Chapter 7

A Practical Guide to Database Hacking with SQL Map: Part-2

Welcome back to the exciting world of database hacking. In the last chapter, we successfully hacked and dumped the database of a website. Today, we'll take it further by targeting a new website and diving into table dumping and understanding URL parameters for SQL injection.

WHAT ARE URL PARAMETERS

URL parameters are like hidden secret codes in a website's URL. They help pass information from one webpage to another. You often see them after a question mark at the end of a URL. For example, in an online store's URL, you might find something like this:

`https://www.example.com/search?query=hacking+books`

Here, `search` is the parameter, and `hacking+books` is the value. This allows the website to display results relevant to the search query.

In simple terms, URL parameters are how websites keep track of dynamic content like search terms, user IDs, and more. These parameters are often vulnerable to SQL injection, which is what we'll focus on today.

STEP 1: FINDING THE WEAK URL PARAMETER

To perform an SQL injection, we first need to find the weak URL, i.e., the URL parameter that can be exploited. Steps:

Copy the Target Website URL

Find the URL of the website you wish to hack.

Write the Command to Find Weak URLs

Use SQL Map to scan for weak links. You can copy this command:

```
sqlmap -u "target_website_url" --crawl 2 --random-agent
--threads 6
```

Replace "*target_website_url*" with the website's URL.

Run the Command in Kali Linux Terminal

After you paste the command into the terminal, SQL Map will start scanning the website for weak URL parameters. It will prompt you for some questions. Answer them as we did in the previous chapter. SQL Map will find vulnerable parameters that are susceptible to SQL injection.

Identify the Weak URL Parameter

After scanning, SQL Map will list the vulnerable URLs with parameters. Choose one of the links.

STEP 2: FINDING THE DATABASE NAME

Now that we have a weak parameter, our next goal is to find the name of the database we want to hack. Steps:

Write the Command to Find the Database

Copy and paste the following command:

```
sqlmap -u "vulnerable_url" --dbs
```

Replace "vulnerable_url" with the URL parameter you copied in Step 1.

Run the Command

After pasting the command into Kali Linux, SQL Map will scan the website and detect the names of all available databases.

Select the Relevant Database

After the scan is complete, SQL Map will list the available databases. Often, the first database will be empty or system-related. Select one of the other databases that contains useful data.

STEP 3: FINDING THE TABLES INSIDE THE DATABASE

Once we know the database name, the next task is to find the tables within that database. Steps:

Write the Command to Find the Tables

Now, we will use SQL Map to find the tables inside the selected database. Use the following command:

```
sqlmap -u "vulnerable_url" -D "database_name" --tables
```

Replace "*vulnerable_url*" with the URL and "*database_name*" with the database you found in Step 2.

Run the Command

After pasting the command, SQL Map will scan the database and detect all the tables within it. Once the scan is complete, it will display the table names.

Choose a Table

From the list of tables, select one that you want to dump.

STEP 4: DUMPING THE TABLE

Now that we have identified a table, the final step is to dump the data from that table. Steps:

Write the Command to Dump the Table

Use the following command to dump the selected table:
sqlmap -u "vulnerable_url" -D "database_name" -T "table_name" --dump

Replace "*vulnerable_url*" with the parameter URL, "*database_name*" with the database name, and "*table_name*" with the table name you selected in Step 3.

Run the Command

After running the command, SQL Map will start dumping the table's data. This process may take some time, depending on the size of the table.

Access the Dumped Data

Once the dump is complete, SQL Map will save the data in a folder on your desktop. You can open this folder to find the dumped data, which may include sensitive information like usernames, passwords, emails, etc.

WRAPPING UP

In this chapter, we covered how to find weak URL parameters, identify the target database, locate the tables, and dump the data. All the commands needed were provided, making it easy for you to follow along and practice.

Remember, hacking without permission is illegal and unethical. Always practice these techniques responsibly in controlled environments or with explicit permission.

By ScripterJee