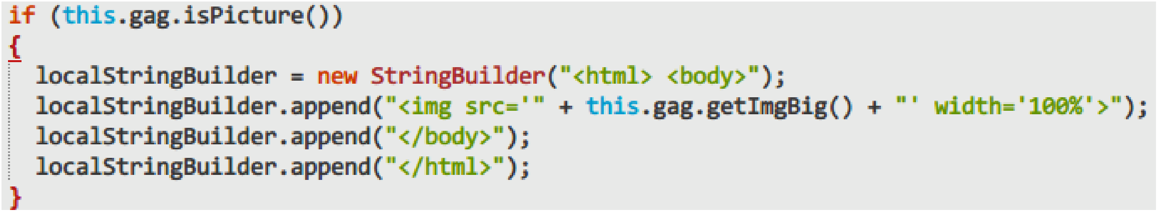


Request to http://d.applovin.com:80 [192.170.146.150]

```
POST /device?api_key=4T6v5C1Q4HSgkQSi7UJIDqlauRTSXgDVZ4sxkc0wdGwGPycb_p8K10NT6xUmO8Au-NmE2M_7hpdMmaTDSxBmfj HTTP/1.1
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; Full Android on Emulator Build/JZO54K)
Host: d.applovin.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 2132

{"app_info":{"package_name":"si.matejpikovnik.ninegag","created_at":1366562838,"app_version":"9","applovin_sdk_version":"4.3.0-4.3.1","app_name":
"GAG Viewer -
FFUUU"},"errors":[],"device_info":{"cpu_speed":"543.94","h_udid":"c02c705e98588f724ca046ac59cafece65501e36","os":"4.1.2","h_nn_wifi_mac":"","mod
el":"Full Android on
Emulator","h_nn_udid":"c02c705e98588f724ca046ac59cafece65501e36","phone_number":"4bdd4f929f3a1062253e4e496bafba0bdfb5db75","locale":"en
_US","h_wifi_mac":"","sdk_version":16,"h_nn_android_id":"516d7aa3d6f6b082cef5c3748821a5d797ca85c0","h_serial_id":"50d8b4a941c26b89482c94ab3
24b5a274f9ced66","type":"android","country_code":"US","h_android_id":"516d7aa3d6f6b082cef5c3748821a5d797ca85c0","carrier":"Android","brand":"u
nknown","h_nn_serial_id":"50d8b4a941c26b89482c94ab324b5a274f9ced66"},"stats":{"ad_req":1,"ad_session_start":1366562896886},"apps":[{"packag
e_name":"4958689d40fa9260","created_at":1366562838},{"package_name":"febbc860d4d7a2fc","created_at":1358932010},{"package_name":"7de87
36fbac195c9","created_at":1358932001},{"package_name":"7262c5f745394251","created_at":1358932001},{"package_name":"42a7dd7816a225ec","
created_at":1358932001},{"package_name":"dbca1157358a2895","created_at":1358932000},{"package_name":"16568adb3f980bfc","created_at":135
8932000},{"package_name":"2bf5b1f5c88af849","created_at":1358932000},{"package_name":"fc991f708b270f04","created_at":1358932000},{"packa
ge_name":"e3c4c9788f818fd9","created_at":1358932000},{"package_name":"0ede5da05521c37a","created_at":1358932000},{"package_name":"277
17f5c9c6d559c","created_at":1358932000},{"package_name":"eec390d1aa173f03","created_at":1358932000},{"package_name":"af3320792710a37f"
,"created_at":1358932000},{"package_name":"6c801094f6504785","created_at":1358932000},{"package_name":"9c40104f66412490","created_at":13
58932000},{"package_name":"3f816fa6882ad841","created_at":1358932000},{"package_name":"26409ebb8c64515d","created_at":1358932000},{"p
ackage_name":"bfc5013ffc85f778","created_at":1349814042},{"package_name":"e2d07cb448d55c1d","created_at":1349814015},{"package_name":"a
9d65cee7359afc1","created_at":1349814015}]}
```



```
[POST] : api.airpush.com/optin/
?event=optIn&imei=af5db89c40ff253eb6cad0b7b64be9
ec&appId=32912
```

- Upload IMEI, Mobile ID, Application List to api.airpush.com
- No Crypto needed
- API key, IMEI, location and android ID are logged
- A binary file (30kb) was downloaded from p.appbrain.com
- Does not provide any encoding function for html entities
    - 

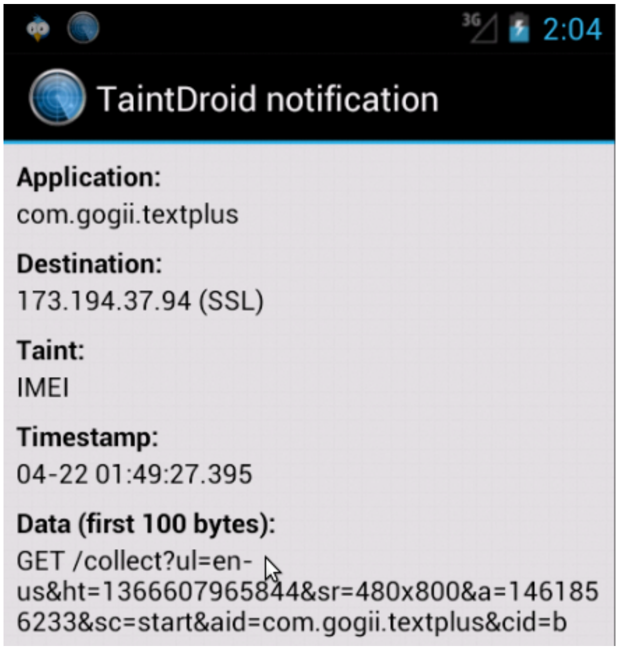
```
if (this.gag.isPicture())
{
  localStringBuilder = new StringBuilder("<html> <body>");
  localStringBuilder.append("<img src='" + this.gag.getImgBig() + "' width='100%'>");
  localStringBuilder.append("</body>");
  localStringBuilder.append("</html>");
}
```

- gag.getImgBig() can be modified and thus can be vulnerable to XSS attack.

----

textPlus

(https://play.google.com/store/apps/details?id=com.gogii.textplus&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5nb2dpaS50ZXh0cGx1cyJd)

- It leaks IMEI a lot of times and uploads to servers that might be vulnerable
  - 

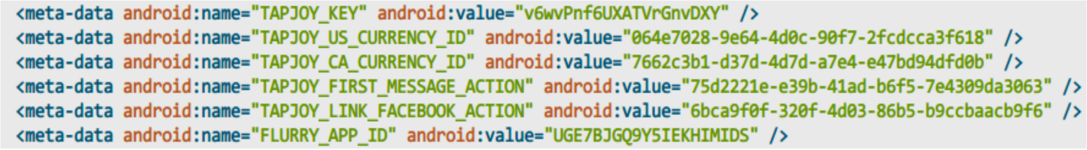
    TaintDroid notification

    Application:
    com.gogii.textplus

    Destination:
    173.194.37.94 (SSL)

    Taint:
    IMEI

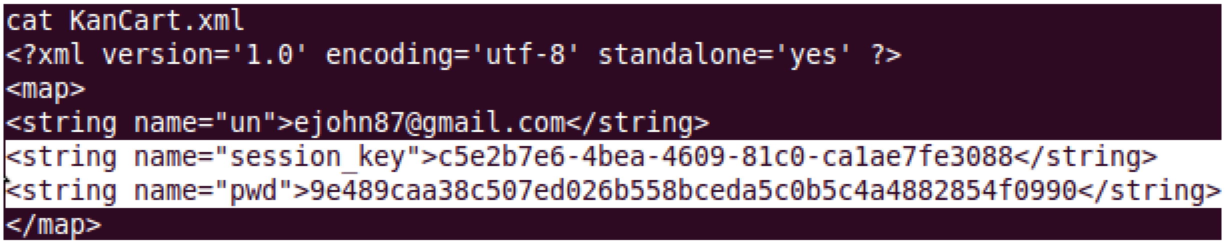
    Timestamp:
    04-22 01:49:27.395

    Data (first 100 bytes):
    GET /collect?ul=en-us&ht=1366607965844&sr=480x800&a=1461856233&sc=start&aid=com.gogii.textplus&cid=b
  - 

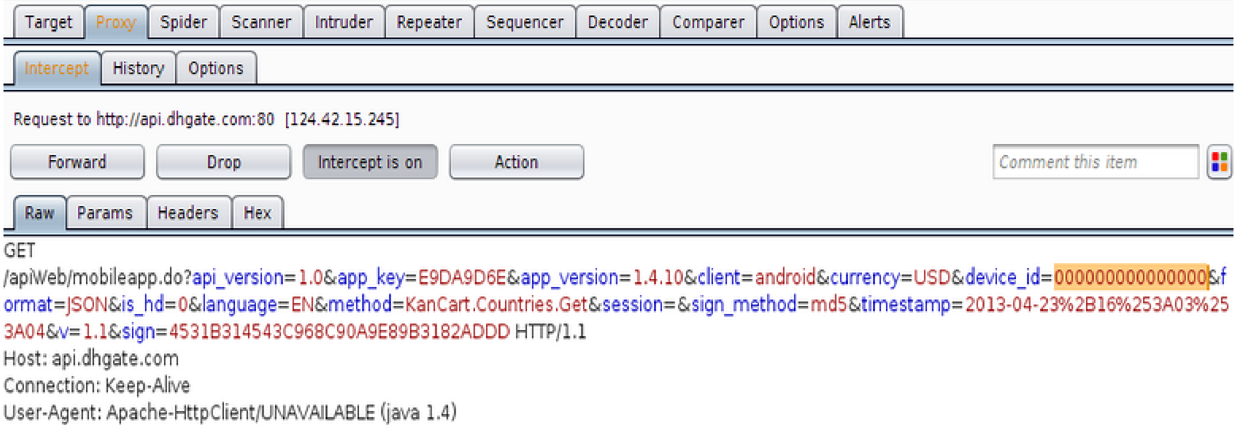
    ```
    <meta-data android:name="TAPJOY_KEY" android:value="v6wvPnf6UXATVrGnvDXY" />
    <meta-data android:name="TAPJOY_US_CURRENCY_ID" android:value="064e7028-9e64-4d0c-90f7-2fcdcca3f618" />
    <meta-data android:name="TAPJOY_CA_CURRENCY_ID" android:value="7662c3b1-d37d-4d7d-a7e4-e47bd94dfd0b" />
    <meta-data android:name="TAPJOY_FIRST_MESSAGE_ACTION" android:value="75d2221e-e39b-41ad-b6f5-7e4309da3063" />
    <meta-data android:name="TAPJOY_LINK_FACEBOOK_ACTION" android:value="6bca9f0f-320f-4d03-86b5-b9ccbaacb9f6" />
    <meta-data android:name="FLURRY_APP_ID" android:value="UGE7BJGQ9Y5IEKHIMIDS" />
    ```
- It stores “TAPJOY_KEY” and “FLURRY_APP_ID” insecurely in files on mobile
- All messages are stored without encryption
- All messages are sent using SSL and not vulnerable to MiTM
- The app uses prepared SQL sequence and no SQL injection vulnerabilities found
- A lot of API keys are hardcoded

DHGate Mobile

(https://play.google.com/store/apps/details?id=com.honestw alker.kancart.DHgate.activity&feature=search_result#?t=W251bGw sMSw yLDEsImNvbS5ob25lc3R3YWxrZXIua2FuY2FydC5ESGdhdGUuYWN0aXZpdHkiXQ..)



```
cat KanCart.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="un">ejohn87@gmail.com</string>
<string name="session_key">c5e2b7e6-4bea-4609-81c0-ca1ae7fe3088</string>
<string name="pwd">9e489caa38c507ed026b558bceda5c0b5c4a4882854f0990</string>
</map>
```



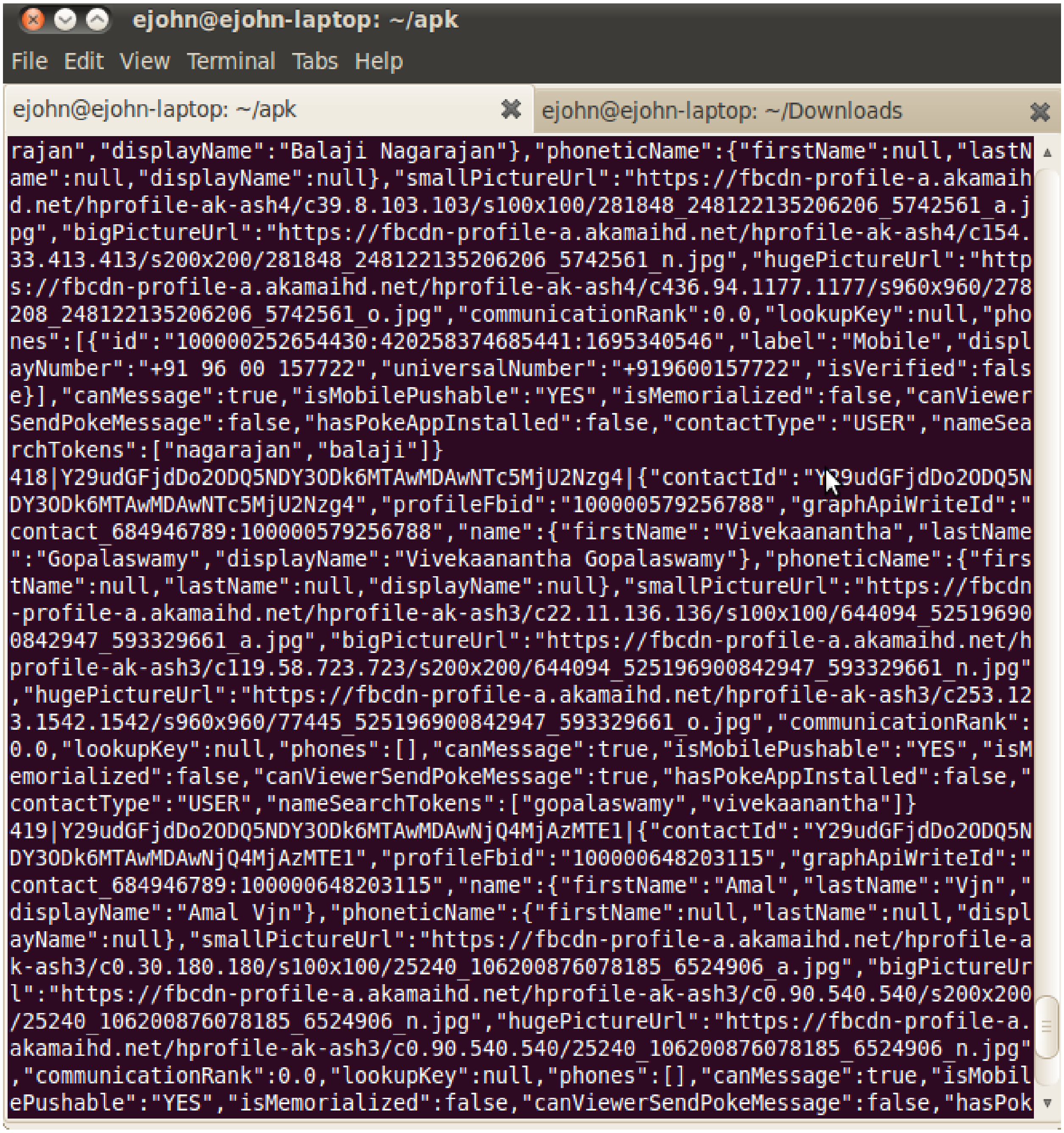
Request to http://api.dhgate.com:80 [124.42.15.245]

```
GET
/apiWeb/mobileapp.do?api_version=1.0&app_key=E9DA9D6E&app_version=1.4.10&client=android&currency=USD&device_id=000000000000000&format=JSON&is_hd=0&language=EN&method=KanCart.Countries.Get&session=&sign_method=md5&timestamp=2013-04-23%2B16%253A03%253A04&v=1.1&sign=4531B314543C968C90A9E89B3182ADDD HTTP/1.1
Host: api.dhgate.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
```

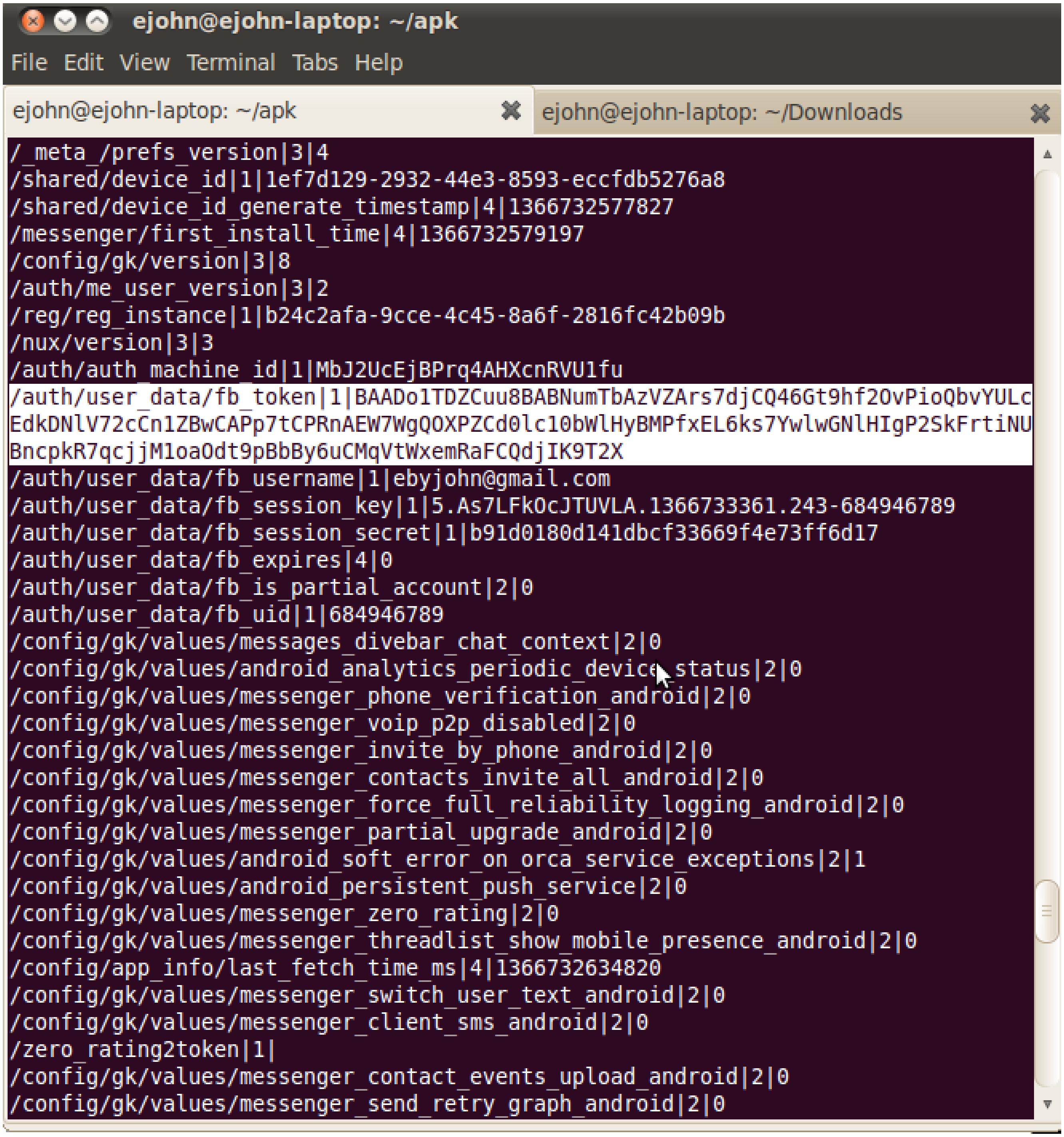
- It uploads IMEI to api.dhgate.com which might cause vulnerability
- It writes log information as plaintext and stores insecurely in SD card
- It use server information as DES key which might cause insufficient crypto
- File system access is not disabled for any webviews
- XSS injection possible in WebView
- Session key and password is hardcoded in the shared preferences.
- HTTPS not used for online transactions.
- Password is hashed using MD5.
- Password is logged.

Facebook Messenger

(https://play.google.com/store/apps/details?id=com.facebook.orca&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5mYWNlYm9vay5vcmNhIl0.)


ejohn@ejohn-laptop: ~/apk
File Edit View Terminal Tabs Help
ejohn@ejohn-laptop: ~/apk
ejohn@ejohn-laptop: ~/Downloads

```
rajan","displayName":"Balaji Nagarajan"},"phoneticName":{"firstName":null,"lastN
ame":null,"displayName":null},"smallPictureUrl":"https://fbcdn-profile-a.akamaih
d.net/hprofile-ak-ash4/c39.8.103.103/s100x100/281848_248122135206206_5742561_a.j
pg","bigPictureUrl":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash4/c154.
33.413.413/s200x200/281848_248122135206206_5742561_n.jpg","hugePictureUrl":"http
s://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash4/c436.94.1177.1177/s960x960/278
208_248122135206206_5742561_o.jpg","communicationRank":0.0,"lookupKey":null,"pho
nes":[{"id":"100000252654430:420258374685441:1695340546","label":"Mobile","displ
ayNumber":"+91 96 00 157722","universalNumber":"+919600157722","isVerified":fals
e}],"canMessage":true,"isMobilePushable":"YES","isMemorialized":false,"canViewer
SendPokeMessage":false,"hasPokeAppInstalled":false,"contactType":"USER","nameSea
rchTokens":["nagarajan","balaji"]}
418|Y29udGFjdDo2ODQ5NDY3ODk6MTAwMDAwNTc5MjU2Nzg4|{"contactId":"Y29udGFjdDo2ODQ5N
DY3ODk6MTAwMDAwNTc5MjU2Nzg4","profileFbid":"100000579256788","graphApiWriteId":"
contact_684946789:100000579256788","name":{"firstName":"Vivekaanantha","lastName
":"Gopalaswamy","displayName":"Vivekaanantha Gopalaswamy"},"phoneticName":{"firs
tName":null,"lastName":null,"displayName":null},"smallPictureUrl":"https://fbcdn
-profile-a.akamaihd.net/hprofile-ak-ash3/c22.11.136.136/s100x100/644094_52519690
0842947_593329661_a.jpg","bigPictureUrl":"https://fbcdn-profile-a.akamaihd.net/h
profile-ak-ash3/c119.58.723.723/s200x200/644094_525196900842947_593329661_n.jpg"
,"hugePictureUrl":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash3/c253.12
3.1542.1542/s960x960/77445_525196900842947_593329661_o.jpg","communicationRank":
0.0,"lookupKey":null,"phones":[],"canMessage":true,"isMobilePushable":"YES","isM
emorialized":false,"canViewerSendPokeMessage":true,"hasPokeAppInstalled":false,"
contactType":"USER","nameSearchTokens":["gopalaswamy","vivekaanantha"]}
419|Y29udGFjdDo2ODQ5NDY3ODk6MTAwMDAwNjQ4MjAzMTE1|{"contactId":"Y29udGFjdDo2ODQ5N
DY3ODk6MTAwMDAwNjQ4MjAzMTE1","profileFbid":"100000648203115","graphApiWriteId":"
contact_684946789:100000648203115","name":{"firstName":"Amal","lastName":"Vjn","
displayName":"Amal Vjn"},"phoneticName":{"firstName":null,"lastName":null,"displ
ayName":null},"smallPictureUrl":"https://fbcdn-profile-a.akamaihd.net/hprofile-a
k-ash3/c0.30.180.180/s100x100/25240_106200876078185_6524906_a.jpg","bigPictureUr
l":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash3/c0.90.540.540/s200x200
/25240_106200876078185_6524906_n.jpg","hugePictureUrl":"https://fbcdn-profile-a.
akamaihd.net/hprofile-ak-ash3/c0.90.540.540/25240_106200876078185_6524906_n.jpg"
,"communicationRank":0.0,"lookupKey":null,"phones":[],"canMessage":true,"isMobil
ePushable":"YES","isMemorialized":false,"canViewerSendPokeMessage":false,"hasPok
```

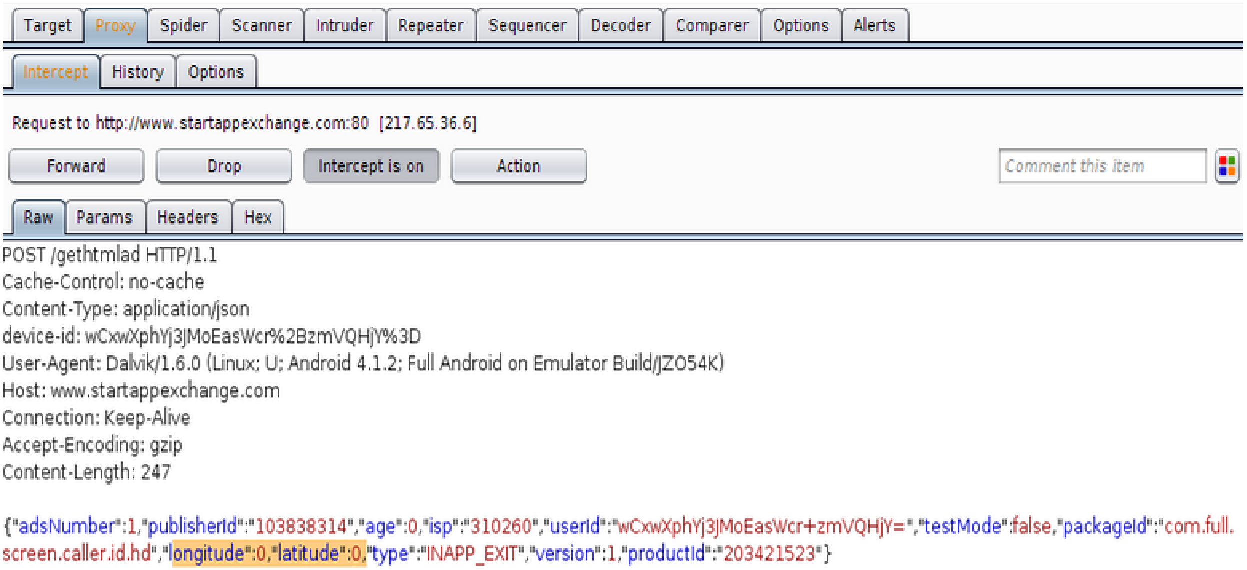

ejohn@ejohn-laptop: ~/apk
File
Edit
View
Terminal
Tabs
Help
ejohn@ejohn-laptop: ~/apk
ejohn@ejohn-laptop: ~/Downloads

```
/_meta_/prefs_version|3|4
/shared/device_id|1|1ef7d129-2932-44e3-8593-eccfdb5276a8
/shared/device_id_generate_timestamp|4|1366732577827
/messenger/first_install_time|4|1366732579197
/config/gk/version|3|8
/auth/me_user_version|3|2
/reg/reg_instance|1|b24c2afa-9cce-4c45-8a6f-2816fc42b09b
/nux/version|3|3
/auth/auth_machine_id|1|MbJ2UcEjBPrq4AHXcnRVU1fu
/auth/user_data/fb_token|1|BAADo1TDZCuu8BABNumTbAzVZArs7djCQ46Gt9hf2OvPioQbvYULc
EdkDNlV72cCn1ZBwCAPp7tCPRnAEW7WgQOXPZCd0lc10bWlHyBMPfxEL6ks7YwlwGNlHIgP2SkFrtiNU
BncpkR7qcjjM1oaOdt9pBbBy6uCMqVtWxemRaFCQdjIK9T2X
/auth/user_data/fb_username|1|ebyjohn@gmail.com
/auth/user_data/fb_session_key|1|5.As7LFkOcJTUVLA.1366733361.243-684946789
/auth/user_data/fb_session_secret|1|b91d0180d141dbcf33669f4e73ff6d17
/auth/user_data/fb_expires|4|0
/auth/user_data/fb_is_partial_account|2|0
/auth/user_data/fb_uid|1|684946789
/config/gk/values/messages_divebar_chat_context|2|0
/config/gk/values/android_analytics_periodic_device_status|2|0
/config/gk/values/messenger_phone_verification_android|2|0
/config/gk/values/messenger_voip_p2p_disabled|2|0
/config/gk/values/messenger_invite_by_phone_android|2|0
/config/gk/values/messenger_contacts_invite_all_android|2|0
/config/gk/values/messenger_force_full_reliability_logging_android|2|0
/config/gk/values/messenger_partial_upgrade_android|2|0
/config/gk/values/android_soft_error_on_orca_service_exceptions|2|1
/config/gk/values/android_persistent_push_service|2|0
/config/gk/values/messenger_zero_rating|2|0
/config/gk/values/messenger_threadlist_show_mobile_presence_android|2|0
/config/app_info/last_fetch_time_ms|4|1366732634820
/config/gk/values/messenger_switch_user_text_android|2|0
/config/gk/values/messenger_client_sms_android|2|0
/zero_rating2token|1|
/config/gk/values/messenger_contact_events_upload_android|2|0
/config/gk/values/messenger_send_retry_graph_android|2|0
```

- All messages are stored in local database (might not be a vulnerability but suspicious)
- Contact information is stored without encryption
- FB token and session secret are stored

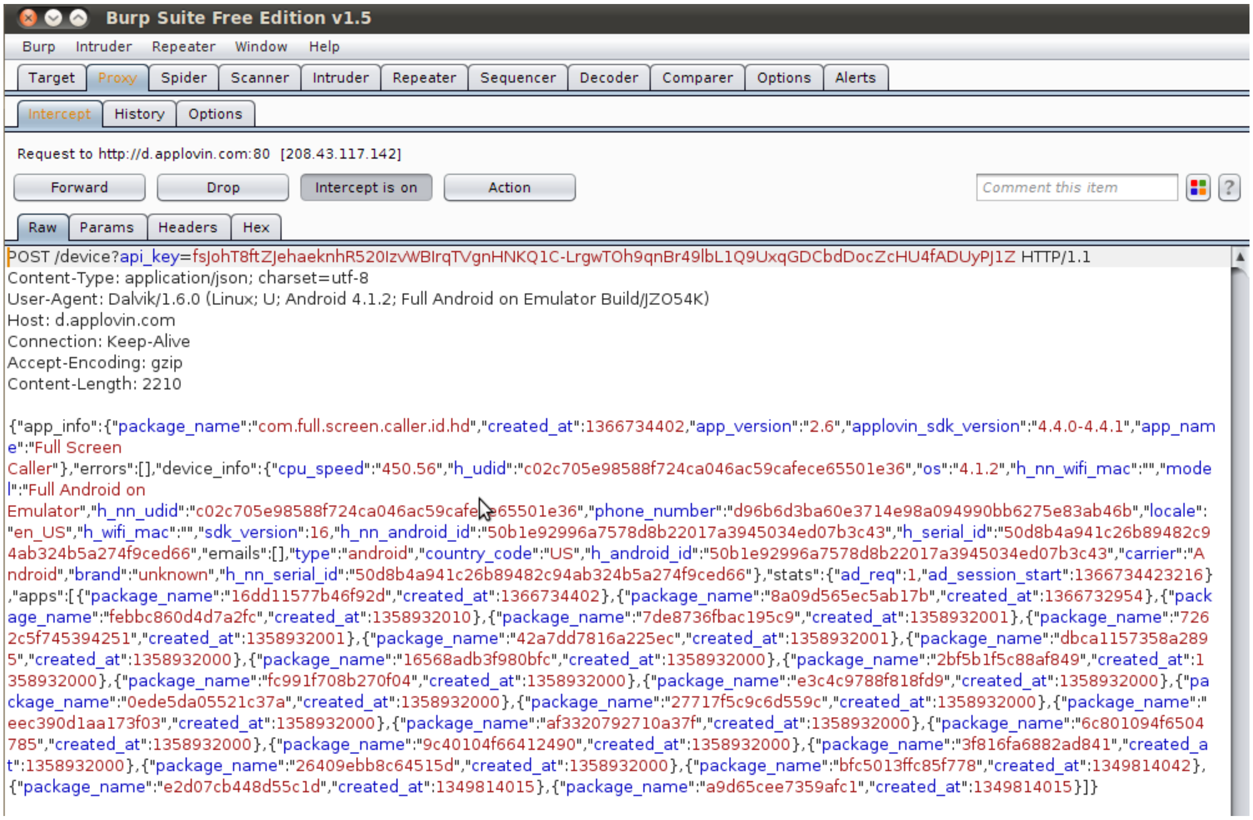
HD Caller ID

(https://play.google.com/store/apps/details?id=com.full.screen.caller.id.hd&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5mdWxsLnNjcmVlbi5jYWxsZXIuaWQuaGQiXQ..)



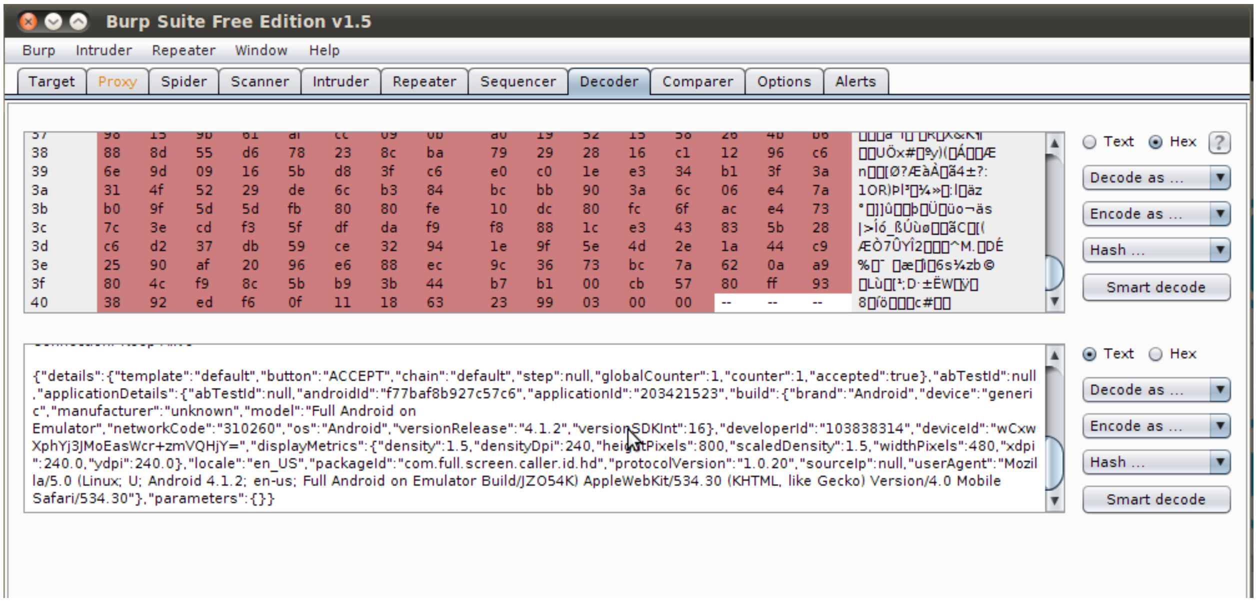
Request to http://www.startappexchange.com:80 [217.65.36.6]

```
POST /gethtmlad HTTP/1.1
Cache-Control: no-cache
Content-Type: application/json
device-id: wCxwXphYj3JMoEasWcr%2BzmVQHjY%3D
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; Full Android on Emulator Build/JZO54K)
Host: www.startappexchange.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 247

{"adsNumber":1,"publisherId":"103838314","age":0,"isp":"310260","userId":"wCxwXphYj3JMoEasWcr+zmVQHjY=","testMode":false,"packageId":"com.full.
screen.caller.id.hd","longitude":0,"latitude":0,"type":"INAPP_EXIT","version":1,"productId":"203421523"}
```


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

Request to http://d.applovin.com:80 [208.43.117.142]

```
POST /device?api_key=fsJohT8ftZJehaeknhR520IzvWBIrqTVgnHNKQ1C-LrgwTOh9qnBr49lbL1Q9UxqGDCbdDocZcHU4fADUyPJ1Z HTTP/1.1
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; Full Android on Emulator Build/JZO54K)
Host: d.applovin.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 2210

{"app_info":{"package_name":"com.full.screen.caller.id.hd","created_at":1366734402,"app_version":"2.6","applovin_sdk_version":"4.4.0-4.4.1","app_nam
e":"Full Screen
Caller"},"errors":[],"device_info":{"cpu_speed":"450.56","h_udid":"c02c705e98588f724ca046ac59cafece65501e36","os":"4.1.2","h_nn_wifi_mac":"","mode
l":"Full Android on
Emulator","h_nn_udid":"c02c705e98588f724ca046ac59cafece65501e36","phone_number":"d96b6d3ba60e3714e98a094990bb6275e83ab46b","locale":
"en_US","h_wifi_mac":"","sdk_version":16,"h_nn_android_id":"50b1e92996a7578d8b22017a3945034ed07b3c43","h_serial_id":"50d8b4a941c26b89482c9
4ab324b5a274f9ced66","emails":[],"type":"android","country_code":"US","h_android_id":"50b1e92996a7578d8b22017a3945034ed07b3c43","carrier":"A
ndroid","brand":"unknown","h_nn_serial_id":"50d8b4a941c26b89482c94ab324b5a274f9ced66"},"stats":{"ad_req":1,"ad_session_start":1366734423216}
,"apps":[{"package_name":"16dd11577b46f92d","created_at":1366734402},{"package_name":"8a09d565ec5ab17b","created_at":1366732954},{"pack
age_name":"febbc860d4d7a2fc","created_at":1358932010},{"package_name":"7de8736fbac195c9","created_at":1358932001},{"package_name":"726
2c5f745394251","created_at":1358932001},{"package_name":"42a7dd7816a225ec","created_at":1358932001},{"package_name":"dbca1157358a289
5","created_at":1358932000},{"package_name":"16568adb3f980bfc","created_at":1358932000},{"package_name":"2bf5b1f5c88af849","created_at":1
358932000},{"package_name":"fc991f708b270f04","created_at":1358932000},{"package_name":"e3c4c9788f818fd9","created_at":1358932000},{"pa
ckage_name":"0ede5da05521c37a","created_at":1358932000},{"package_name":"27717f5c9c6d559c","created_at":1358932000},{"package_name":"
eec390d1aa173f03","created_at":1358932000},{"package_name":"af3320792710a37f","created_at":1358932000},{"package_name":"6c801094f6504
785","created_at":1358932000},{"package_name":"9c40104f66412490","created_at":1358932000},{"package_name":"3f816fa6882ad841","created_a
t":1358932000},{"package_name":"26409ebb8c64515d","created_at":1358932000},{"package_name":"bfc5013ffc85f778","created_at":1349814042},
{"package_name":"e2d07cb448d55c1d","created_at":1349814015},{"package_name":"a9d65cee7359afc1","created_at":1349814015}]}
```


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
○ Text ● Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
38   88 8d 55 d6 78 23 8c ba 79 29 28 16 c1 12 96 c6
39   6e 9d 09 16 5b d8 3f c6 e0 c0 1e e3 34 b1 3f 3a
3a   31 4f 52 29 de 6c b3 84 bc bb 90 3a 6c 06 e4 7a
3b   b0 9f 5d 5d fb 80 80 fe 10 dc 80 fc 6f ac e4 73
3c   7c 3e cd f3 5f df da f9 f8 88 1c e3 43 83 5b 28
3d   c6 d2 37 db 59 ce 32 94 1e 9f 5e 4d 2e 1a 44 c9
3e   25 90 af 20 96 e6 88 ec 9c 36 73 bc 7a 62 0a a9
3f   80 4c f9 8c 5b b9 3b 44 b7 b1 00 cb 57 80 ff 93
40   38 92 ed f6 0f 11 18 63 23 99 03 00 00 -- -- --
```

```
{"details":{"template":"default","button":"ACCEPT","chain":"default","step":null,"globalCounter":1,"counter":1,"accepted":true},"abTestId":null
,"applicationDetails":{"abTestId":null,"androidId":"f77baf8b927c57c6","applicationId":"203421523","build":{"brand":"Android","device":"generi
c","manufacturer":"unknown","model":"Full Android on
Emulator","networkCode":"310260","os":"Android","versionRelease":"4.1.2","versionSDKInt":16},"developerId":"103838314","deviceId":"wCxw
XphYj3JMoEasWcr+zmVQHjY=","displayMetrics":{"density":1.5,"densityDpi":240,"heightPixels":800,"scaledDensity":1.5,"widthPixels":480,"xdpi
":240.0,"ydpi":240.0},"locale":"en_US","packageId":"com.full.screen.caller.id.hd","protocolVersion":"1.0.20","sourceIp":null,"userAgent":"Mozil
la/5.0 (Linux; U; Android 4.1.2; en-us; Full Android on Emulator Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile
Safari/534.30"},"parameters":{}}
```

- It sends location information, device ID and even phonenumber to server startappexchange.com
- It also leaks phone number and device ID through 3rd party library
- Sensitive information is sent without using SSL

- It asks permission to write on SD card which might cause vulnerability

----

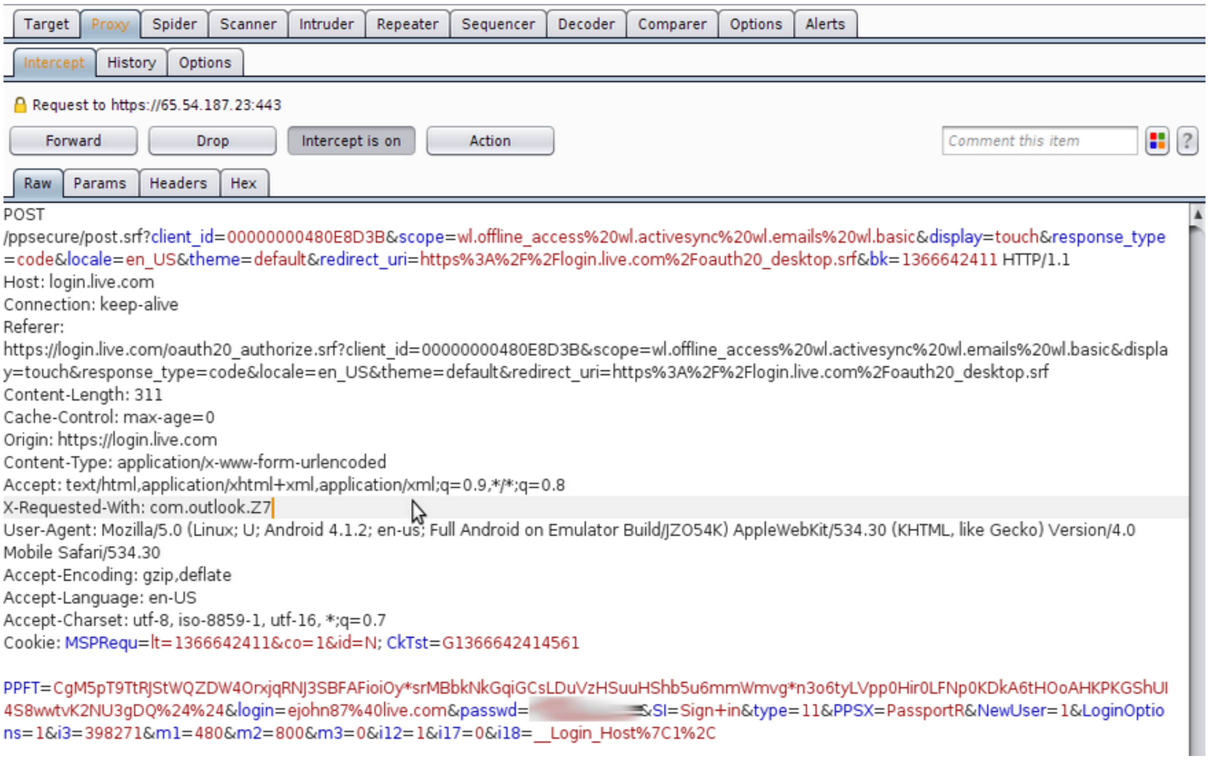
Biz Barcode

(https://play.google.com/store/apps/details?id=com.bizbarcode.client.android&feature=also_installed#?t=W251bGw sMSw xLDEw NCw iY29tLmJpemJhcmNvZGUuY2xpZW50LmFuZHJvaWQiXQ..)

- (This is a simple app and no risks discovered)

Outlook.com

(https://play.google.com/store/apps/details?id=com.outlook.Z7&feature=search_result#?t=W251bGw sMSw xLDEsImNvbS5vdXRsb29rLlo3Il0.)



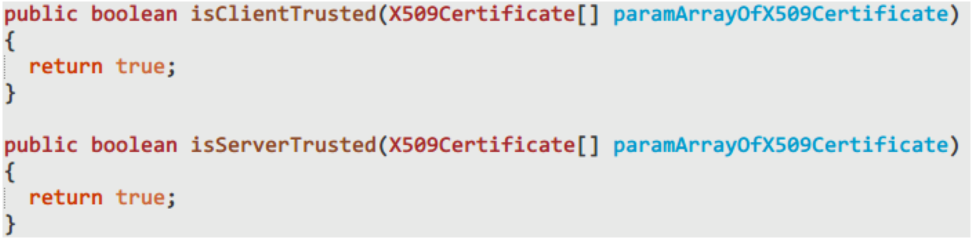
Request to https://65.54.187.23:443

```
POST
/ppsecure/post.srf?client_id=00000000480E8D3B&scope=wl.offline_access%20wl.activesync%20wl.emails%20wl.basic&display=touch&response_type
=code&locale=en_US&theme=default&redirect_uri=https%3A%2F%2Flogin.live.com%2Foauth20_desktop.srf&bk=1366642411 HTTP/1.1
Host: login.live.com
Connection: keep-alive
Referer:
https://login.live.com/oauth20_authorize.srf?client_id=00000000480E8D3B&scope=wl.offline_access%20wl.activesync%20wl.emails%20wl.basic&displa
y=touch&response_type=code&locale=en_US&theme=default&redirect_uri=https%3A%2F%2Flogin.live.com%2Foauth20_desktop.srf
Content-Length: 311
Cache-Control: max-age=0
Origin: https://login.live.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
X-Requested-With: com.outlook.Z7
User-Agent: Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; Full Android on Emulator Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0
Mobile Safari/534.30
Accept-Encoding: gzip,deflate
Accept-Language: en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Cookie: MSPRequ=lt=1366642411&co=1&id=N; CkTst=G1366642414561

PPFT=CgM5pT9TtRJStWQZDW4OrxjqRNJ3SBFAFioiOy*srMBbkNkGqiGCsLDuVzHSuuHShb5u6mmWmvg*n3o6tyLVpp0Hir0LFNp0KDkA6tHOoAHKPKGShUI
4S8wwtvK2NU3gDQ%24%24&login=ejohn87%40live.com&passwd=[redacted]&SI=Sign+in&type=11&PPSX=PassportR&NewUser=1&LoginOptio
ns=1&i3=398271&m1=480&m2=800&m3=0&i12=1&i17=0&i18=__Login_Host%7C1%2C
```

- SSL is not configured properly
- MiTM is possible, password can be recovered
- The database is not encrypted but the password is hashed
- Emails can be recovered

AliExpress

(https://play.google.com/store/apps/details?id=com.alibaba.aliexpresshd&feature=personalized-recommendations#?t=W251bGw sMSw xLDIxMyw iY29tLmFsaWJhYmEuYWxpZXhw cmVzc2hkIl0.)

- 

```
public boolean isClientTrusted(X509Certificate[] paramArrayOfX509Certificate)
{
  return true;
}

public boolean isServerTrusted(X509Certificate[] paramArrayOfX509Certificate)
{
  return true;
}
```

  - This app blindly trust Client’s and Server’s certificates
  - SSL is not configured properly and MiTM attack is possible
- The database with account details is not encrypted
- Email account, Personal Information are stored locally without any encryption

----

Android Developer Security Checklist

Avoiding OWASP Mobile Top 10 Risks

Prepare Work

- Decompile .apk file to get files such like AndroidManifest.xml and resource file with tool
- Get Java code using APK One Click
- Analyze Tools
  - Static Analysis
    - SandDroid
    - Dexter
    - FireEye
    - AndroGuard
  - Dynamic Analysis
    - TaintDroid

Checklist in Detail

- M1: Insecure Data Storage
  - Is sensitive information like Usernames, Passwords, Location data, SSN, Address etc **stored insecurely** in files on the mobile?
  - Is sensitive information stored on SDCard **encrypted?**
  - Is sensitive information being **logged?**
  - Is any file marked **MODE_WORLD_WRITEABLE or MODE_WORLD_READABLE** unnecessarily **?**
- M2: Weak Authentication Mechanisms
  - Is a device dependant variable being used as an authentication token?
  - Is data properly validated before authentication proceeds?
  - Does the password recovery feature allow account hijacking?
  - Are passwords being hashed and salted before being stored on the server?
- M3: Insufficient Transport Layer Protection
  - Is the SSL Certificate properly validated before establishing connection or are all certificates accepted?
  - Is a MiTM attack possible.

- Is the Cipher used of strength sufficient? [Also M9]
- Do not send sensitive data over alternate channels, such as SMS, MMS, or notifications.[Also M10]

- M4: Client Side Injection
  - Is Input data properly validated?
  - Is there any Local file inclusion?
  - Use parameterized queries.
  - Verify that File System Access is disabled for any WebViews (webview.getSettings().setAllowFileAccess(false);).
  - Intent Injection/Fuzzing: Verify actions and data are validated via an Intent Filter for all Activities.
- M5: Poor Authorization and Authentication
  - Does the application rely solely on immutable, potentially compromised values (IMEI, IMSI, UUID)?
  - Are there Hardcoded/default accounts in the application?
  - Test if direct access to backend resources is possible.
- M6: Improper Session Handling
  - Is sensitive information utilized within the application flushed from memory upon session expiration?
  - Ensure that sessions time out locally as well as server side.
    - e.g. .setConnectionTimeout()
  - `When HttpClient instance is no longer needed, shut down the connection manager to ensure immediate deallocation of all system resources`
    - `e.g. httpclient.getConnectionManager().shutdown();`
- M7: Security Decisions Via Untrusted Inputs
  - An intent injection attack is possible if the intent address is derived from untrusted input. e.g. URLConnection.getInputStream()
  - Buffer Overflows
    - Review all code that accepts input from users via the HTTP request and ensure that it provides **appropriate size checking on all such inputs on the server-side.**

    - Potential Problem: Cross-Site Scripting
        - The best way to protect a web application from XSS attacks is ensure that your application performs validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be allowed.
- M8: Side Channel Data Leakage
    - Is sensitive information being logged?
    - Ensure 3rd party libraries are not leaking sensitive information.
- M9: Broken Cryptography
    - Use standard security algorithms and their standard implementations. Avoid custom algorithms and protocols.
    - Store sensitive information in char array instead of Java strings.
    - Use a key generation algorithm like PKCS#5 when using password based authentication.
    - Use unpredictable initialization vectors.
    - Ensure the key size is sufficiently large.
- M10: Sensitive Information Disclosure
    - Does the app expose sensitive information like IMEI or other uniquely identifiable details?
    - Is there sensitive information stored in the SharedPreference file?
    - Does the application send sensitive information in the URL parameters without using SSL?
    - Are there hardcoded passwords or API keys?