Pengujian Keamanan Aplikasi Mobile

Studi Kasus: Android

Zaki Akhmad

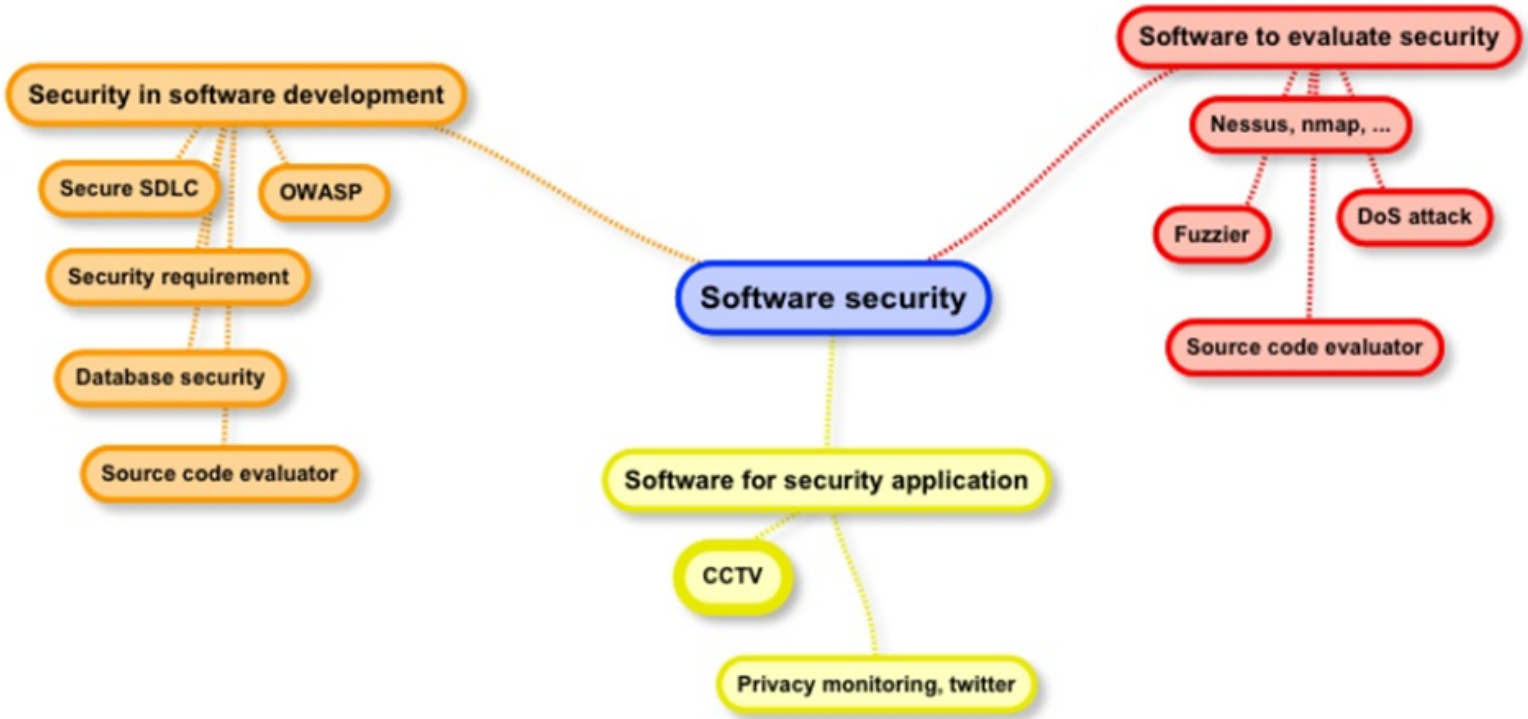
indocisc

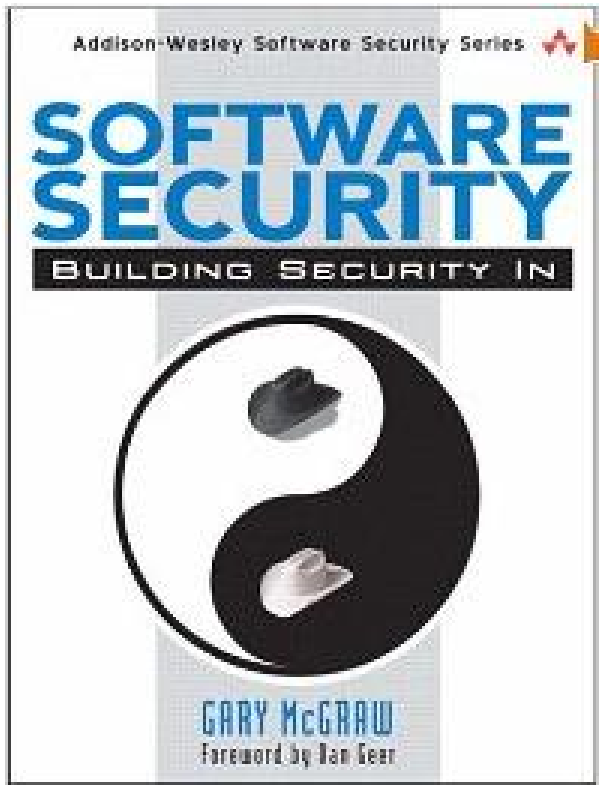
10 Juni 2012

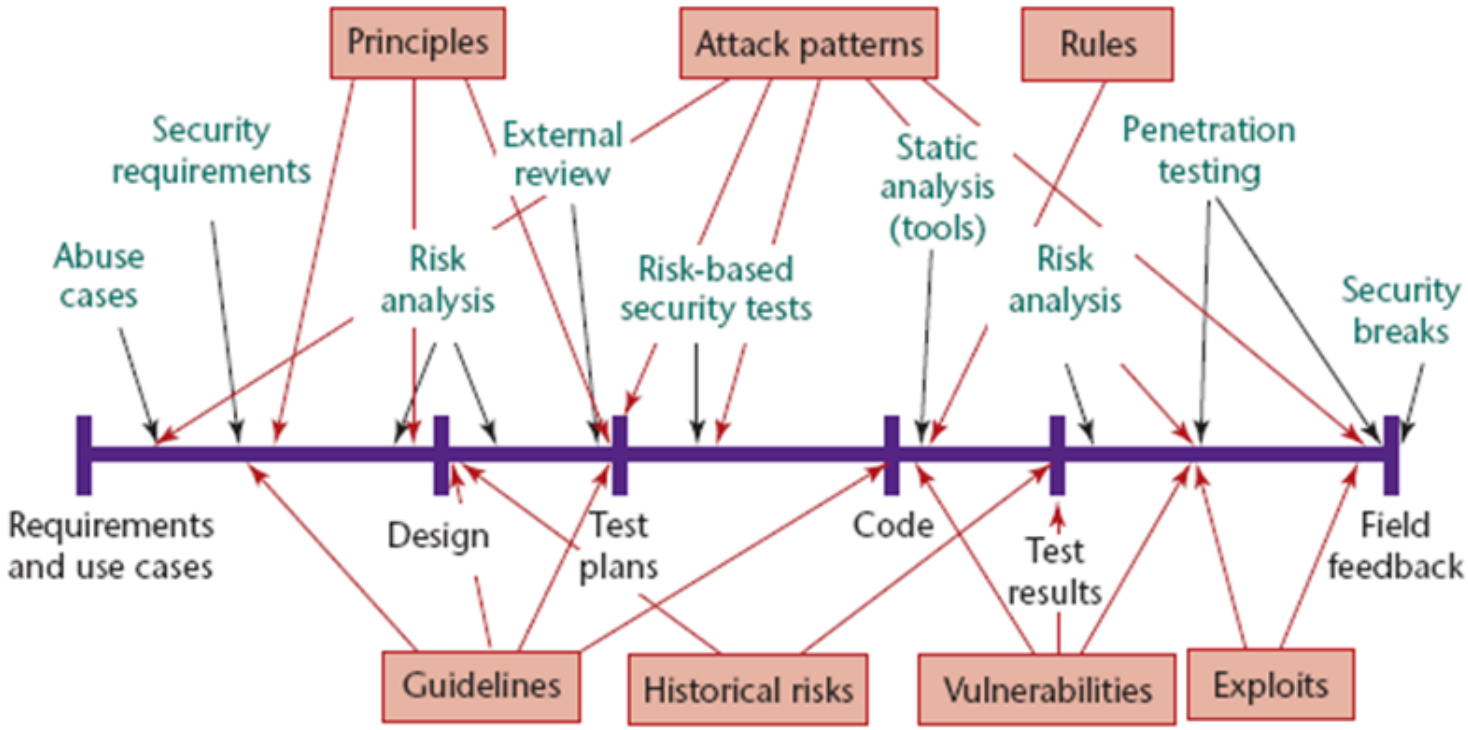
Tentang Zaki Akhmad

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)


Software to evaluate security
Security in software development
Nessus, nmap, ...
Secure SDLC
OWASP
Fuzzier
DoS attack
Security requirement
Software security
Database security
Source code evaluator
Source code evaluator
Software for security application
CCTV
Privacy monitoring, twitter


Addison-Wesley Software Security Series
SOFTWARE SECURITY
BUILDING SECURITY IN
GARY McGRAW
Foreword by Dan Geer


Principles
Attack patterns
Rules
Security requirements
External review
Static analysis (tools)
Penetration testing
Abuse cases
Risk analysis
Risk-based security tests
Risk analysis
Security breaks
Requirements and use cases
Design
Test plans
Code
Test results
Field feedback
Guidelines
Historical risks
Vulnerabilities
Exploits

Daftar Isi

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
```

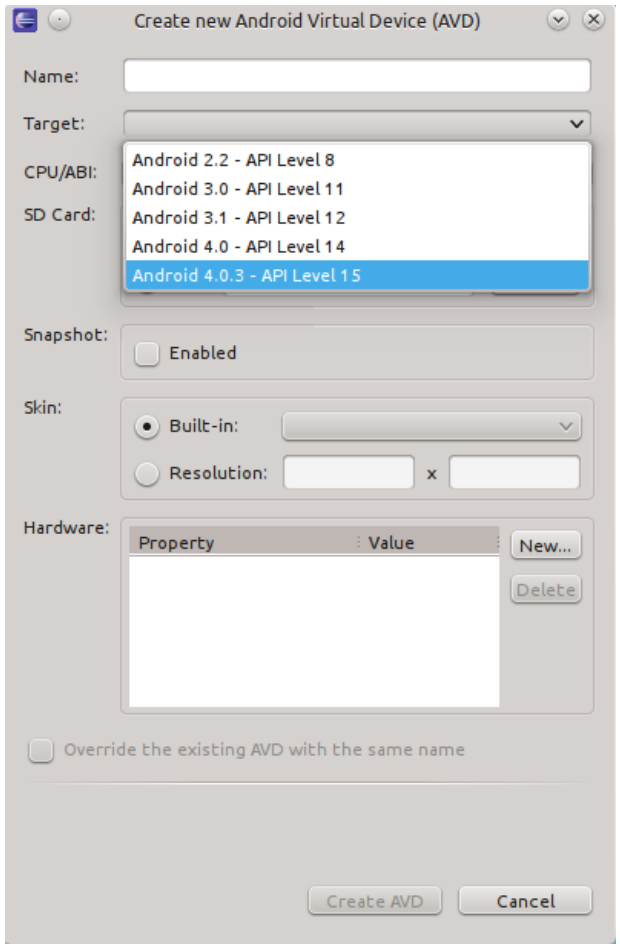
Konfigurasi Lab

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

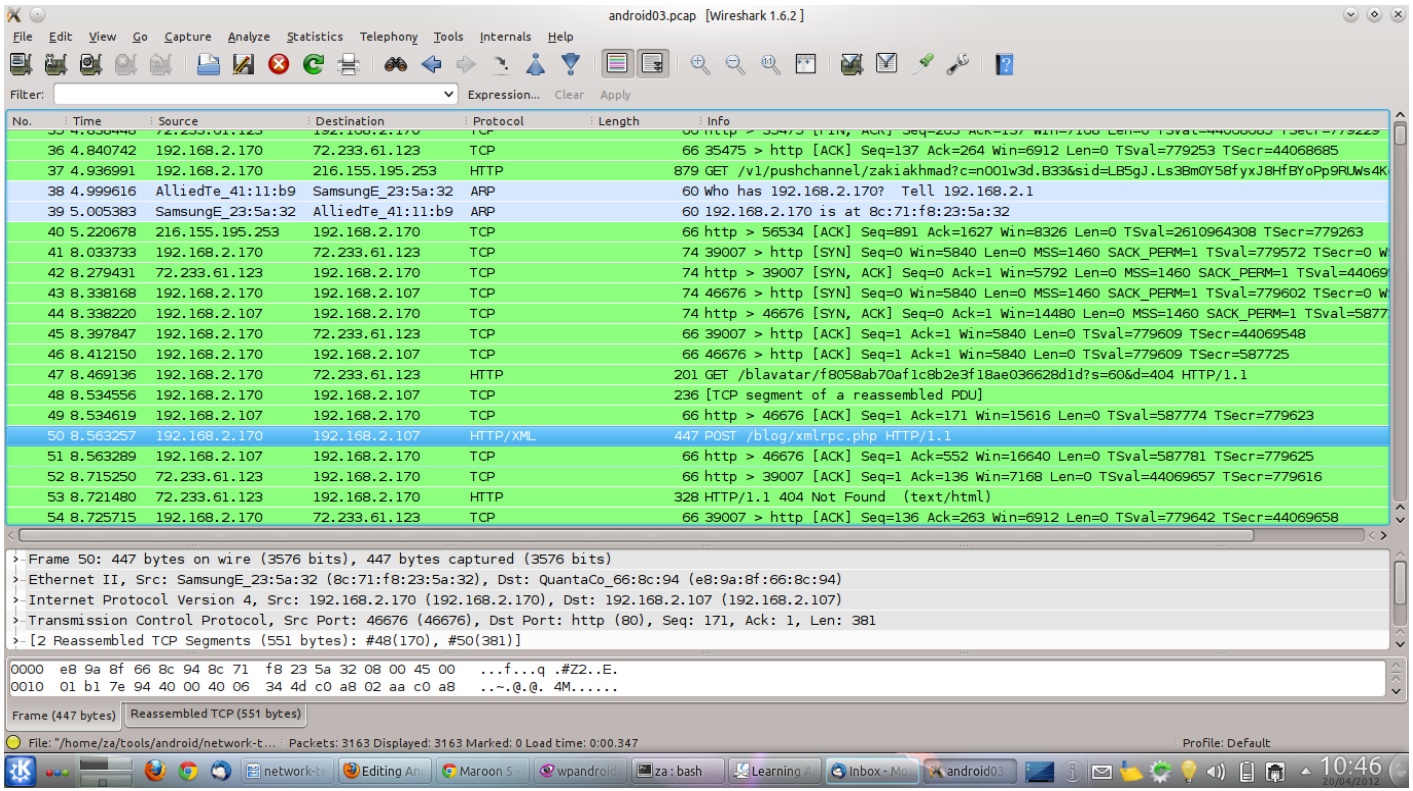
1. Dapatkan aplikasi
   1. Ekstrak aplikasi dari device
   2. Dapatkan berkas installer dari pengembang
2. Lakukan *reverse engineering*
3. Lakukan *source code review*

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

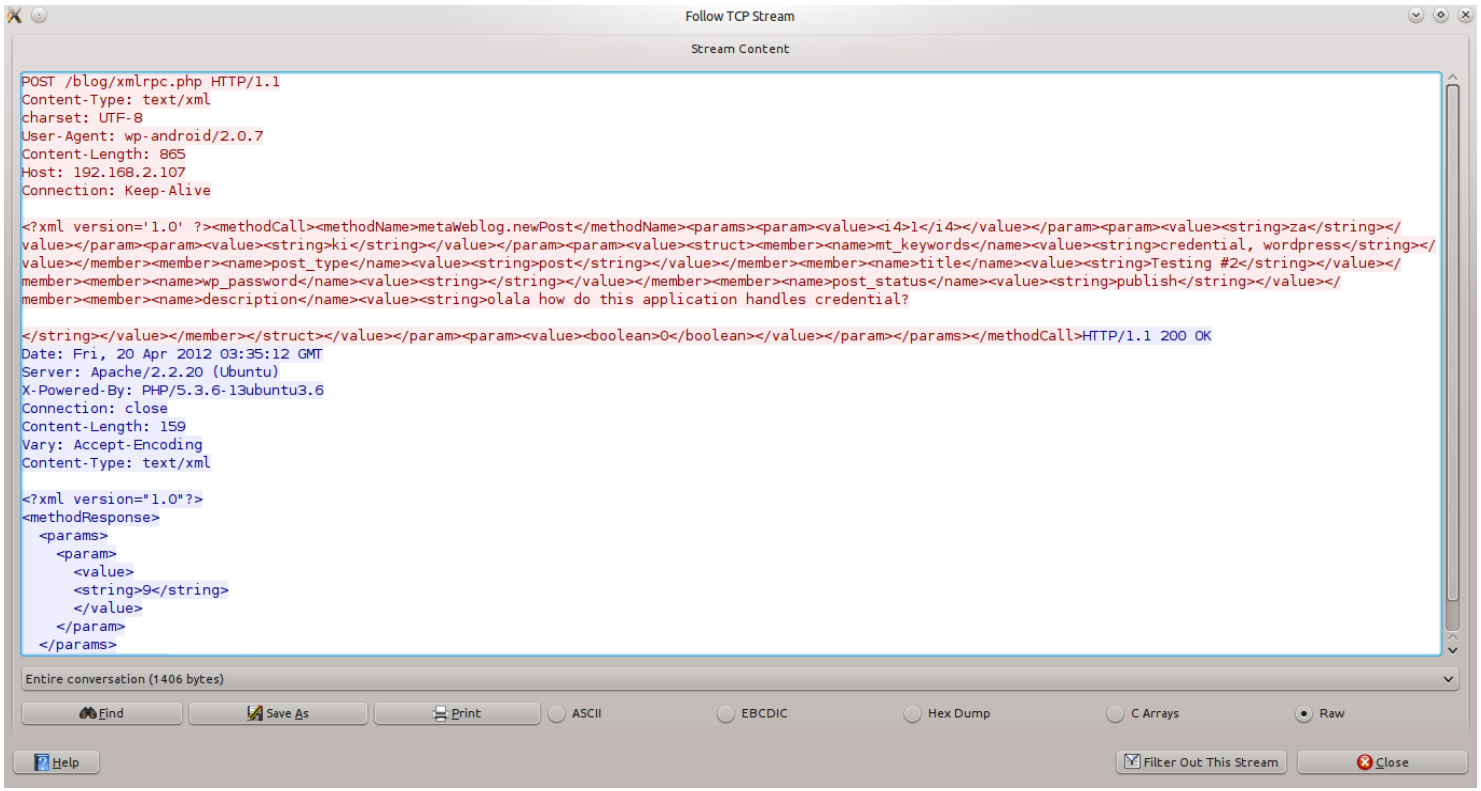
Pengujian Dinamis Aplikasi Wordpress

Analisis *Network Traffic*



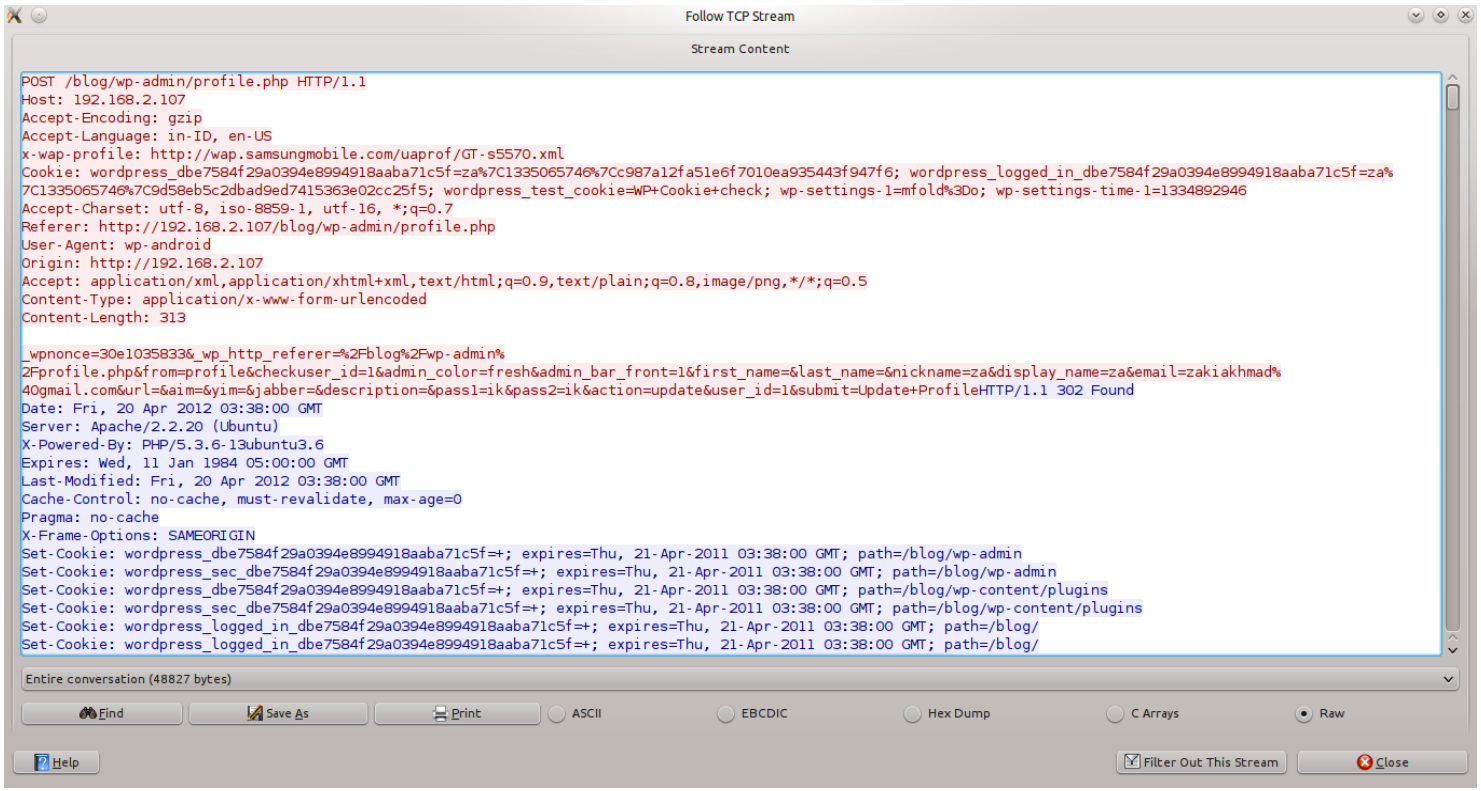
Pengujian Dinamis Aplikasi Wordpress

Analisis *Network Traffic*



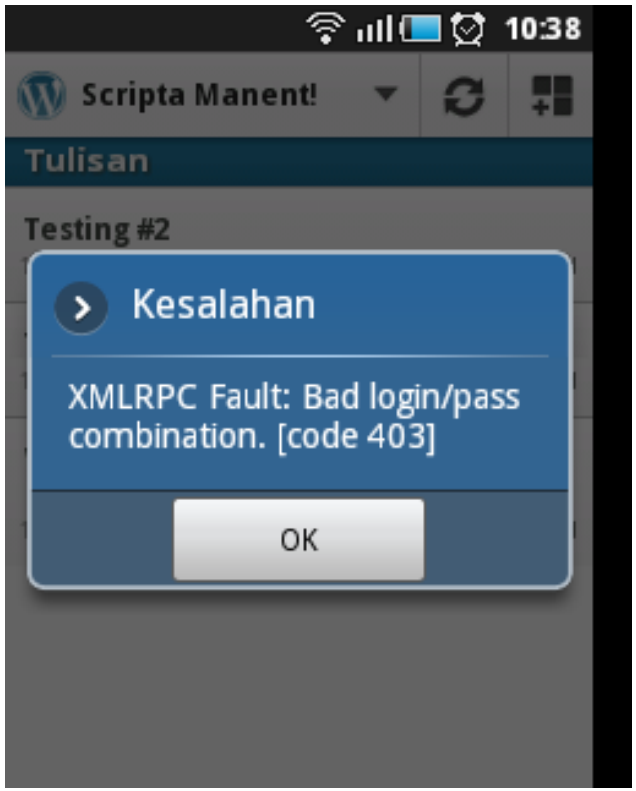
Pengujian Dinamis Aplikasi Wordpress

Analisis *Network Traffic*



Pengujian Dinamis Aplikasi Wordpress

Analisis *Network Traffic*



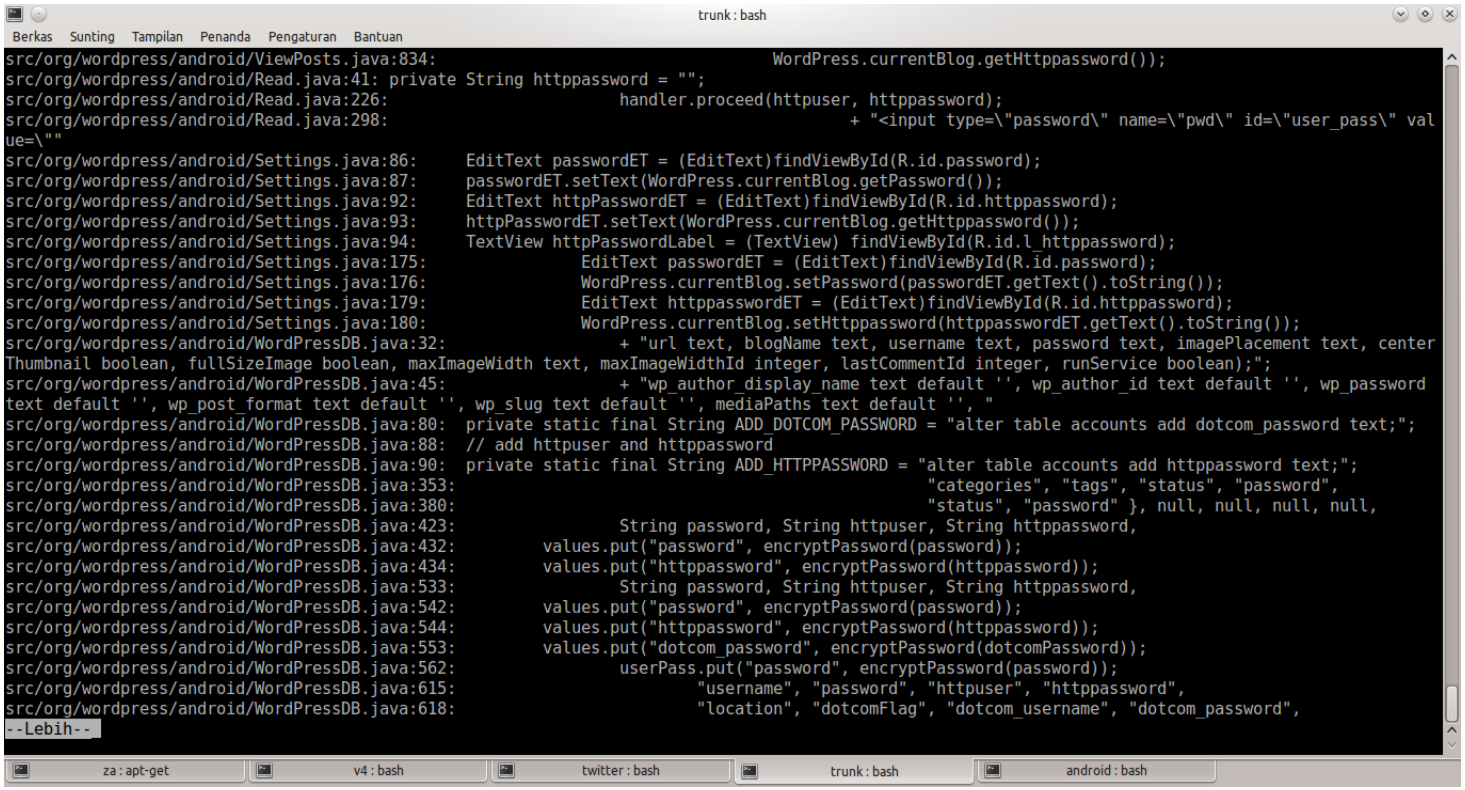
Pengujian Dinamis Aplikasi Wordpress

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



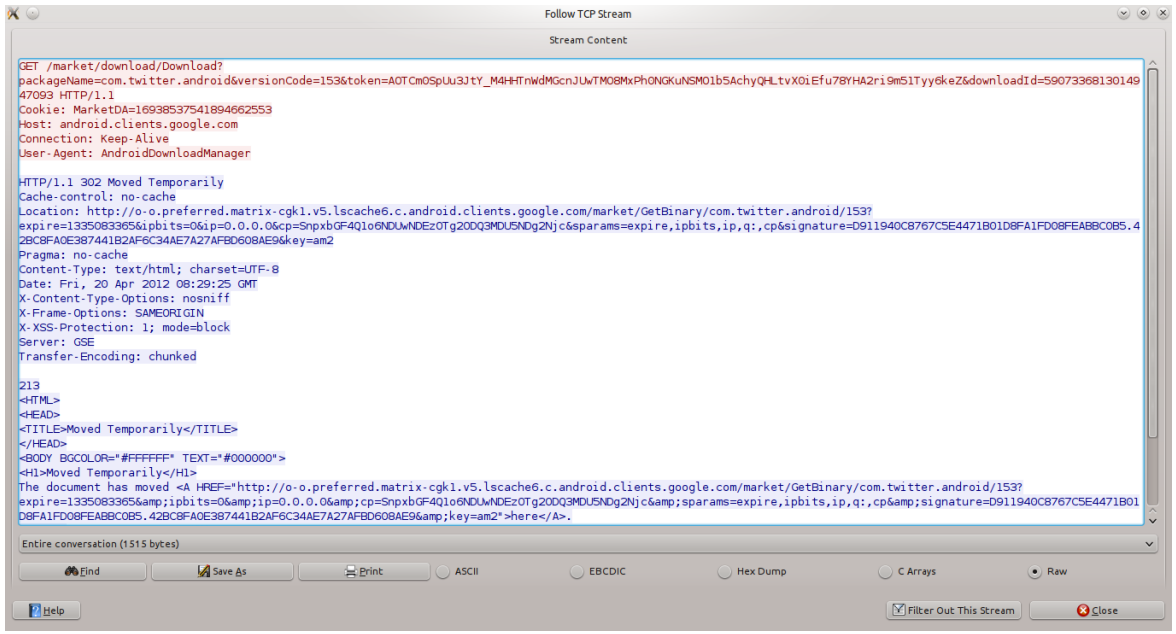
Mencari kata `password`

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

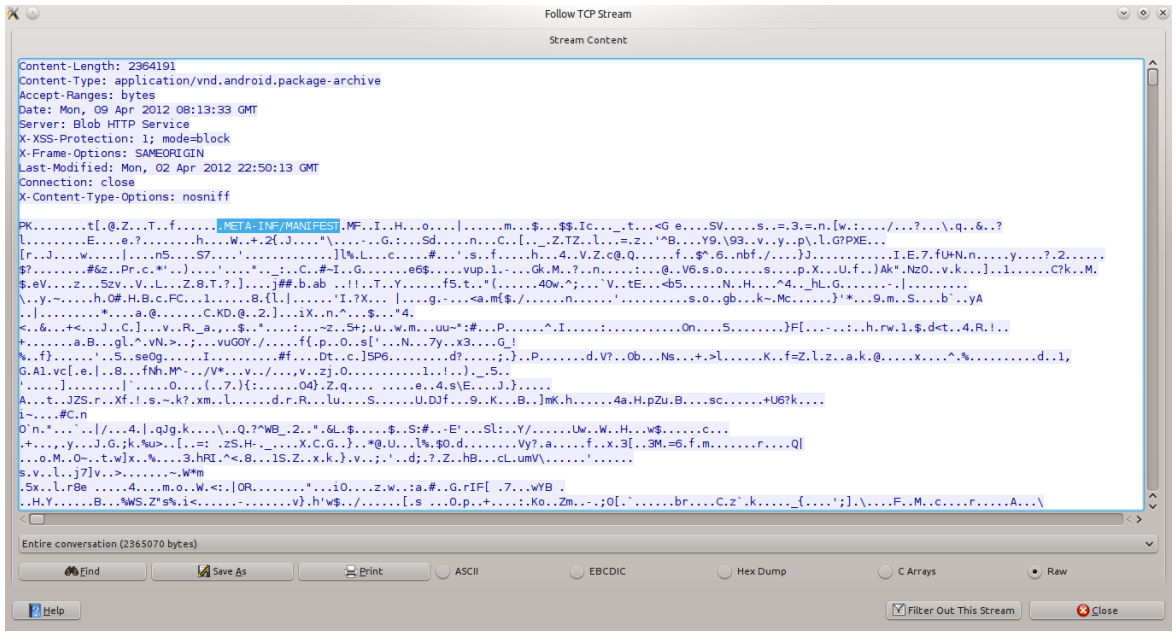
Pengujian Dinamis Aplikasi Twitter

Analisis *Network Traffic*



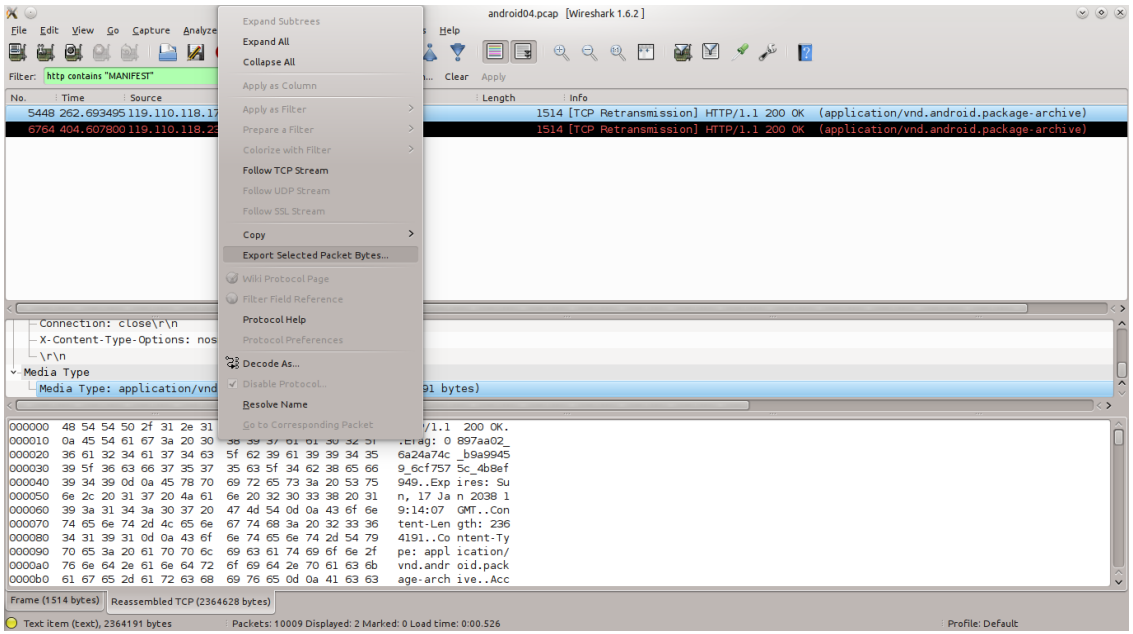
Pengujian Dinamis Aplikasi Twitter

Analisis *Network Traffic*



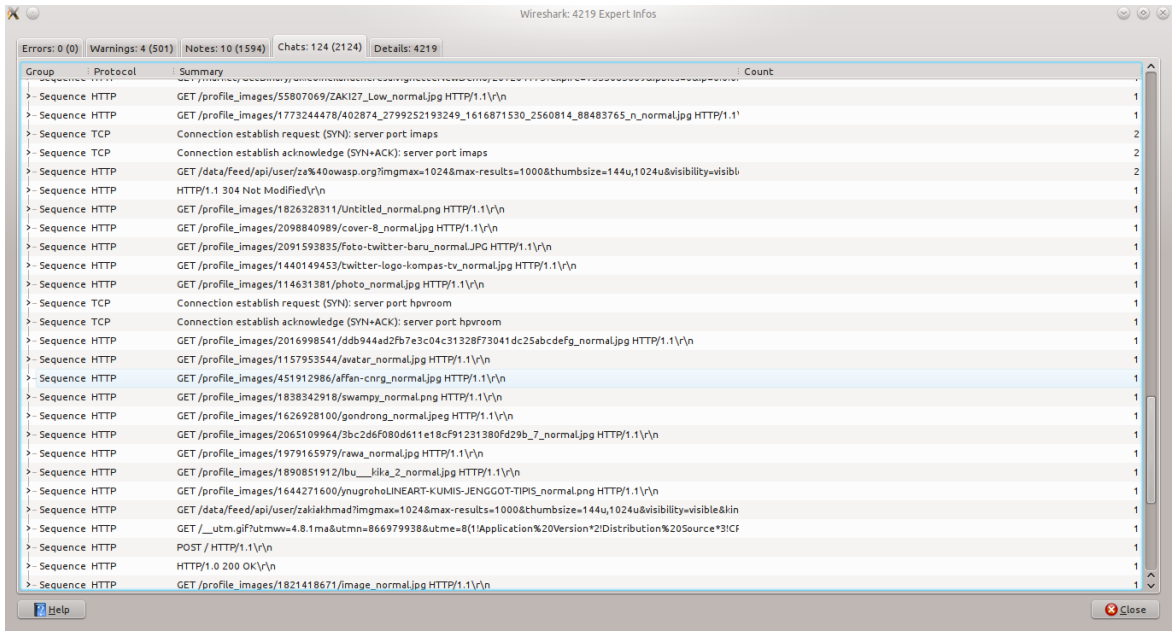
Pengujian Dinamis Aplikasi Twitter

Analisis *Network Traffic*



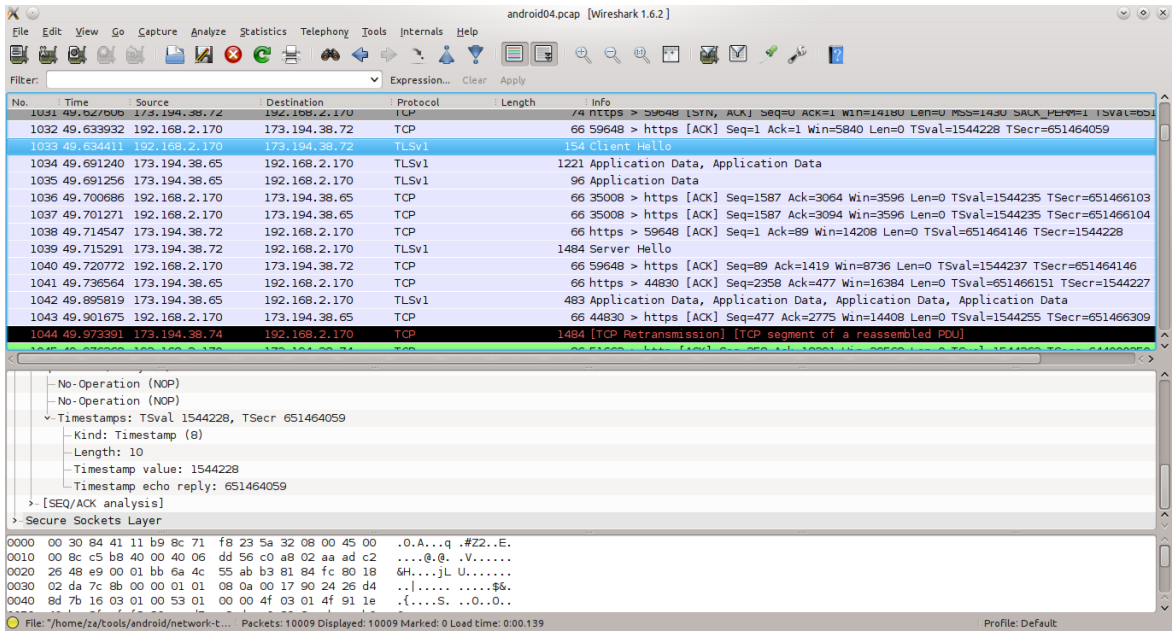
Pengujian Dinamis Aplikasi Twitter

Analisis *Network Traffic*



Pengujian Dinamis Aplikasi Twitter

Analisis *Network Traffic*



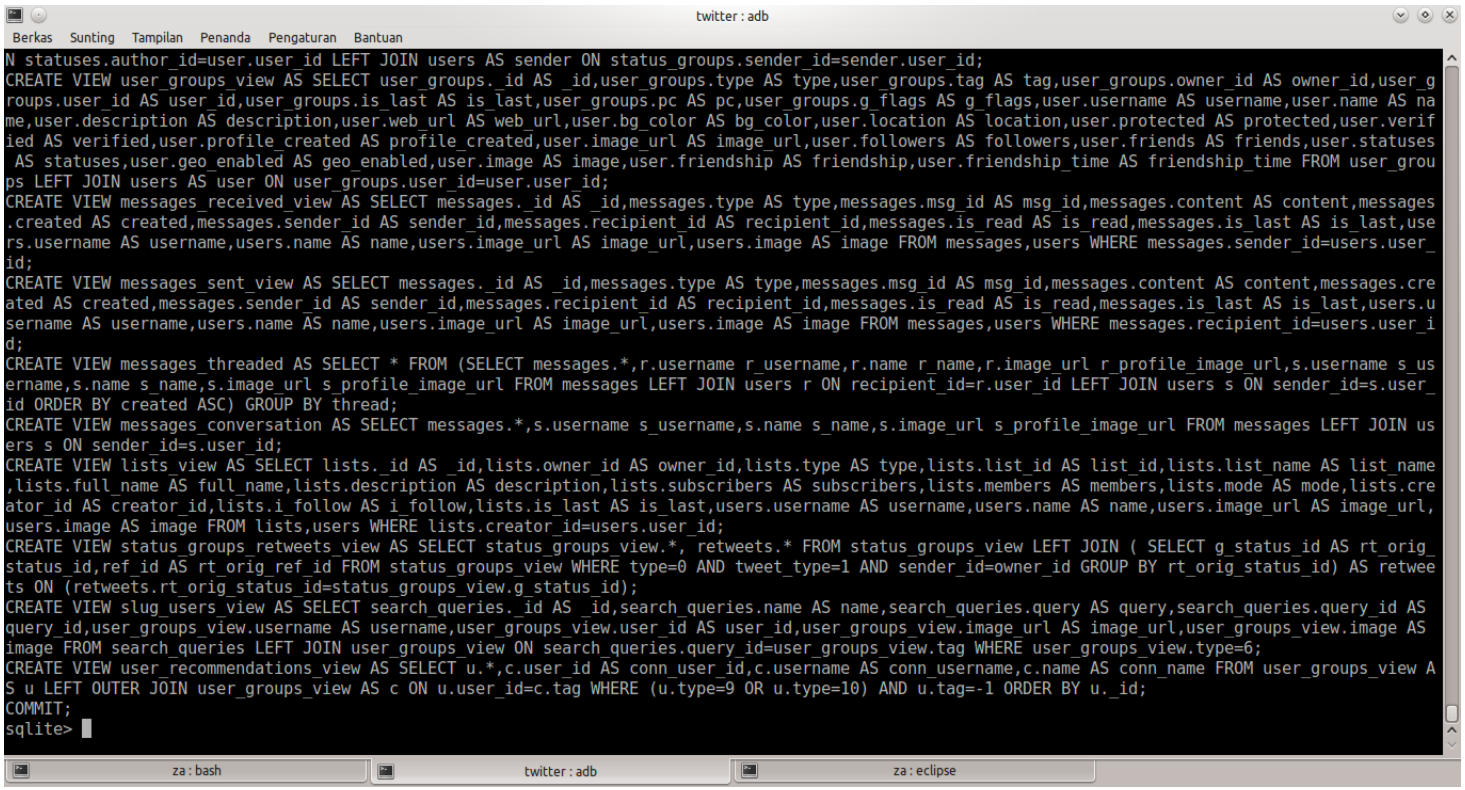
Pengujian Dinamis Aplikasi Twitter

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



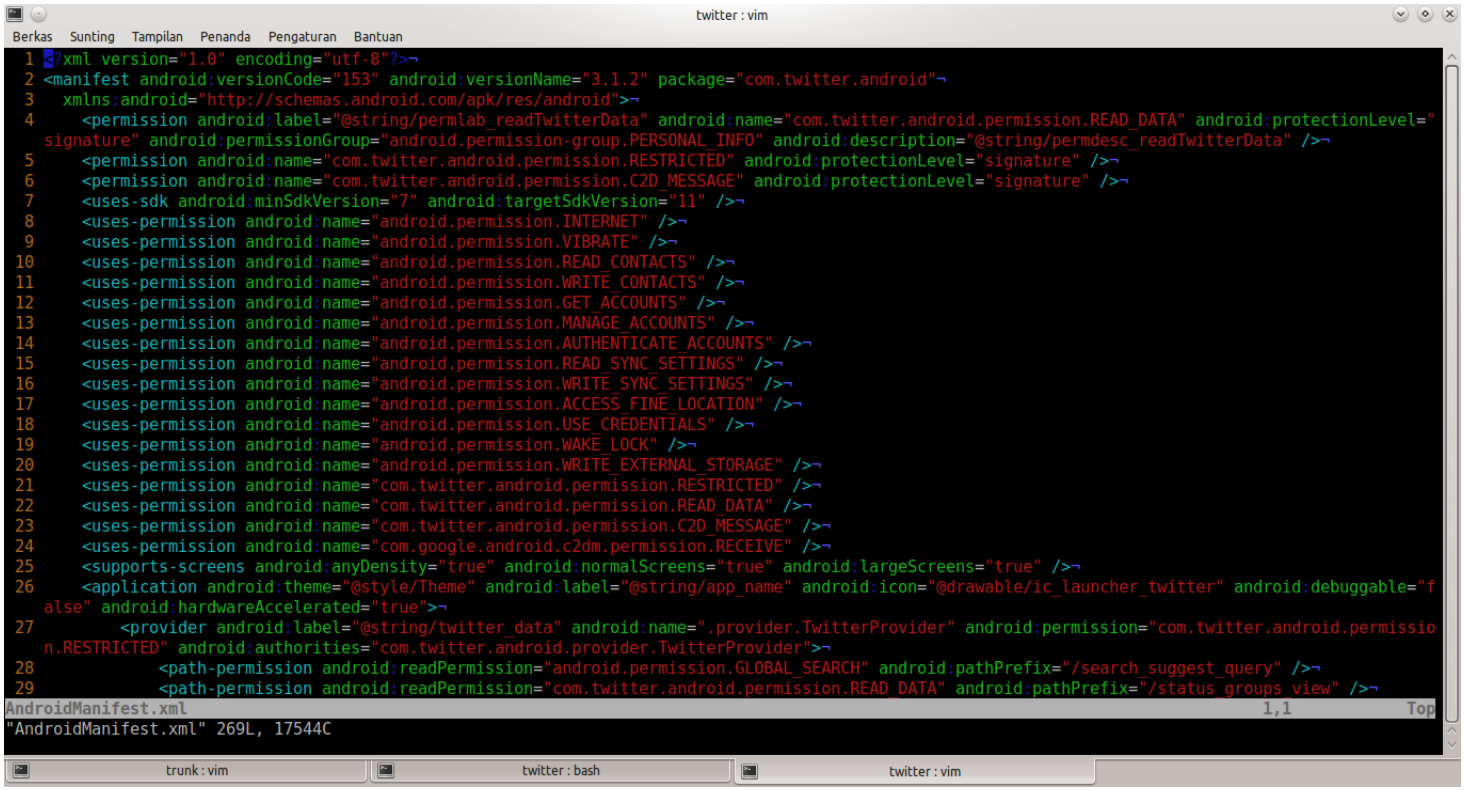
Dump database twitter

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 `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