

# Pengujian Keamanan Aplikasi Mobile

## Studi Kasus: Android

Zaki Akhmad

indocisc

10 Juni 2012

# Tentang Zaki Akhmad

Surel za@indocisc.co.id

Kunci Publik 0xFD57BE80 di pgp.mit.edu

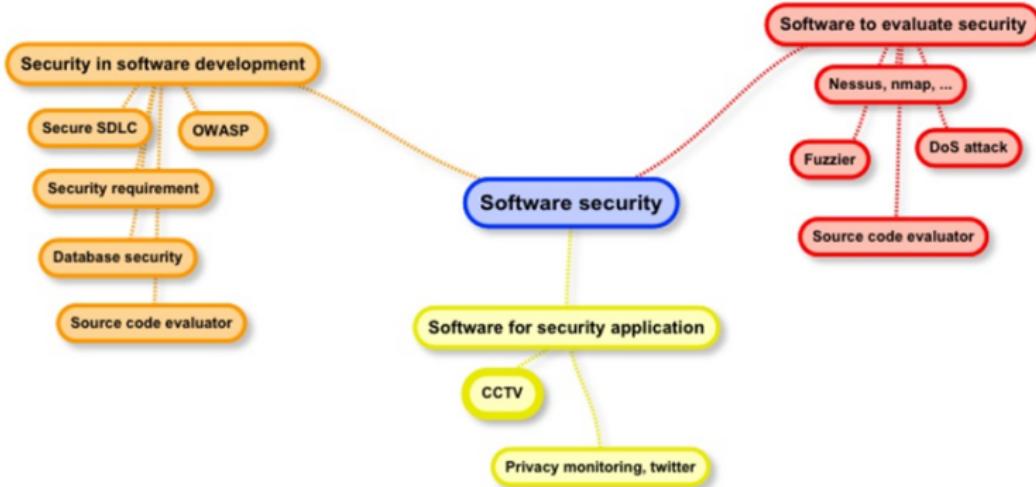
Twitter @zakiakhmad

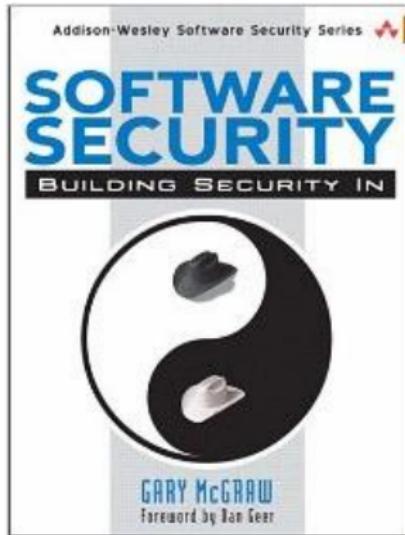
indocisc Analis, 2007 - sekarang

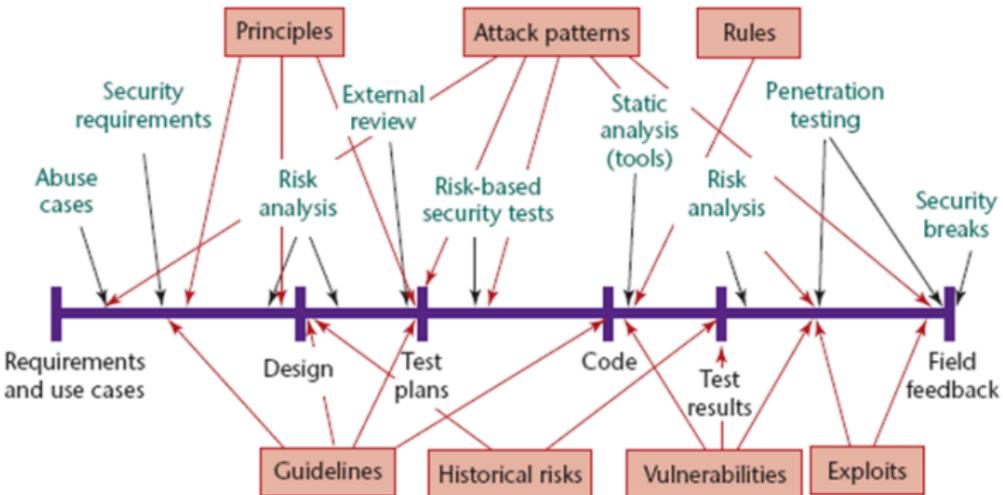


If you **fail** a penetration test  
you know you have a very bad problem indeed.

If you **pass** a penetration test  
you do not know that you don't have a very bad problem (Gary McGraw)

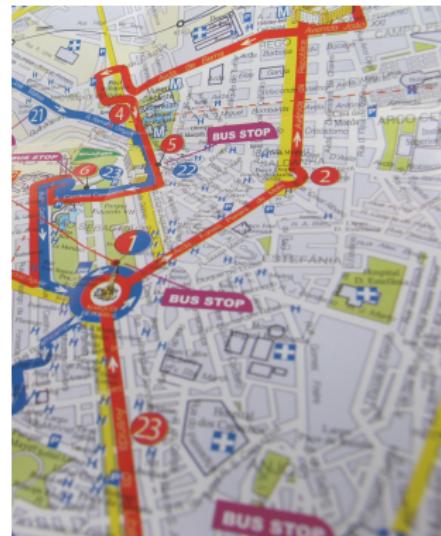






# Daftar Isi

- 1 Pengantar**
  - Konfigurasi Lab
- 2 Teori Pengujian**
  - Pengujian Dinamis
  - Pengujian Statis
- 3 Hasil Pengujian**
  - Wordpress
    - Dinamis
    - Statis
  - Twitter
    - Dinamis
    - Statis
- 4 Penutup**
  - Kesimpulan dan Saran
- 5 Referensi**



# Pengantar

## Ponsel Pintar **Hanya** Sepintar Penggunanya

- 1 Penggunaan di tempat umum
- 2 Risiko hilang, siap?
- 3 Aplikasi
  - 1 Kecenderungan membuat *password* yang sama
  - 2 Tidak tahu apakah menggunakan kanal terenkripsi/tidak

# Konfigurasi Lab

## Langsung dari Device

komputer -> kabel data - > ponsel

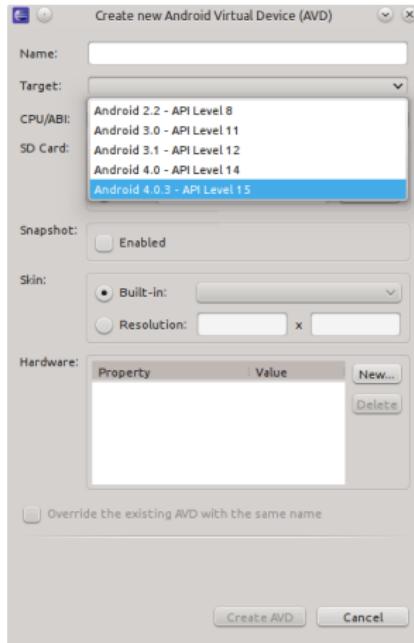
# Konfigurasi Lab

## Menggunakan Hub

ponsel -> hub - > Komputer:Internet

# Konfigurasi Lab

## Menggunakan Emulator



# Dinamis vs Statis



# Pengujian Dinamis

Pengujian dinamis adalah pengujian yang dilakukan **dengan** menjalankan aplikasi

- 1 Analisis *network traffic*
- 2 Analisis *remote services* (HTTP/SOAP/dll)
- 3 Debug aplikasi

# Pengujian Statis

Pengujian statis adalah pengujian yang dilakukan **tanpa** menjalankan aplikasi

- 1 Dapatkan aplikasi
  - 1 Ekstrak aplikasi dari device
  - 2 Dapatkan berkas installer dari pengembang
- 2 Lakukan *reverse engineering*
- 3 Lakukan *source code review*

# Pengujian Dinamis Aplikasi Wordpress

## ■ Analisis *Network Traffic*

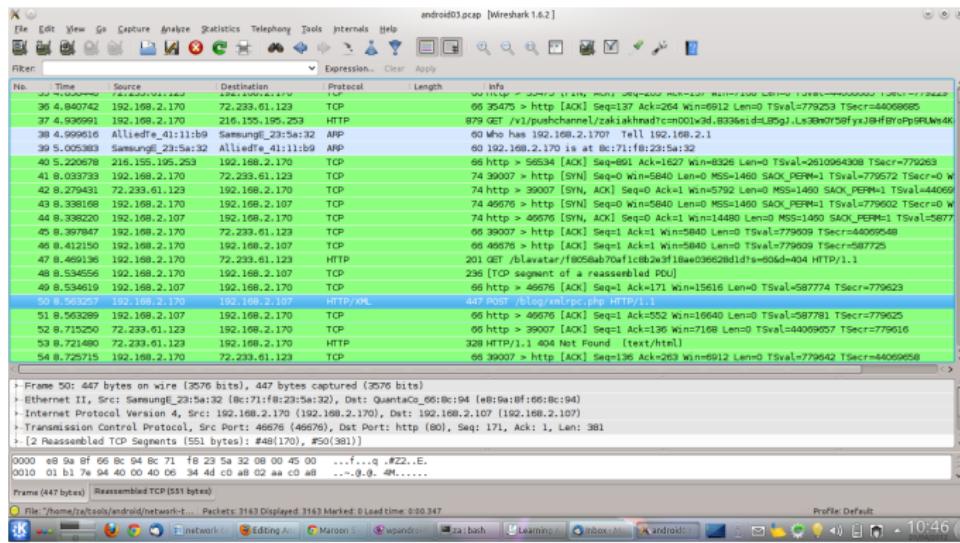
Aktivitas yang dilakukan:

- Akses sebagai publik (tanpa otentikasi)
- Melakukan otentikasi, masuk sebagai *authorized user*
- Menulis tulisan baru
- Akses menu Wordpress
- Mengubah password

## ■ Debug Aplikasi

# Pengujian Dinamis Aplikasi Wordpress

## Analisis Network Traffic



# Pengujian Dinamis Aplikasi Wordpress

## Analisis Network Traffic

The screenshot shows a NetworkMiner capture window. The top status bar says "Follow TCP Stream" and "Stream Content". The main pane displays a POST request to "/blog/xmlrpc.php" over HTTP/1.1. The request headers include:

```
POST /blog/xmlrpc.php HTTP/1.1
Content-Type: text/xml
charset: UTF-8
User-Agent: Android/2.0.7
Content-Length: 865
Host: 192.168.2.107
Connection: Keep-Alive
```

The XML payload sent in the request body is:

```
<?xml version='1.0' ?><methodCall><methodName>metaWeblog.newPost</methodName><params><param><value>c14>1</i4</value></param><param><value>za</string></value></param><param><value>stringpk1</string></value></param><param><value>struct</value></param><param><name>mt_keywords</name><value>string:credential, wordpress</value></param><param><name>post_type</name><value>string:post</value></param><param><name>title</name><value>string:Testing #2</value></param><param><name>password</name><value>string:</value></param><param><name>post_status</name><value>string:publish</value></param><param><name>description</name><value>string:lala how do this application handles credential?</value></param></params></methodCall>
```

The response from the server is:

```
Date: Fri, 20 Apr 2012 09:35:12 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.6
Connection: close
Content-Length: 159
Vary: Accept-Encoding
Content-Type: text/xml

<?xml version='1.0'?>
<methodResponse>
<params>
<param>
<value>
<string>0</string>
</value>
</param>
</params>
</methodResponse>
```

At the bottom of the window, there are various options like Bind, Save As, Print, EBCDIC, Hex Dump, C Arrays, Raw, Help, Filter Out This Stream, and Close.

# Pengujian Dinamis Aplikasi Wordpress

## Analisis Network Traffic

Follow TCP Stream  
Stream Content

```

POST /blog/wp-admin/profile.php HTTP/1.1
Host: 192.168.2.107
Accept-Encoding: gzip
Accept-Language: en-US
X-wp-profile: http://www.samsungmobile.com/uaprof/Gf-s5570.xml
Cookie: wordpress_dbe7584f29a0394e8994918aab71c5f=>a7C133506574697C987a12fa5le6f7010ea905443f947f6; wordpress_logged_in_dbe7584f29a0394e8994918aab71c5f=zakiaikhmad7C133506574697C9d5ab5c2abaaed741533e02cc2f5; wordpress_test_cookie=WP+Cookie+check; wp-settings-1=mfd930e; wp-settings-time-1=1334802946
Accept-Charset: utf-8, iso-8859-1, utf-16, ;q=0.7
Referer: http://192.168.2.107/blog/wp-admin/profile.php
User-Agent: wp-android
Origin: http://192.168.2.107
Accept: application/xml,application/xhtml+xml,application/xml;text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 313

_wpnonce=30e10356939e_wp_http_referer=%2Fblog%2Fwp-admin%
&profile.php&from=profile&checkuser_id=1&admin_color=fresh&admin_bar_front=1&first_name=&last_name=&nickname=&display_name=zakiakhmad%
4@gmail.com&url=&ain=syin=&jabbers=&description=&pass1=z1k&pass2=z1k&action=update&user_id=1&submit=Update+ProfileHTTP/1.1 302 Found
Date: Fri, 20 Apr 2012 03:38:00 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.6
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Fri, 20 Apr 2012 03:38:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/wp-admin
Set-Cookie: wordpress_sec_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/wp-admin
Set-Cookie: wordpress_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/wp-content/plugins
Set-Cookie: wordpress_sec_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/wp-content/plugins
Set-Cookie: wordpress_logged_in_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/
Set-Cookie: wordpress_logged_in_dbe7584f29a0394e8994918aab71c5f=>; expires=Thu, 21-Apr-2011 03:38:00 GMT; path=/blog/

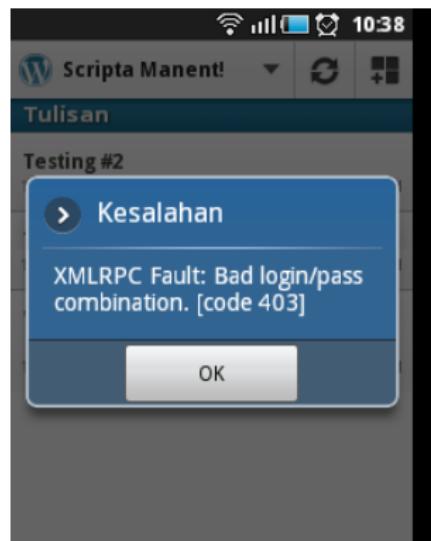
```

Entire conversation (40827 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw Filter Out This Stream Close Help

# Pengujian Dinamis Aplikasi Wordpress

## Analisis Network Traffic



# Pengujian Dinamis Aplikasi Wordpress

## Debug Aplikasi

Mencari informasi sensitif yang tersimpan dalam device

- 1 List device menggunakan adb
- 2 Masuk ke shell
- 3 Cari direktori database aplikasi
- 4 Gunakan perintah dump untuk melihat isi database

# Pengujian Statis Aplikasi Wordpress

```

Berkas  Sunting  Tampilan  Penanda  Pengaturan  Bantuan
src/org/wordpress/android/ViewPosts.java:834;                                WordPress.currentBlog.getHttpPassword());
src/org/wordpress/android/Read.java:41: private String httppassword = "";           handler.proceed(httpuser, httppassword);
src/org/wordpress/android/Read.java:226;                                         + "<input type=\"password\" name=\"pwd\" id=\"user_pass\" value=\"\""
src/org/wordpress/android/Read.java:298:
src/org/wordpress/android/Settings.java:86;     EditText passwordET = (EditText)findViewById(R.id.password);
src/org/wordpress/android/Settings.java:87;     passwordET.setText(WordPress.currentBlog.getPassword());
src/org/wordpress/android/Settings.java:92;     EditText httpPasswordET = (EditText)findViewById(R.id.httppassword);
src/org/wordpress/android/Settings.java:93;     httpPasswordET.setText(WordPress.currentBlog.getHttpPassword());
src/org/wordpress/android/Settings.java:94;     TextView httpPasswordLabel = (TextView) findViewById(R.id.l_httppassword);
src/org/wordpress/android/Settings.java:175;    EditText passwordET = (EditText)findViewById(R.id.password);
src/org/wordpress/android/Settings.java:176;    WordPress.currentBlog.setPassword(passwordET.getText().toString());
src/org/wordpress/android/Settings.java:179;    EditText httpPasswordET = (EditText)findViewById(R.id.httppassword);
src/org/wordpress/android/Settings.java:180;    WordPress.currentBlog.setHttpPassword(httpPasswordET.getText().toString());
src/org/wordpress/android/WordpressDB.java:32;   + "url text, blogName text, username text, password text, imagePlacement text, center
Thumbnail boolean, fullSizeImage boolean, maxWidthWidth text, maxImageWidthId integer, lastCommentId integer, runService boolean";
src/org/wordpress/android/WordpressDB.java:45;   + "wp_author display_name text default '', wp_author_id text default '', wp_password
" text default '', wp_post format text default '', wp_slug text default '', mediaPaths text default ''."
src/org/wordpress/android/WordpressDB.java:80;   private static final String ADD_DOTCOM_PASSWORD = "alter table accounts add dotcom_password text;" ;
src/org/wordpress/android/WordpressDB.java:88; // add httpuser and httppassword
src/org/wordpress/android/WordpressDB.java:90; private static final String ADD_HTTPPASSWORD = "alter table accounts add httppassword text;" ;
src/org/wordpress/android/WordpressDB.java:353;   "categories", "tags", "status", "password",
src/org/wordpress/android/WordpressDB.java:388;   "status", "password" }, null, null, null, null,
src/org/wordpress/android/WordpressDB.java:423;   String password, String httpuser, String httppassword,
src/org/wordpress/android/WordpressDB.java:432;   values.put("password", encryptPassword(password));
src/org/wordpress/android/WordpressDB.java:434;   values.put("httppassword", encryptPassword(httppassword));
src/org/wordpress/android/WordpressDB.java:533;   String password, String httpuser, String httppassword,
src/org/wordpress/android/WordpressDB.java:542;   values.put("password", encryptPassword(password));
src/org/wordpress/android/WordpressDB.java:544;   values.put("httppassword", encryptPassword(httppassword));
src/org/wordpress/android/WordpressDB.java:553;   values.put("dotcom_password", encryptPassword(dotcomPassword));
src/org/wordpress/android/WordpressDB.java:562;   userPass.put("password", encryptPassword(password));
src/org/wordpress/android/WordpressDB.java:615;   "username", "password", "httpuser", "httppassword",
src/org/wordpress/android/WordpressDB.java:618;   "location", "dotcomFlag", "dotcom_username", "dotcom_password",
--Lebih...

```

Mencari kata password

# Pengujian Dinamis Aplikasi Twitter

## ■ Analisis *Network Traffic*

Aktivitas yang dilakukan:

- Install aplikasi Twitter untuk Android dari Google Play
- Jalankan kali pertama
- Login
- Twit

## ■ Debug Aplikasi

# Pengujian Dinamis Aplikasi Twitter

## Analisis Network Traffic

Follow TCP Stream Stream Content

```

GET /market/download/Download
Accept: application/x-m泗n+json
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win32; rv:10.0) Gecko/20100101 Firefox/10.0
Cookie: _ga=GA1.1.1699557948.1314942593
Host: android.clients.google.com
Connection: Keep-Alive
User-Agent: AndroidDownloadManager

HTTP/1.1 302 Moved Temporarily
Cache-control: no-cache
Location: http://o-s.preferred.matrix-cgk1.v5.lcache6.c.android.clients.google.com/market/GetBinary/com.twitter.android/1537
expires=1322033235&signature=0911940C8767C3E4471B01D8FA1P00AeABcc05
Date: Fri, 20 Apr 2012 08:28:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
X-Content-Type-Options: nosniff
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE
Transfer-Encoding: chunked

213
deflate
gzip
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Content-Length: 1000000000
Last-Modified: Fri, 20 Apr 2012 08:28:10 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
<head>
<title>Moved Temporarily</title>
</head>
<body>
<div style="background-color:#FFFFFF; text-align:center; width:100%; height:100%; position: absolute; top: 0; left: 0; z-index: 1;>
The document has moved <a href="http://o-s.preferred.matrix-cgk1.v5.lcache6.c.android.clients.google.com/market/GetBinary/com.twitter.android/1537
expires=1322033235&signature=0911940C8767C3E4471B01D8FA1P00AeABcc05">here</a>.
</div>
</body>
</html>

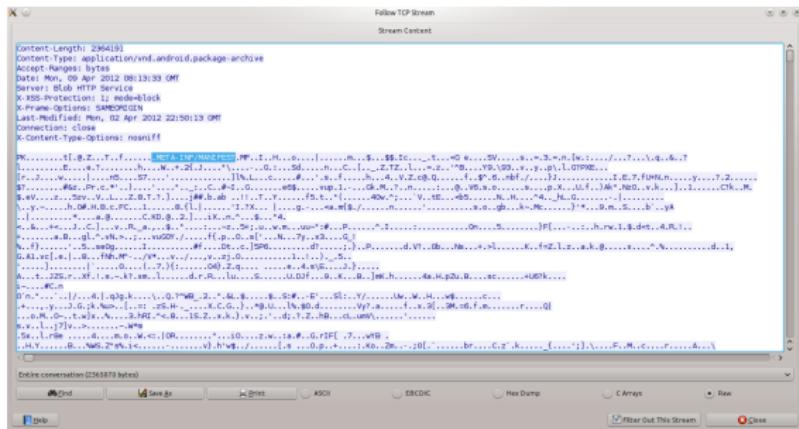
```

Entire conversation (151 bytes)

Raw Save As Print ASCII Hex Dump C Arrays Filter Out This Stream Close

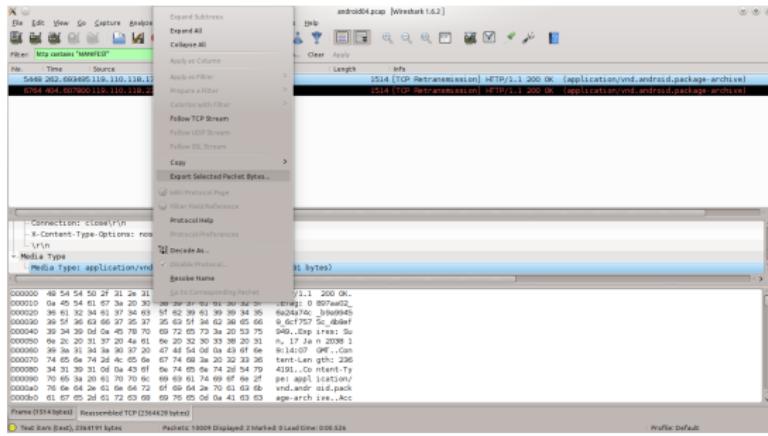
# Pengujian Dinamis Aplikasi Twitter

## Analisis Network Traffic



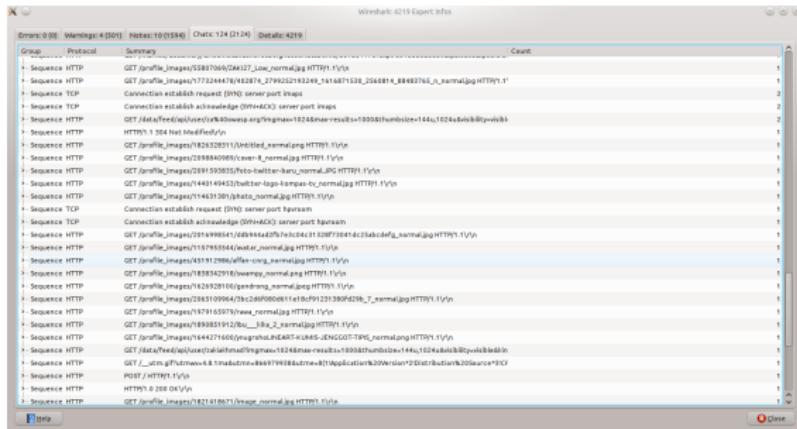
# Pengujian Dinamis Aplikasi Twitter

## Analisis Network Traffic



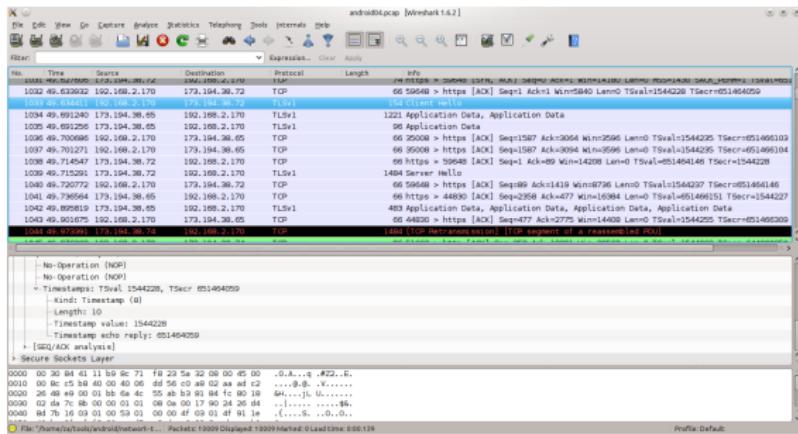
# Pengujian Dinamis Aplikasi Twitter

## Analisis Network Traffic



# Pengujian Dinamis Aplikasi Twitter

## Analisis Network Traffic



# Pengujian Dinamis Aplikasi Twitter

## Debug Aplikasi

Mencari informasi sensitif yang tersimpan dalam device

- 1 Dapatkan file .apk Twitter untuk Android
- 2 Install aplikasi pada emulator
- 3 Cari direktori database
- 4 Dump database

# Pengujian Dinamis Aplikasi Twitter



```

Berkas  Sunting  Tampilan  Penanda  Pengaturan  Bantuan
twitter : adb
N statuses,_author_id=user.user_id LEFT JOIN users AS sender ON status.groups.sender_id=sender.user_id;
CREATE VIEW user_groups_view AS SELECT user.groups._id AS _id,user.groups.type AS type,user.groups.tag AS tag,user.groups.owner_id AS owner_id,user.g
roups.user_id AS user_id,user.groups.is_last AS is_last,user.groups.pc AS pc,user.groups.g_flags AS g_flags,user.username AS username,user.name AS na
me,user.description AS description,user.web_url AS web_url,user.bg_color AS bg_color,user.location AS location,user.protected AS protected,user.verif
ied AS verified,user.profile_created AS profile_created,user.image_url AS image_url,user.followers AS followers,user.friends AS friends,user.statuses
AS statuses,user.geo_enabled AS geo_enabled,user.image AS image,user.friendship AS friendship,user.friendship_time AS friendship_time FROM user_grou
ps LEFT JOIN users AS user ON user_groups.user_id=user.user_id;
CREATE VIEW messages_received_view AS SELECT messages._id AS _id,messages.type AS type,messages.msg_id AS msg_id,messages.content AS content,messages
.created AS created,messages.sender_id AS sender_id,messages.recipient_id AS recipient_id,messages.is_read AS is_read,messages.is_last AS is_last,use
rs.username AS username,users.name AS name,users.image_url AS image_url,users.image AS image FROM messages,users WHERE messages.sender_id=users.user_
id;
CREATE VIEW messages_sent_view AS SELECT messages._id AS _id,messages.type AS type,messages.msg_id AS msg_id,messages.content AS content,messages.cre
ated AS created,messages.sender_id AS sender_id,messages.recipient_id AS recipient_id,messages.is_read AS is_read,messages.is_last AS is_last,users.u
sername AS username,users.name AS name,users.image_url AS image_url,users.image AS image FROM messages,users WHERE messages.recipient_id=users.user_i
d;
CREATE VIEW messages_threaded AS SELECT * FROM (SELECT messages.* ,r.username r.name,r.image_url r.profile_image_url,s.username s.us
ername,s.name s.image_url s.profile_image_url FROM messages LEFT JOIN users r ON recipient_id=r.user_id LEFT JOIN users s ON sender_id=s.user_
id ORDER BY created ASC) GROUP BY thread;
CREATE VIEW messages_conversation AS SELECT messages.* ,s.username s.username,s.name s_name,s.image_url s.profile_image_url FROM messages LEFT JOIN us
ers s ON sender_id=s.user_id;
CREATE VIEW lists_view AS SELECT lists._id AS _id,lists.owner_id AS owner_id,lists.type AS type,lists.list_id AS list_id,lists.list_name AS list_name
,lists.full_name AS full_name,lists.description AS description,lists.subscribers AS subscribers,lists.members AS members,lists.mode AS mode,lists.cre
ator_id AS creator_id,lists.i_follow AS i_follow,lists.is_last AS is_last,users.username AS username,users.name AS name,users.image_url AS image_url
,users.image AS image FROM lists,users WHERE lists.creator_id=users.user_id;
CREATE VIEW status_groups_retweets_view AS SELECT status.groups_view.* ,retweets.* FROM status.groups_view LEFT JOIN ( SELECT q_status_id AS rt_orig_
status_id,ref_id AS rt_orig_ref_id FROM status.groups_view WHERE type=0 AND tweet_type=1 AND sender_id=owner_id GROUP BY rt_orig_status_id ) AS retwee
ts ON (retweets.rt_orig_status_id=status.groups_view.q_status_id);
CREATE VIEW slug_users_view AS SELECT search_queries._id AS _id,search_queries.name AS name,search_queries.query AS query,search_queries.query_id AS
query_id,user_groups_view.username AS username,user_groups_view.id AS user_id,user_groups_view.image_url AS image_url,user_groups_view.image AS
image FROM search_queries LEFT JOIN user_groups_view ON search_queries.query_id=user_groups_view.tag WHERE user_groups_view.type=6;
CREATE VIEW user_recommendations_view AS SELECT u.*,c.user_id AS conn_user_id,c.username AS conn_username,c.name AS conn_name FROM user_groups_view A
S u LEFT OUTER JOIN user_groups_view AS c ON u.user_id=c.tag WHERE (u.type=9 OR u.type=10) AND u.tag=-1 ORDER BY u._id;
COMMIT;
sqlite: 

```

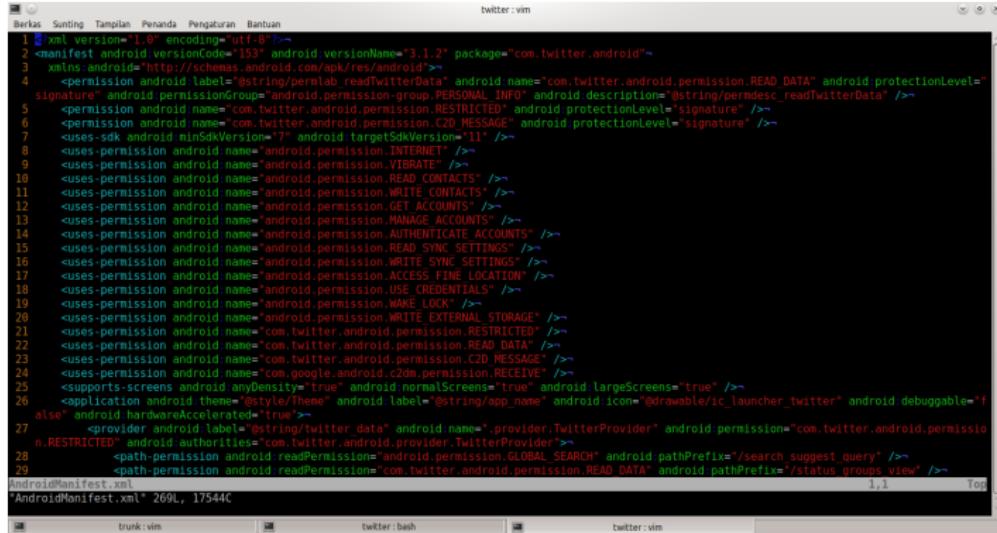
Dump database twitter

# Pengujian Statis Aplikasi Twitter

Lakukan *reverse engineering*

- 1 unzip twitter.apk
- 2 Gunakan apk tool untuk mendapatkan berkas AndroidManifest.xml dalam format *plain text*.
- 3 Analisis berkas AndroidManifest.xml

# Pengujian Statis Aplikasi Twitter



```

Berkas Sunting Tampilan Penanda Pengaturan Bantuan
twitter:vim
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest android:versionCode="153" android:versionName="3.1.2" package="com.twitter.android">
3   <uses-sdk android:minSdkVersion="7" android:targetSdkVersion="11" />
4     <permission android:name="com.twitter.android.permission.READ_TWITTER_DATA" android:name="com.twitter.android.permission.READ_DATA" android:protectionLevel="signature" android:permissionGroup="android.permission_group.PERSONAL_INFO" android:description="@string/permdesc_readTwitterData" />
5     <permission android:name="com.twitter.android.permission.RESTRICTED" android:protectionLevel="signature" />
6     <uses-permission android:name="com.twitter.android.permission.C2D_MESSAGE" android:protectionLevel="signature" />
7     <uses-permission android:name="android.permission.INTERNET" />
8     <uses-permission android:name="android.permission.VIBRATE" />
9     <uses-permission android:name="android.permission.READ_CONTACTS" />
10    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
11    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
12    <uses-permission android:name="android.permission.MANAGE_ACCOUNTS" />
13    <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS" />
14    <uses-permission android:name="android.permission.READ_SYNC_SETTINGS" />
15    <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS" />
16    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
17    <uses-permission android:name="android.permission.USE_CREDENTIALS" />
18    <uses-permission android:name="android.permission.WAKE_LOCK" />
19    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
20    <uses-permission android:name="com.twitter.android.permission.RESTRICTED" />
21    <uses-permission android:name="com.twitter.android.permission.READ_DATA" />
22    <uses-permission android:name="com.twitter.android.permission.C2D_MESSAGE" />
23    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE" />
24    <supports-screens android:anyDensity="true" android:normalScreens="true" android:largeScreens="true" />
25  <application android:theme="@style/Theme" android:label="@string/app_name" android:icon="@drawable/ic_launcher_twitter" android:debuggable="false" android:hardwareAccelerated="true">
26    <provider android:name="com.twitter.data.provider.TwitterProvider" android:permission="com.twitter.android.permission.RESTRICTED" android:authorities="com.twitter.android.provider.TwitterProvider">
27      <path-permission android:readPermission="android.permission.GLOBAL_SEARCH" android:pathPrefix="/search_suggest_query" />
28      <path-permission android:readPermission="com.twitter.android.permission.READ_DATA" android:pathPrefix="/status_groups_view" />
AndroidManifest.xml 1,1 1,1 Top
"AndroidManifest.xml" 269L, 17544C
trunk:vim          trunks:bash

```

Berkas AndroidManifest.xml Twitter

# Kesimpulan

## Kesimpulan

### 1 Wordpress untuk Android

- 1 Setiap melakukan request, UserID dan Password dikirim dalam keadaan clear text.
- 2 UserID dan password tersimpan dalam database dalam format clear text.

### 2 Twitter untuk Android

- 1 Menggunakan transport layer terenkripsi saat mengakses server
- 2 UserID dan password tersimpan dalam keadaan terenkripsi
- 3 Direct message tersimpan dalam format clear text

# Saran

## Saran

- 1 Pada pengujian dinamis, lakukan *intercept traffic* antara aplikasi dengan server menggunakan *proxy* sehingga dapat dilakukan analisis lebih mendalam
- 2 Pada pengujian statis, pelajari lebih detail bagaimana mengembangkan aplikasi Android (atau aplikasi mobile pada umumnya) sehingga dapat melakukan *code review* lebih baik

# Referensi

- APK-Tool
- Jack Maninno, Reversing Android Apps 101
- Jeff Six, Application Security for the Android Platform, O'Reilly
- OWASP Mobile Security Project
- Situs Pengembang Android
- Situs Pengembang Twitter
- Situs Pengembang Wordpress

# Terima Kasih



*kurru sumanga  
thank you, arigatou, danke, merci beaucoup*

foto-foto flickr.com/zakiakhmad