**Demo Write-Up**

**(1)(learning and observing website)**

**\* Try using the search bar**

1)It is an HTTP GET request, the user can directly see information about the database, knowing how this works:

* The request is cached and in the user history.
* The request is visible in the URL.
* Should not be used for more confidential information.

2)There is a table already given, mostly like the table column names are directly what's listed on the website, so there should be columns for:

**\* Title release character genre IMDd(link)**

3)Using the inspect tool(ctrl f), we learn that the name of the user input is title, which most likely aligns with its column name in the table.

**(2)(beginning to send db queries)**

1)let's try searching for something simple *(what is the syntax)*

* the (looking at the link, you can see the title value for the table input is(the + anything concated after)

2)Let's also try creating an SQL error message, it might say what type and version this database is:

**\* (MySQL, SQLite, PostgreSQL)**

It's MySQL, which will be very helpful in utilizing the correct syntax to type in the SQL query.

Now let’s try figuring out the number of columns this query is supposed to return now

**(3)(column hunting)**

1)I see five columns for this table, so I am going to try to return 5, it hopefully will work.

2)how to use a union and select commands:

* **select** -> retrieve a column from a table
* **union** -> concates the results of two or more select statements, this can be anything from db\_table calls to just integers, strings, functions…
* **#** --> *mySql comment,* this will comment out the rest of the old SQL query

3)let's try some commands

title='user input' (rest of SQL query)

(user input)'UNION SELECT 1,2,3,4,5 #

* what is each part of the query?
* **union select** (append multiple select statements into one query)
* 1,2,3,4,5 (just numbers, which SQL understands as integers)

**It doesn't work, error says**

***Error:*** *The used* ***SELECT*** *statements have a different number of columns*

What does this error information tell us? It states that the query used an incorrect amount of columns, and somewhere on the backend of the website, our query can't be outputted. Let’s keep trying different # numbers of columns until we do not get an error.

**the'UNION SELECT 1,2,3,4,5,6,7 #**

No error, time to start the fun

**(3)(the fun begins)**

From that last query, this statement is supposed to give out 7 outputs, so knowing that, we can now start querying the table using database functions

**information\_schema (fun!)**

1)definition: ***information\_schema*** (this is in all SQL databases, and contains the metadata of your database tree structure. This can be queried to learn about any tables in a db if not protected)

2)Let's now curate a more aggressive query using the same template as before, but now using information\_schema.columns and information\_schema.tables to find out the structure of this db hopefully.

we want to SELECT \* FROM statement *from* the information schema

**the'union select 1,2,3,4,5,6,7 from information\_schema.tables #**

We can use some SQL functions utilizing this table, however it is important that we use the function in columns we see on the page, so that would be 2,3,4, and 5.

**the'union select 1,database(),current\_user(),table\_name,5,6,7 from information\_schema.tables #**

* database() returns the DB name
* current\_user() returns db\_user name
* table\_name is the var of info\_schema.table will give the names of all tables in the database structure of this user

#all of this can be found on MySQL documentation, if anything seems a little confusing, you can look there, the link should be referred to at the bottom of the write-up.

*Now we have all tables in the database tree*

#note that a lot of the tables exist in all SQL table trees, so like for more unique names to see what is created by the database administration.

3)From here, there are a lot of potential places to go, but note that a lot of these tables are in most database structures, so sifting through them for a while to find what you may be interested

potential interesting tables: user... (movies is the one used for this page)

**(4)(target acquired => user)**

1)Now we still need more information about this table to query it, that is the column names of the table. However, by doing a similar process with information\_schema.columns, we can find out all the columns where the table is used.

**the'union select 1,column\_name,current\_user(),4,5,6,7 from information\_schema.columns where table\_name = 'users'#**

2)This will return all column names in the info\_schema.columns

Column\_names: id, password, email, login, secret, admin… a few others

**the'union select 1,id,secret,password,email,6,7 from users #**

Now that’s not what you should be allowed to see! That covers the extent of what this demo will do, but there is a LOT you can do from here like…

- Find out what the hashes are, maybe they use an old encrypt type like md5 (what the last workshop was about)

- If you can decrypt the password, you can then see if the email has credentials elsewhere, go from there

- There are other tables in the database, check them out!

- I challenge you to find out what columns of the movie table weren’t displayed on the website, and how many tickets are left in stock for the Dark Knight Rises movie! :)

Resources Used:

*Forever CTF (they have basic challenges on SQL injection)(last forever)*

*bWAPP and Docker*

**Videos about how to set Docker and bWAPP GitHub:**

[Docker Tutorial for Beginners (youtube.com)](https://www.youtube.com/watch?v=pTFZFxd4hOI&t=1090s)

[(577) Setting up an Extremely Buggy Web Application bWAPP with Docker in 5 mins Web Pen Testing Lab - YouTube](https://www.youtube.com/watch?v=MQy7JkWcQHE)

[bWAPP/README.md at master · raesene/bWAPP (github.com)](https://github.com/raesene/bWAPP/blob/master/README.md)

[bWAPP, a buggy web application! (itsecgames.com)](http://itsecgames.com/) *(don't download from here, get it from the GitHub repository)*

[12 - bWAPP Tutorials - SQL Injection(GET/Search) (youtube.com)](https://www.youtube.com/watch?v=jbZ3XbfvZJY&t=281s)

[13 - bWAPP Tutorials - SQL Injection(GET/Select) (youtube.com)](https://www.youtube.com/watch?v=1XdJtXSwKPE)

**Links about MySQL documentation:**

[MySQL :: MySQL 8.0 Reference Manual :: 28.3.38 The INFORMATION\_SCHEMA TABLES Table](https://dev.mysql.com/doc/refman/8.0/en/information-schema-tables-table.html)

[MySQL :: MySQL 8.3 Reference Manual :: 14 Functions and Operators](https://dev.mysql.com/doc/refman/8.3/en/functions.html)