Perancangan Metode Kriptanalisis terhadap Web Studi Kasus : Situs Jejaring Sosial

Aqsath Rasyid Naradhipa – NIM : 13506006
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganeca 10, Bandung
E-mail : aqsath@gmail.com

Abstrak

Makalah ini membahas tentang metode keamanan pada situs jejaring sosial dan menganalisa berbagai macam kemungkinan serangan terhadapnya. Metode keamanan pada web bermacam – macam dan dibagi menjadi tiga kriteria, yaitu autentikasi, otorisasi, dan akses kontrol. Autentikasi adalah proses untuk memverifikasi apakah orang yang masuk adalah orang yang benar. Otorisasi adalah proses untuk memverifikasi apakah orang yang bersangkutan memiliki izin untuk mengakses *resource* tertentu. Dan terakhir, Akses Kontrol adalah cara untuk mengontrol akses seseorang ke *web resource*. [2]

Setiap web memiliki metode autentikasi, otorisasi, dan akses kontrol yang berbeda – beda dan menentukan tingkat keamanan dari web tersebut. Di balik metode – metode keamanan yang dipakai oleh web tersebut, tentu memiliki kelemahan yang dapat menyebabkan orang lain dapat melakukan yang tidak semestinya dapat dilakukan. Makalah ini membahas metode – metode kripanalisis terhadap metode autentikasi, otorisasi, dan akses kontrol pada web. Dalam makalah ini akan diambil contoh studi kasus dari situs jejaring sosial, sehingga dengan mempelajari cara kerja *web* tersebut maka kita dapat membuat program yang berinteraksi dengan *web* tersebut dan seolah – olah kita memang terintegrasi dengan web tersebut dan hal ini memungkinkan kita untuk menggunakan fitur – fitur yang ada di situs jejaring sosial tersebut tanpa harus mengakses situs jejaring sosial tersebut.

Kata kunci : Kripanalisis, *web*, *jejaring sosial*.

1. Pendahuluan

Dewasa ini begitu maraknya situs jejaring sosial yang beredar di masyarakat. Hal ini dipicu oleh kemunculan web 2.0 yang memungkinkan penggunanya berinteraksi dan memberikan konten di web yang tersedia. Situs jejaring sosial yang ada sekarang biasanya memiliki multifungsi seperti chat, blog, game, dan lain – lain. [5]

Ada kalanya kita menginginkan salah satu fitur dari situs jejaring sosial itu tanpa harus mengakses web tersebut melalui *browser*. Contohnya, mungkin kita ingin menggunakan fitur chat agar bisa mengobrol dengan teman yang sudah ada jejaring sosial itu namun terlalu repot jika harus mengakses *web* itu melalui *browser*. Kebanyakan jejaring sosial memang menyediakan API (*Application Programming Interface*) untuk menghubungkan aplikasi yang ingin dibuat dengan situs jejaring sosial. API ini pun

memiliki kemampuan untuk memungkinkan kita mengakses fitur – fitur dari jejaring sosial tersebut namun terkadang API tersebut masih memiliki keterbatasan. [3]

Dengan kriptanalisis terhadap web maka kita dapat mempelajari cara kerja web tersebut dan membuat API sendiri yang sesuai dengan kebutuhan kita. Contohnya mungkin kita bisa membuat aplikasi *chatting* di *desktop application* yang merupakan fitur dari salah satu jejaring sosial atau mungkin saja bisa diimplementasi di perangkat *mobile* dan disesuaikan dengan kebutuhan kita.

2. Keamanan Web

Keamanan web dibagi menjadi tiga kriteria yaitu autentikasi, otorisasi, dan akses kontrol. Autentikasi adalah proses untuk memverifikasi apakah orang yang masuk adalah orang yang benar. Otorisasi adalah proses untuk memverifikasi apakah orang yang bersangkutan memiliki izin untuk mengakses *resource* tertentu. Dan terakhir, Akses Kontrol adalah cara untuk mengontrol akses seseorang ke *web resource*. Namun dalam kenyataannya autentikasi dan otorisasi tidak terpisahkan dan selalu menjadi kesatuan. [2]

Ketika ada *resource* yang diproteksi menggunakan autentikasi standar, Apache akan mengirimkan *header 401 Authentication Required*, yang menandakan bahwa pengguna yang ingin mengakses *resource* tersebut diharuskan memasukkan data yang dibutuhkan. Jika pengguna menggunakan browser yang mendukung GUI (Graphical User Interface) maka biasanya akan menampilkan tempat untuk memasukkan *username* dan *password*. Jika *username* dan *password* yang dimasukkan cocok maka *resource* yang diminta oleh pengguna dapat ditampilkan ke pengguna.

Karena HTTP bersifat *stateless*, setiap permintaan ke *resource* yang memiliki proteksi akan diperlakukan dengan cara yang sama yaitu meminta username dan password setiap kali akan mengakses *resource* tersebut. Namun, kebanyakan browser yang ada sekarang memiliki fungsi *caching* sehingga data tersebut dapat disimpan dan memungkinkan pengguna untuk tidak memasukkannya berulang kali.Server menyimpan data username dan passwordnya dengan berbagai macam cara. Dapat berupa file textual biasa, file textual dengan MD5 (*digest authentication*), atau disimpan ke dalam basis data (SQL, Oracle, dll).

Autentikasi dan otorisasi hanyalah bagian dari sesuatu yang besar. Terkadang ada *resource* – *resource* tertentu yang hanya bisa diaskses oleh sebagian pengguna saja tergantung dari hak yang diberikan kepada pengguna itu contohnya hak administrator tentu lebih besar daripada pengguna biasa. Selain itu juga ada kalanya hanya alamat IP (Internet Protocol) tertentu saja yang bisa mengakses *web resource* tertentu hal ini tentu dapat meningkatkan keamanan web dari orang – orang yang tidak memiliki hak untuk melakukannya.

Beberapa isu yang mengancam keamanan web diantaranya validasi data yang dimasukkan dan data yang dikeluarkan, akses data secara langsung (dan pencurian data), pengubahan data, eksekusi file yang berbahaya, manajemen otentikasi dan *session*, konfigurasi dan arsitektur sistem, *phishing*, *Denial of Service*, kelemahan informasi sistem, penanganan kesalahan (*error handling*), dan ancaman – ancaman lain yang dapat menggangu kinerja dari web tersebut.

3. Jejaring Sosial

Layanan jejaring sosial berfokus pada membangun dan merefleksikan jaringan sosial atau hubungan sosial antar manusia seperti mereka yang membagi minatnya dan/atau aktivitas mereka. Pada hakikatnya, layanan jejaring sosial merepresentasikan profil tiap penggunanya, kerabat penggunanya, dan berbagai macam layanan tambahan. Kebanyakan jejaring sosial berbasis web dan menyediakan berbagai cara untuk melakukan interaksi antar penggunanya seperti surat elektronik (e-mail) atau *instant messaging*. [7]

Jejaring sosial yang ada sekarang sudah banyak memiliki fitur – fitur yang memungkinkan kita untuk

berinteraksi dengan jaringan sosial kita seperti *publisher* yang memungkinkan penggunanya untuk memberitahu kerabatnya apa yang sedang mereka lakukan atau pikirkan, *News Feed* yang memungkinkan penggunanya untuk mengetahui aktivitas apa saja yang dilakukan oleh kerabatnya di situs jejaring sosial tersebut, *Wall* yang memungkinkan penggunanya untuk mengirim pesan kepada kerabatnya misalnya ucapan selamat ulang tahun, mengunggah foto yang memungkinkan kerabatnya untuk mengetahui aktivitas penggunanya dengan gambar sehingga dapat lebih tergambar apa yang dilakukannya, menggunggah video yang memungkinkan kerabatnya untuk melihat video dan mengetahui aktivitas penggunanya melalu video tersebut, *Notes* semacam blog yang memungkinkan penggunanya untuk menulis cerita atau tulisan yang dapat dilihat oleh kerabatnya sehingga kerabatnya tau apa yang pengguna lakukan atau pikirkan, *Gifts* adalah fitur yang memungkinkan penggunanya untuk memberi barang yang menunjukkan kepeduliannya kepada kerabatnya di situs jejaring sosial, Poke yang memungkinkan penggunanya untuk "menyapa" kerabatnya di situs jejaring sosial, Status Updates yang memungkinkan penggunanya untuk menuliskan status berupa apa yang sedang dia lakukan atau sedang dipikirkan sehingga kerabatnya dapat mengetahui apa yang sedang dilakukan atau dipikirkan kerabatnya yang lain. *Events* yang memungkinkan penggunanya untuk membagi acara atau kegiatan dan dapat mengundang kerabatnya untuk bersama – sama menghadiri acara atau kegiatan tersebut, dan *Chat* yang memungkinkan penggunanya dapat "mengobrol" teman – temannya yang kebetulan sedang mengakses situs jejaring sosial tersebut dalam waktu yang sama.

Beberapa situs jejaring sosial yang ada sekarang sebenarnya sudah memiliki API (*Application Programming Interface*) sendiri yang digunakan untuk mengakses fitur – fitur yang ada di situs jejaring sosial tersebut, namun API yang ada terkadang tidak semuanya mendukung kebutuhan penggunanya, seperti contohnya facebook tidak menyediakan API untuk facebook chatnya. Hal ini tentu mengurangi kebebasan penggunanya yang ingin menggunakan fitur chat yang ada di facebook tersebut. Beberapa API lainnya pun mengharuskan kita untuk mendaftarkan diri terlebih dahulu dan diharuskan memenuhi beberapa persyaratan tertentu yang tentu mengurangi kenyamanan pengguna dalam menggunakan API dan situs jejaring sosial tersebut. [3]

4. Metode Kripanalisis terhadap web

Dalam makalah ini diambil contoh kasus dari salah satu situs jejaring sosial yaitu facebook (http://www.facebook.com). Contoh kasus ini diambil karena facebook dianggap memiliki fitur yang cukup lengkap namun tidak memiliki API yang mendukung fitur – fitur yang disediakan dari situs jejaring sosial tersebut.

Langkah pertama yang dibutuhkan adalah mempelajari cara kerja web tersebut dimulai dari bagaimana dia bertransaksi data, memvalidasi data tersebut, dan menggunakan data tersebut. Hal ini dapat dilakukan dengan berbagai macam tool yang dapat mendeteksi koneksi yang keluar ataupun masuk dari komputer kita, contohnya adalah ekstensi *add-ons* Firefox yang bernama *Tamper Data*. [8]

Di dalam web dikenal dua metode untuk meminta halaman atau resource yang ada di web yaitu GET dan POST. Jika dengan metode GET kita hanya cukup mengirimkan URL (Uniform Resource Locator) saja, jika dengan metode POST selain mengirimkan URL-nya, kita juga harus mengirimkan data apa yang mau dikirimkan ke URL tersebut. Dengan Tamper Data, kita dapat mengetahui dalam mengakses halaman atau resource yang dibutuhkan menggunakan metode apa dan data apa saja yang dikirimkan sehingga cara kerja dari web tersebut dapat kita ketahui.

Ketika kita akan login ke facebook, URL yang ditangkap dari Tamper Data adalah "https://login.facebook.com/login.php?login_attempt=1" dan data yang dikirimkan ada 3 parameter yaitu email, pass, dan lsd. lsd adalah sebuah string yang dibangkitkan secara acak berukuran 5 karakter

misalnya “6Lzed”, hal ini dilakukan untuk memastikan apakah akses login facebook ini memang berasal dari situs jaringan sosial tersebut atau tidak dan lsd ini dapat kita peroleh ketika kita mengakses situs jejaring sosial tersebut. Nilai dari lsd tersebut disimpan dalam cookies dan hanya didapatkan ketika kita mengakses situs jejaring sosial tersebut.

Salah satu fitur yang mau dijadikan kasus uji coba dalam makalah ini adalah fitur chat yang memungkinkan penggunanya untuk “mengobrol” secara tekstual di situs jejaring sosial dengan kerabatnya di jejaring sosial tersebut yang sedang mengakses situs tersebut dalam waktu yang bersamaan. Dari hasil yang ditangkap oleh Data Tamper, URL yang dikirimkan untuk mendapatkan daftar kerabat kita yang sedang mengakses situs jejaring sosial tersebut dalam waktu yang bersamaan adalah "http://www.facebook.com/ajax/chat/buddy_list.php?__a=1" dengan parameter user, popped_out, force_render, buddy_list, fb_dtsg, post_form_id, dan post_form_id_source. post_form_id adalah id yang diberikan facebook ke penggunanya untuk menandakan seorang pengguna pada sesi itu dan berbeda – beda tiap pengguna. Ketika URL tersebut diakses dengan metode post dan data – data yang dimasukkan maka respon dari facebook akan seperti ini :


```
for
(;;);{"error":0,"errorSummary":"","erro
rDescription":"","errorIsWarning":false
,"silentError":0,"payload":{"time":1269
417831000,"buddy_list":{"listChanged":t
rue,"availableCount":60,"nowAvailableLi
st":{"591929033":{"i":false,"fl":["-
1"]}},"wasAvailableIDs":[],"userInfos":
{"591929033":{"name":"Lafrania
Taufik","firstName":"Lafrania","thumbSr
c":"http:\/\/profile.ak.fbcdn.net\/v224
\/29\/124\/q591929033_3642.jpg"}},"forc
edRender":true,"flMode":true,"flData":{
"1398800775094":{"n":"Business","o":0,"
c":1,"h":0},"1398799375059":{"n":"Dosen
","o":1,"c":3,"h":0},"1398799655066":{"
n":"IF","o":1,"c":33,"h":0},"1398798455
036":{"n":"ITB","o":1,"c":27,"h":0},"13
98800935098":{"n":"SD","o":1,"c":2,"h":
0},"1398798735043":{"n":"SMA","o":1,"c"
:16,"h":0},"-1":{"n":"Other
Friends","h":0,"o":1}},"userToFlMap":nu
ll}}}
```


Respon tersebut merupakan format JSON (JavaScript Object Notation), yaitu format yang digunakan untuk pertukaran data yang ringan. Didalamnya terdapat data – data yang dimampatkan jika sekilas saja kita lihat dari hasil respon yang didapat maka ada kata – kata userInfos, firstName, name, dll. [10]

Facebook memiliki format data sendiri dan memampatkannya dalam bentuk JSON dan ketika kita mau menggunakan data tersebut, maka kita harus mendekripsi data tersebut agar mendapatkan informasi yang dibutuhkan. Dengan mendekripsi respon berupa JSON tersebut kita dapat mendapatkan Nama dan id user kerabat kita yang sedang mengakses situs jejaring sosial tersebut secara bersamaan.

Sedangkan cara untuk melihat proses pengiriman pesan ke kerabat kita dapat dilakukan dengan cara melakukan pengiriman pesan ke kerabat dan dengan Tamper Data. Hasil yang diperoleh dari Tamper Data yang dilakukan tersebut adalah proses yang dilakukan menggunakan metode post dengan URL dari pengiriman pesan tersebut adalah “http://www.facebook.com/ajax/chat/send.php?__a=1” dan parameter yang diberikan adalah to, msg_text, msg_id, fb_dtsg, client_time, post_form_id, dan post_form_id_source. Beberapa parameter yang penting dari proses pengiriman pesan ini adalah to dan msg_text yaitu kepada siapa pesan ini dikirimkan dan isi dari pesan yang dikirimkan.

Proses terakhir dalam proses *Chat* adalah mendapatkan pesan yang dikirimkan kerabat kita kepada kita. Cara yang dilakukan agar mengetahui proses mendapatkan pesan ini sama dengan proses yang sudah dilakukan sebelumnya yaitu dengan melakukan aksi tersebut dan menjalankan proses Tamper Data. Hasil yang diperoleh dari Tamper Data yang dilakukan tersebut adalah facebook terus meminta halaman tertentu yaitu

"http://0.channel<nomor_channel>.facebook.com/x/0/false/p_<id_user>=-1" dan akan mendapatkan respon berupa :

```
for (;;);{"t":"refresh", "seq":2}
```

Dari respon tersebut kita mendapatkan nomor seq yang menandakan bahwa pesan chat yang aktif sekarang ada di seq nomor 2. Ketika ada pesan yang masuk maka nomor seq itu akan berubah dan mengacu ke nomor seq yang mengandung pesan tersebut. Nomor seq itu dimasukkan ke URL "http://0.channel<nomor_channel>.facebook.com/x/0/false/p_<id_user>=<no_seq>" dan respon yang didapat ketika mengakses URL tersebut dengan metode GET adalah :

```
for
(;;);{"t":"msg","c":"p_1384526172","ms"
:[{"type":"msg","msg":{"text":"bikin
program                              apa
lo?","time":1269453451371,"clientTime":
1269453451824,"msgID":"1810820627"},"fr
om":1302442707,"to":1384526172,"from_na
me":"Ade                           Putri
Marina","to_name":"Aqsath         Rasyid
Naradhipa","from_first_name":"Ade
Putri","to_first_name":"Aqsath"}]}
```

Hasil dekripsi dari respon yang didapat dapat menghasilkan id dan nama pengirimnya berikut isi dari pesan dan waktu ketika pesan itu dikirimkan dalam bentuk timestamp.

5. Kesimpulan

Kita dapat melakukan kripanalisis terhadap web dengan cara mempelajari proses kerja web tersebut, cara bertransaksi data, dan bagaimana data itu digunakan. Proses tersebut dapat dipelajari dengan cara menangkap data – data yang dikirimkan dalam setiap proses dijalankan.

Dengan metode kripanalisis terhadap web seperti ini maka kita dapat membuat API sendiri untuk situs jejaring sosial yang sesuai dengan kebutuhan sendiri dan kita dapat menggunakan fitur – fitur yang ada di jejaring sosial tersebut tanpa harus mengaksesnya melalu situs jejaring sosial tersebut sehingga lebih memudahkan penggunanya dalam menggunakan jejaring sosial tersebut.

Daftar Referensi

[1] Munir, Rinaldi. Kriptografi, Institut Teknologi Bandung, 2006.

[2] Authentication, Authorization, and Access Control
http://httpd.apache.org/docs/1.3/howto/auth.html
Tanggal Akses 22 Maret 2010 pukul 02.00

[3] Plurk API
http://www.plurk.com/API
Tanggal Akses 22 Maret 2010 pukul 11.00

[4] Facebook Chat: Now We're Talking
http://blog.facebook.com/blog.php?post=12811122130
Tanggal Akses 22 Maret 2010 pukul 11.00

[5] Facebook features – Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Facebook_features
Tanggal Akses 22 Maret 2010 pukul 11.00

[6] Top 10 website security issues
http://www.watsonhall.com/resources/downloads/top10-website-security-issues.pdf
Tanggal Akses 22 Maret 2010 pukul 12.00

[7] Social Network Service – Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Social_network_service
Tanggal Akses 23 Maret 2010 pukul 16.00

[8] Tamper Data :: Add-ons for Firefox
https://addons.mozilla.org/en-US/firefox/addon/966
Tanggal Akses 24 Maret 2010 pukul 12.00

[9] HTTP Dalam Java : Basic << Kode – kode yang terpecah
http://serpihankode.wordpress.com/2010/01/26/http-dalam-java-basic
Tanggal Akses 24 Maret 2010 pukul 13.00

[10] JSON
http://www.json.org
Tanggal Akses 24 Maret 2010 pukul 13.00