

Forum:[Hack Forums](#)

Thread: [\[tutorial\] Basic SQL Injection, automated with SQLmap](#)

compalabee - October 13, 2019, 11:15 pm

This post is for educational purposes only, and should not be used for illegal means. Misuse of information in this thread can get you to jail, and no one's responsible for that except you. Use this information wisely.

Hi guys! Compie here, posting a tutorial thread in the Hacking Tutorials section. This is only a basic tutorial, made for hackers who are still getting their feet wet. Feel free to add more in the comments section!

What is SQL Injection?

SQL Injection (or SQLi for short), is a cyberattack that targets machines that run Service Query Language (SQL). According to the OWASP Foundation, a "huge percentage" of all cyberattacks are injections, and SQLi is no exception in this. Placed at #1 in the OWASP Top 10, this is by far, the most dangerous hack you can ever accomplish.

There are many versions of SQL, such as PostgreSQL, MySQL, MSSQL, Oracle, and others. Each version of SQL uses a different version of some commands. For example, SQL Server comments like this:

Code DROP exampletable;#

Whereas MySQL comments like this:

Code DROP exampletable; --

There are other examples, but since this is a tut on automation, that won't be our focus.

What is SQLmap?

SQLmap ([link to GitHub page](#)) is an automated SQL Injection tool. It was made to be able to attack most (if not all) versions of SQL. It uses a dictionary system, and, while sometimes unreliable, it can even plant Metasploit backdoors.

It uses a dictionary of attacks to apply on a target endpoint. From there, it would be able to dump all database information, whether manually, or automatically.

How do I find a target for SQLmap?

Although there are exceptions, in the past years, the most probable vulnerabilities in SQL are those in .php endpoints. Examples are index.php, category.php, and the like. The requirement is that it needs to run with a variable, for example:

```
Code index.php?id=4  
category.php?page=1325  
showentry.php?list=29
```

Finding these endpoints can be accomplished in many ways, such as via spidering, directory bruteforcing, or Google dorks.

There are other ways to commit SQLi, but since this is only a basic tutorial, we'll get to those later.

Get to the point!

The plainest way to make an SQLmap query is like this:

```
Code sqlmap --url https://www.example.com /index.php? id =1
```

As you can see, I simply posted the URL of the target, including the endpoint. But wait, is it really that simple?

Not exactly. You see, you would simply get a SQLi check (this is a matter that is used by white hat hackers), but if you're trying to do a database dump, you're going to have to dig in deeper.

The fastest way?

PHP Code

```
<?php  
sqlmap --url https://www.example.com/index.php? id =1 --dump-all
```

Adding the --dump-all parameter makes sqlmap print all the database tables on the screen. Although it might take time because the program will have to dig into each column, row, and entry, it's easy, quick, and simple.

I did that, but it didn't work!

Patched vulnerabilities are a fact of life in the hacker world. Still, if you're pretty sure that the endpoint is vulnerable somehow, there are other options.

SQLmap can run with different attack levels, and attack risks too.

```
Code --level <1-5>  
--risk <1-3>
```

Increasing the level makes SQLmap use bigger dictionaries (and therefore a bigger chance of hacking the database), and increasing the risk means using "riskier" values, things that could get your IP blacklisted.

There are also ways to obfuscate (stealth) your attacks by using "tamper scripts", usable using

```
Code --tamper
```

You can list down all tamper scripts using

Code sqlmap --list-tampers

Well then, I hope you got some idea of how automating SQL injection works with SQLmap. This is merely a basic tutorial, and I'm sure that as you use the program more often, you'll get to experiment on the different options. Again, if you would like to add more, just comment below.

ArviX - *October 14, 2019, 2:32 pm*

Can sql injection be done without id?

compalabee - *October 14, 2019, 7:15 pm*

(Oct 14, 2019 02:32 PM)ArviX Wrote: [\[CITE\]](#) Can sql injection be done without id?

SQL injection requires variable input. It is an injection hack, therefore, you need something that sends data into the server. Whether it is id, username, page, whatever it may be -- so long as the target communicates via SQL through that variable, there is a chance it can be attacked.

Last_viking - *October 17, 2019, 1:28 am*

Thread is well written. He has explained each aspects of SQLi well thread bookmarked