

Forum:[Hack Forums](#)

Thread: [?\[TUT\] Extracting information with SQLMAP \[/TUT\]?](#)

Dyme - April 5, 2012, 6:42 am

Hello members, I'm here today to present the website hacking section with my 2nd tutorial here on HF. If you have any questions feel free to post them below. Enjoy!

?NOTICE?: Before reading this tutorial, it's STRONGLY encouraged that you at LEAST know how to perform a Union & String based SQL Injection. Always remember that a tool should never replace your mind.

Link to a tutorial on Manual Union based Injection provided by -Downfall:

<https://hackforums.net/showthread.php?tid=1923250>

What is SQLMap?

In short, SQLMap is a Exploitation tool used for SQL Injections. It is coded in python and is in a command line UI. It comes with a variety of extremely useful features, such as tor integration. SQLMap is currently able to exploit the following SQL databases: MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird, Sybase and SAP MaxD. For more information on SQLMap, visit <http://sqlmap.sourceforge.net/>

Setting Up

Before you can start exploiting, there are a few things that you should configure. As mentioned before, SQLMap has tor integrated so you can stay anonymous. For a tutorial on setting up tor with SQLMap, Just visit <http://www.coresec.org/2011/04/24/sqlmap-with-tor/>

Because SQLMap is coded in python, it's also recommended that you have either a linux PC or virtual machine. You may be able to run it on windows, but I'm not sure of this as I've never tried myself. If you don't have a linux system I advise you to download BackTrack 5. BackTrack is Ubuntu 10.4 with many different pen-testing tools pre-installed, Including SQLMap. This can be found here: <http://www.backtrack-linux.org/downloads/>

The final and most obvious thing you'll need is a site Vulnerable to SQLi. To learn how to find a vulnerable site, check out the tutorial made by -Zer0freak-:

<https://hackforums.net/showthread.php?tid=2059771>

EXPLOITING!

To get SQLMap ready for use in BackTrack, simply click on Applications --> BackTrack --> Exploitation Tools --> Web Exploitation Tools --> sqlmap

If your using another distro/version of linux, I'm assuming you know how to cd into a directory.

Now your ready to start typing away. For this tutorial, I will just go through some of the basic commands that I use to Exploit databases.

Finding databases

Like if we were doing this manually, we first must find the databases of the website that we want to inject. In my case I will be injecting http://forzen-tech.com/product_list.php?fid=28

To find the databases of a site simply enter the following command:

Code `./sqlmap.py -u your_vulnerable_link_here --dbs`

If you set up tor, it would be the same exact thing except with `--tor` added. The same this will go for the rest of the commands that I will use later on during the tutorial.

Code `./sqlmap.py -u your_vulnerable_link_here --tor --dbs`Screen: Spoiler ([Click to View](#))

Once you enter the command, SQLMap will begin testing various possible methods of SQLi, and choose the appropriate one for the site you are injecting. When its done, you will be able to see your sites databases above the command line. In my case, I received one database (not counting `information_schema`).

Screen: Spoiler ([Click to View](#))

Finding Tables

Now that we know which database we want to inject, we can start searching for it's tables.

To find the Tables of a site simply enter the following command:

Code `./sqlmap.py -u your_vulnerable_link_here -D your_database_here --tables`Screen: Spoiler ([Click to View](#))

When this command is executed, SQLMap will find the tables and print them in the log above the command line.

Screen: Spoiler ([Click to View](#))

Finding Columns

First choose the table that you want to inject. In my case, I'll be injecting `forzen_ysmember`, as this is most likely the table which contains the admin login credentials.

To find the Columns of a site simply enter the following command:

Code `./sqlmap.py -u your_vulnerable_site_here -D your_database_here -T your_table_here --columns`Screen: Spoiler ([Click to View](#))

This command will find the columns of your desired table and then once again print them above the command line.

Screen:

Spoiler ([Click to View](#))

Final Step: Finding Data

As this is the final step, we must incorporate all the information we have gathered before into our command. This includes a database, table, and column.

To exploit Data from a site simply enter the following command:

Code `./sqlmap.py -u your_vulnerable_site_here -D your_database_here -T your_table_here -C your_column_here --dump`Screen: Spoiler ([Click to View](#))

When SQLMap is done, you will be able to see the Data from your column above the command line.

Screen:

Spoiler ([Click to View](#))

If your looking for the admin login, you'll have to do this with both the password column and the username column.

Done

Optional: Cracking hashes with SQLMap

SQLMap also has the ability to crack hashes when it finds one. To do this simply enter a command like you would normally, and if SQLMap finds a hash, it will ask you if you would like to crack it.

Screen:

Spoiler ([Click to View](#))

Thanks for reading, I hope this helps some people here!

Did this really get ed to the 5th page without a single comment? Can't have my tutorial get beat out by a bunch of "Ratez my deface pl0x"

IAmTheAg - April 6, 2012, 6:16 pm

Thanks for the tutorial, Bookmarked!

-Ag

Best Teemo NA - April 6, 2012, 6:31 pm

Im not on nix atm but some thing you should def use are,

Code proxychains

--threads=10

--useragent-random

--batch

Thats all I can think of the top of my head atm.

zer0pwn - April 6, 2012, 7:16 pm

Nice tutorial, but you should add how to dump it into a file, and then read the file. That's where I'm stuck, xD.

Dyme - April 6, 2012, 7:32 pm

(Apr 6, 2012 07:16 PM)Zer0Pwn Wrote: [\[CITE\]](#) Nice tutorial, but you should add how to dump it into a file, and then read the file. That's where I'm stuck, xD.

Im not sure about this, but I think sqlmap automatically saves dumps an logs. From what I remember, they should be somewhere in your sqlmap directory. Sqlmap will also make folders for every site you start to exploit. I'll check later for sure.

zer0pwn - April 6, 2012, 7:34 pm

(Apr 6, 2012 07:32 PM)Dyme Wrote: [\[CITE\]](#) Im not sure about this, but I think sqlmap automatically saves dumps an logs. From what I remember, they should be somewhere in your sqlmap directory. Sqlmap will also make folders for every site you start to exploit. I'll check later for sure.

Yeah, I did all this on BackBox.

It saved as like... .sqlite or something. Not sure how I'm supposed to open it, can't open it with Gedit or Genie. x.x

Best Teemo NA - April 6, 2012, 7:45 pm

(Apr 6, 2012 07:32 PM)Dyme Wrote: [\[CITE\]](#) Im not sure about this, but I think sqlmap automatically saves dumps an logs. From what I remember, they should be somewhere in your sqlmap directory. Sqlmap will also make folders for every site you start to exploit. I'll check later for sure.

Yeah it saves in the hidden folder sqlmap in your home dir.

zer0pwn - April 6, 2012, 7:46 pm

(Apr 6, 2012 07:45 PM)KYR SP33DY Wrote: [\[CITE\]](#) Yeah it saves in the hidden folder sqlmap in your home dir.

Yeah, you pretty much have to use the "Go To Directory" to get to there, lol.

Best Teemo NA - April 6, 2012, 7:48 pm

(Apr 6, 2012 07:46 PM)Zer0Pwn Wrote: [\[CITE\]](#) Yeah, you pretty much have to use the "Go To Directory" to get to there, lol.

ctrl+h to show your hidden folders... lmao its that easy.

mirkops - April 7, 2012, 7:52 am

Excellent just i needed this....thansk a lot..bookamrking..!!!

Cometfire - April 7, 2012, 9:19 am

Thanks for this tut, it really helped me with some problems I was having with sqlmap.

Z e r o - April 7, 2012, 9:22 am

Thanks for this tutorial, I found it very interesting.

Th3PonyWizard - April 22, 2012, 12:31 pm

Bump for this awesome tutorial, exactly what I was needed.

Dyme - April 22, 2012, 6:18 pm

Glad that everyone has been enjoying the tutorial. If anyone has questions or wants to learn how to use SQLMap further, either ask me or even just use the --help command!

Phizo - April 22, 2012, 6:26 pm

Nice tutorial, pretty HQ.

The only time I'll ever resort to SQLMap is when I need to dump the database though.