

# Menembus Password Login Menggunakan SQL Injection

**Happy Chandraleka**

*hchandrakeka@gmail.com*

*http://thecakraborawa.wordpress.com*

## **Lisensi Dokumen:**

*Copyright © 2003-2007 IlmuKomputer.Com*

*Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.*

## **Pengantar**

Pada tulisan ini saya akan jelaskan tentang cara menembus *password* login dengan SQL injection secara teoritis dengan melihat pada sisi kelemahan *query* bahasa SQL itu sendiri. SQL injection itu sendiri adalah suatu cara untuk mengeksploitasi kelemahan bahasa SQL dengan cara memasukkan (menginjeksikan) beberapa karakter tertentu. Deretan karakter tersebut biasa dikenal dengan nama *injection string*. Ada banyak hal yang dapat dilakukan dengan *injection string*. Diantaranya, mem-*bypass* password, mendapatkan nama tabel, menyisipkan anggota baru, dll, bahkan sampai menghapus tabel pada suatu database.

## **SQL Injection**

Bila seseorang ingin mengakses suatu sistem komputer, biasanya diperlukan login. Penerapannya pada website ditampilkan dengan dua kotak isian, yaitu kotak User Name, User Id, atau User Account dan kotak Password. Login ini berguna untuk memfilter dan mengetahui identitas seseorang yang ingin mengakses suatu sistem. Sistem login merupakan suatu cara dalam dunia sekuriti komputer untuk memfilter orang yang masuk ke sistem sehingga orang – orang yang tidak terdaftar tidak dapat masuk ke sistem tersebut.

Tetapi teknologi yang ada selalu saja tidak sempurna. Ada banyak cara untuk menembus filter pada sistem login tersebut. Sehingga seseorang yang tidak mengetahui password dapat juga ikut menikmati dan masuk ke sistem tersebut. Salah satunya adalah dengan SQL injection.

Pada tulisan ini saya akan jelaskan tentang cara menembus *password* login dengan SQL injection secara teoritis dengan melihat pada sisi kelemahan *query* bahasa SQL itu sendiri. SQL injection itu sendiri adalah suatu cara untuk mengeksploitasi kelemahan bahasa SQL dengan cara memasukkan (menginjeksikan) beberapa karakter tertentu. Deretan karakter tersebut biasa dikenal dengan nama *injection string*. Ada banyak hal yang dapat dilakukan dengan *injection string*. Diantaranya, mem-*bypass* password, mendapatkan nama tabel, menyisipkan anggota baru, dll, bahkan sampai menghapus tabel pada suatu database.

## Memahami Cara Kerja SQL Injection

Semisal ada seorang user yang bernama Joko yang ingin mengakses suatu sistem yang menggunakan sistem login. Maka Joko akan memasukkan isian pada kotak **User Id** dengan 'Joko' (tanpa kutip) dan pada kotak **Password** dengan 'rahasia' (tanpa kutip). Bila kemudian ditekan tombol **OK** atau tombol Login – nama tombolnya bisa berbeda – maka sistem tersebut akan menjalankan perintah *query* dalam bahasa SQL seperti berikut ini.



The image shows a simple login interface. It consists of two text input fields. The first field is labeled 'User Id:' and the second is labeled 'Password:'. Below these fields is a blue button with the text 'login' in white.

*Gambar Login dengan User Id dan Password*

```
Select * from TUser where UserId = 'joko' AND Password = 'rahasia'
```

Arti dari perintah tersebut adalah menampilkan data dari seluruh *record* (perhatikan tanda \* di perintah tersebut) di database sistem tersebut. Tetapi tidak semua record akan ditampilkan, karena pada perintah di atas ada filter atau pemilihan, yaitu hanya data yang *record* **UserId**-nya berisi 'joko' dan **Password**-nya berisi 'rahasia'. Perhatikan penggalan perintah setelah klausa **where**. Dan harus dipahami juga bahwa isian **UserId** dan **Password** yang diinputkan oleh *user*, **keduanya** harus bersesuaian dengan yang tersimpan di database sistem. Karena digunakan logika **AND** pada perintah tersebut.

Dengan demikian, bila isian **UserId** dan **Password** sesuai dengan yang tersimpan di database, barulah user tersebut dapat masuk ke sistem.

## Dua Cara Menembus Password

Untuk menembus – atau mem-*bypass* – password pada sistem login, bisa ditempuh dengan dua cara. Dari kedua cara tersebut seseorang bisa masuk ke suatu sistem tanpa perlu mengetahui password-nya.

**Cara pertama** adalah dengan menambahkan karakter '#' setelah **UserId**. Sehingga bila Anda menginputkan pada kotak **User Id** dengan 'Joko'#' (tanpa kutip) dan pada kotak **Password** Anda inputkan sembarang karakter, seperti pada gambar ini.

User Id:

Password:

Gambar Injection string dengan '#' pada kotak User Id

Maka ketika Anda menekan tombol Login, sistem website tersebut akan menjalankan perintah *query* sebagai berikut.

```
Select * from TUser where UserId = 'joko'#'  
AND Password = 'sembarang'
```

Tanda # merupakan cara untuk membuat komentar (*remark*) dalam bahasa SQL. Sebagaimana tanda // dalam bahasa Pascal. *Remark* atau komentar akan menyebabkan karakter sesudah tanda komentar akan diabaikan oleh program dan tidak akan dianggap sebagai kode program. Yang menariknya disini, dengan *injection string* '#' akan menyebabkan kode program setelah tanda # akan diabaikan. Perhatikan perintah di atas. Yang imbasnya adalah Anda bisa menginputkan sembarang karakter pada kotak **Password** dan Anda tetap bisa login dengan User Id 'joko'!!

**Cara kedua** adalah dengan menambahkan *injection string* **sembarang' OR 'x'='x** pada kotak Password.

User Id:

Password:

Gambar Injection string pada kotak Password

Sehingga bila Anda tekan tombol Login, maka sistem website akan menjalankan perintah sebagai berikut

```
Select * from TUser where UserId = 'joko'  
AND Password = 'sembarang' OR 'x'='x'
```

Akibatnya pada bagian **Password** akan terisi dengan nilai **'sembarang'**. Tentu saja inputan tersebut akan bernilai *false* dan akan menyebabkan Anda tidak bisa login ke sistem tersebut.

Sederhana saja alasannya, isian password tidak sama dengan yang tersimpan di sistem. Tetapi ada *query* lanjutannya, yaitu **OR 'x'='x'**. Yang artinya sistem diberikan pilihan. Bila sebelumnya, inputan password bernilai salah, maka dijalankan pilihan berikutnya yang sudah **pasti** benar, karena **'x'='x'**. Akibatnya Anda bisa masuk ke dalam sistem tanpa mengetahui password yang sesungguhnya dengan **User Id** 'joko'!!

## Bagaimana Penerapannya?

Demikian teori *SQL injection* untuk menembus password login. Saya katakan teori karena memang begitulah secara teoritis kelemahan bahasa SQL. Tentu saja dalam penerapannya pada keadaan sesungguhnya akan sedikit berbeda. Sehingga bila Anda mencoba bermain – main dengan kiat ini, Anda tidak bisa begitu saja masuk menembus password pada login website. Karena para web developer akan mengantisipasi adanya serangan *SQL injection* ini. Diantaranya dengan mendeteksi inputan karakter yang tergolong aneh. Kecuali pada beberapa website yang mereka belum memperbaiki diri.

## Biografi Penulis

**Happy Chandraleka**. Seorang penulis TI independen. Menyelesaikan S1 di Teknik Elektro Universitas Diponegoro. Saat ini mengelola Open Journal System Badan Penelitian dan Pengembangan Kesehatan, Kementerian Kesehatan Republik Indonesia. Informasi tentang penulis dapat dilihat di <http://thecakrabirawa.wordpress.com> dan dapat dihubungi via email [hchandraleka@gmail.com](mailto:hchandraleka@gmail.com).

(ditulis di Ruang 7 Depok, 5 November 2013, pukul 12.45 siang)