

HACKING MENGGUNAKAN TEHNIK SQL INJECTION

Author : Slamet Risnanto
Alumni STMIK-IM angkatan 1999 (Karyawan)
Email : it.dept@satriasejati.com

PENDAHULUAN

Kata hacker pada jaman sekarang ini sudah tidak asing lagi ditelinga kita khususnya dunia information technology (IT) dan hacker yang dulu dipandang sebagai penjahat, pencuri atau pembobol suatu system komputer sekarang sudah bergeser , keberadaan hacker yang identik dengan aktifitas underground kini sudah mulai menampakkan diri , sebagai contoh dinegara negara maju , perusahaan perusahaan besar yang mempunyai system komputer yang besar sudah mulai menyewa hacker hacker untuk mencari kelemahan kelemahan system mereka.

Penulis dalam menulis artikel ini bukan bermaksud untuk mengajari para pembaca untuk menjadi perusak, pencuri atau penjahat suatu system komputer akan tetapi bertujuan untuk adik adik mahasiswa yang akan turun di dunia IT khususnya calon system administrator atau web administrator untuk keamanan system yang dipegangnya sehingga selalu waspada terhadap aktifitas pancurian/penjarahan data dan lain lain , penulis berpendapat bahwa untuk mengamankan rumah kita dari penjarahan dan pencurian belajar dan mempelajari pola pikir pencuri dan penjahat adalah hal yang sangat tepat , begitupun dalam keamanan system komputer.

SQL INJECTION

Teknik hacking sql injection mulai mencuat kepermukaan semenjak dijebolnya situs KPU pada pemilu putaran pertama kemarin oleh Dani Firmansyah atau Xnuxer , dengan teknik ini beliau dapat masuk sebagai web administrator tanpa susah payah scan port port yang terbuka , tanpa terdeteksi oleh firewall dan tanpa tool .ke situs tersebut yang konon system yang seharga 152 milyar itu keamanannya berlapis lapis

Apa yang penulis bahas ini adalah basic atau dasar dasar dari teknik hacking yang dinamakan sql injection , teknik ini memungkinkan kita masuk ke suatu system yang terproteksi sebagai siapa saja dengan hanya mengetahui username tanpa harus mengetahui passwordnya bahkan kita juga bisa login **tanpa perlu mengetahui username dan password sama sekali**

Diilustrasikan STMIK-IM mempunyai situs dengan nama www.stmik-im.ac.id , untuk mengelola situs ini administrator membuat halaman web untuk aktifitas update semua halaman web sehingga bisa dikelola darimanapun dan kapanpun , halaman web tersebut tersimpan di www.stmik-im.ac.id/admin.asp , untuk mengamankan halaman2 yang dikhususkan untuk web administrator ini , web admin membuat halaman web yang terproteksi yang berfungsi sebagai pintu masuk ke halama2 berikutnya ,sehingga setiap

user yang akan masuk ke halaman halaman yang terproteksi harus memasukan username dan password mereka , daftar password dan user tersebut tersimpan dalam sql server dengan nama table admin dengan field field diantaranya username dan password.

Statement sql bukanlah bahasa pemrograman seperti pascal,Delphi atau visual basic , statemen sql biasanya digunakan bersama sama dengan bahasa pemrograman lain pada saat mengakses database , pada ilustrasi diatas , untuk mencocokkan user yang login , maka digunakan statemen sql yang kurang lebih sebagai berikut

```
Select * from admin where username = input_username  
And password = input_password
```

Sebagai contoh apabila penulis sebagai administrator dengan username = administrator dan password = admin bermaksud login maka sql statemennya sebagai berikut

```
Select * from admin where username = 'administrator' and  
Password = 'admin'
```

Dapat dipastikan bahwa apabila field username terdapat record administrator dengan filed password terdapat admin penulis dapat melewati proteksi dan masuk kehalaman berikutnya ,akan tetapi apabila sebaliknya ,maka akan keluar pesan kesalahan yang kurang lebih isinya kita tidak bisa masuk ke halaman berikutnya , lalu bagaimana kalau penulis memasukan input ' or '=' pada username dan password , perhatikan perubahan statemen sql berikut ini

```
Select * from admin where username = ' or '=' = ' and  
Password = ' or '='
```

Logika OR menyebabkan statement membalikan nilai false jadi true sehingga kita bisa masuk sebagai user yang terdapat pada record pertama dalam table admin (record pertama biasanya administrator) , dan bagaimana kalo kita hanya mengetahui username saja tapi passwordnya tidak , misalkan username = administrator , caranya cukup sederhana , pada text box tempat menginput username isi dengan "administrator"—“ sedangkan pada textbox password boleh diisi sembarang misalkan ' or '=' maka statement sql akan berubah menjadi

```
Select * from admin where username = ' administrator —“  
And password = ' or '='
```

Tanda “—“ (dua tanda minus) di sql server berarti akhir dari statement sql sehingga perintah dibelakangnya tidak dieksekusi lagi.

Untuk web admin , bagaimana cara mencegahnya , jangan izinkan user menginput selain karakter a - z atau A - Z atau 0 - 9 , selain dari pada itu ditolak pada saat pengecekan.

PENUTUP

Sebenarnya dari teknik dasar sql injection ini , pembaca bisa mengembangkan teknik ini sehingga akses yang ditimbulkan akan lebih dasyat dari cumin sekedar bisa masuk sebagai web administrator.

Penulis yakin bahwa sampai saat ini masih banyak situs situs yang bisa dieplor memakai teknik sql injection dikarenakan ketidak tahuan para adminnya , apabila para pembaca hendak mencobanya bisa mencari situs situs dengan menggunakan web searching misalkan yahoo atau google , masukan keynya login.asp/php atau admin.asp/php , tapi jangan merusaknya dan ingat aktifitas kita akan dicatat di log file yang akan mencatat IP kita dan aktifitas kita , penulis sarankan menggunakan anonymous proxy (akan dijelaskan pada artikel berikutnya).

Terakhir , penulis minta tanggapannya atas artikel ini melalui email it.dept@satriasejati.com , insya allah penulis akan melanjutkan artikel ini apabila para pembaca menghendakinya .dan penulis mohon maaf kepada para dosen dan para ahli keamana jaringan yang berada di sivitas akademika STMIK- , penulis tidak bermaksud menggurui akan tetapi untuk berbagi pengalaman dimana penulis sebagai web dan sytem admin disuatu perusahaan yang setiap hari berusaha mengamankan system jaringan dari aktifitas hacking dan lain lain.

Bandung , Agustus 2004

Slamet Risnanto