

Forum:[Hack Forums](#)

Thread: [SQL Tutorial](#)

MindOfLogic - April 29, 2013, 7:54 am

So a lot of people here often have trouble performing a blind SQL attack. I think most of the reason comes from people not really knowing the language in the first place. They just either follow the tutorial and if it works, they just keep trying that method. I'll explain some SQL basics here.

So suppose we have a table of Students:

Students(SID, fname, lname, password)

SID, fname, lname and password are column names.

So say we have some data in the database, just any data for this example.

We could do something like:

Code Select fname from students where fname = 'Joe';

This would return, yep you guessed it, anyone with the first name Joe. So you can imagine what other simple queries would be like.

We can throw something in there like this:

Code Select SID from students where fname = 'Joe' and lname = 'Davis'

Order By:

So on to check how many columns are in the table.

Order By - the order by clause tells the database to order columns by a number.

If no errors returned, then there is a column for that number. If no column is there, there will be an error on the page. So when you are doing your ORDER BY 1,2,3,4 you keep going until an error displays.

The reason you do this? Well when you start to union select, you put the numbers that were there in the select statement. There has to be as much selects there to match the number of columns or it will not work.

Union:

I'm not going to go through all of the basics, but you can use And and OR as well, just get your logic right.

I'm going to skip to the union statement as this is the most popular way to inject. So what exactly is a union? Ever remember when you were in math class and the teacher went over union and you weren't paying attention because you thought you'd never use it? Well should have paid attention.

Union of two sets:

Set 1 - {1,2,3}

Set 2 - {5,6}

Set 1 U Set 2 = {1,2,3,5,6}

See what I did there? You just take whats in every set. So how does this work to an inject? Well when you add a comment on to the end of the url, you are actually stopping SQL command there and you add your UNION SELECT statement.

What this does is this: it says, return everything that is usually queried in the url, and then whatever is union selected.

So UNION Select 1,2,3,4 or how ever many columns there are.

Using Metadata:

Metadata is data about data. An example of this is how you find out the table names or the column names with SQL commands. The two you have probably used is the table_name and information_schema.tab

You can use this like so:

Select table_name from information_schema.tab

There is also column_name from information_schema.columns

So next time you get the version by doing @@version, just look up metadata commands for that version and it will make your life a lot easier.

les