waph-kanamala

WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student Name: Lakshmi Narayana Kanamarlapudi

Email: kanamala@mail.uc.edu

Short-bio: I am having interest towards data science and web development.

Repository Information

Respository's URL: https://github.com/LakshmiNarayanaKanamarlapudi/kanamala-uc.github.io

This is a public repository for Kanamarlapudi Lakshmi Narayana to store all code from the course. The organization of this repository is as follows.

Individual Projects

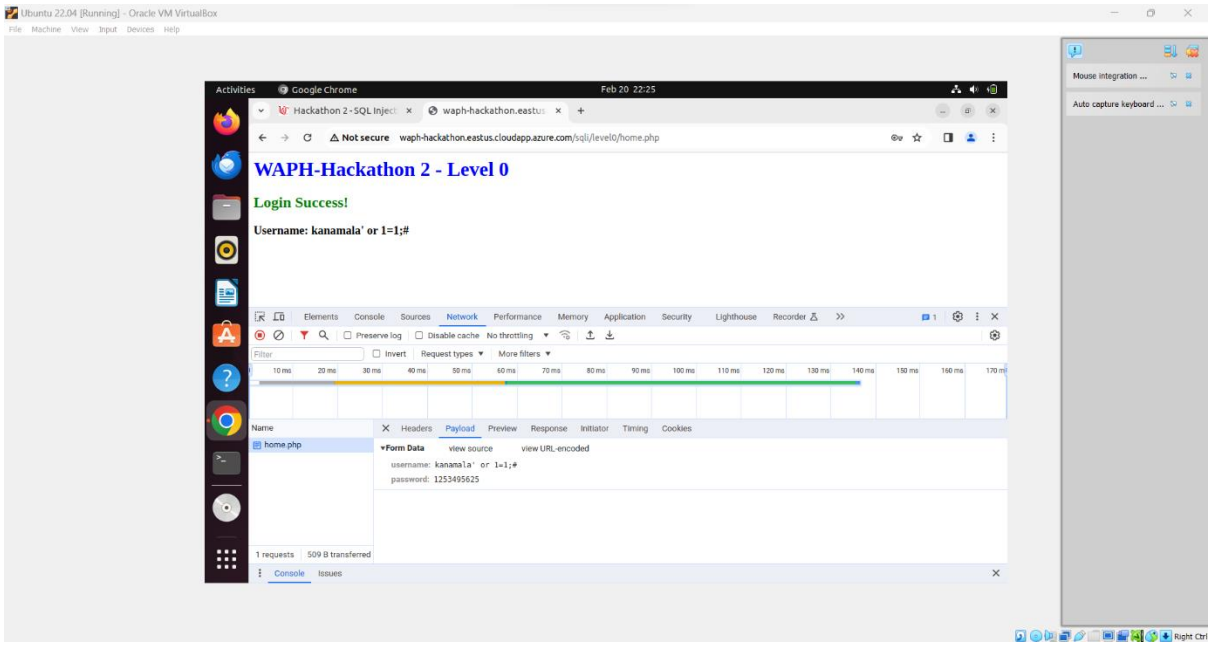
Hackathon2 URL : https://github.com/LakshmiNarayanaKanamarlapudi/waph-kanamala/tree/main/hackathons/hackathon2

Project Overview:

- In this hackathon we will be covering the sql injection techniques to by pass the security.
- We will be bypassing different levels of security where every level has different vulnerabilities.
- And checks the database schemas and the tables in the database.
- We need login the database using the original username and password.

Level0:

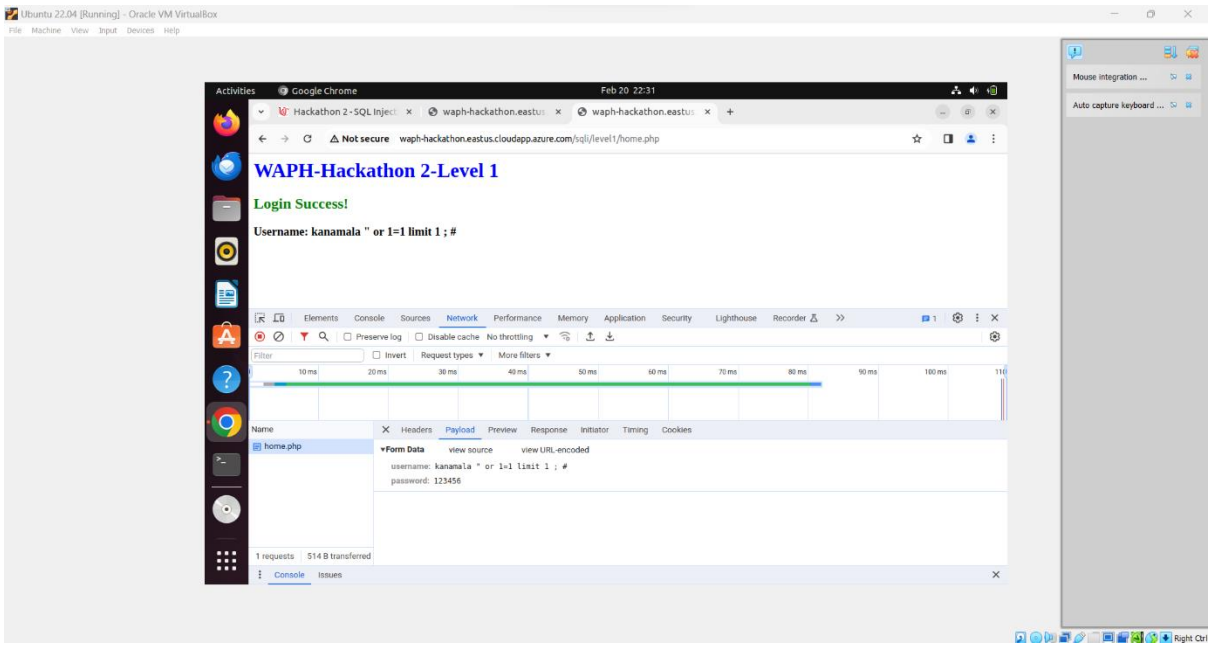
- The main aim of the level 0 task is to login to the system by using the SQL injection.
- So, I have used the following string to perform SQL injection and by pass system "kanamala' or 1=1 ;#".
- Where firstly I have used university username as per the rubric and the used "or" to see that "1=1" always become true and end the SQL.
- In the above I have done the SQL injection in the level 0. And out put was mention below.



Level 1:

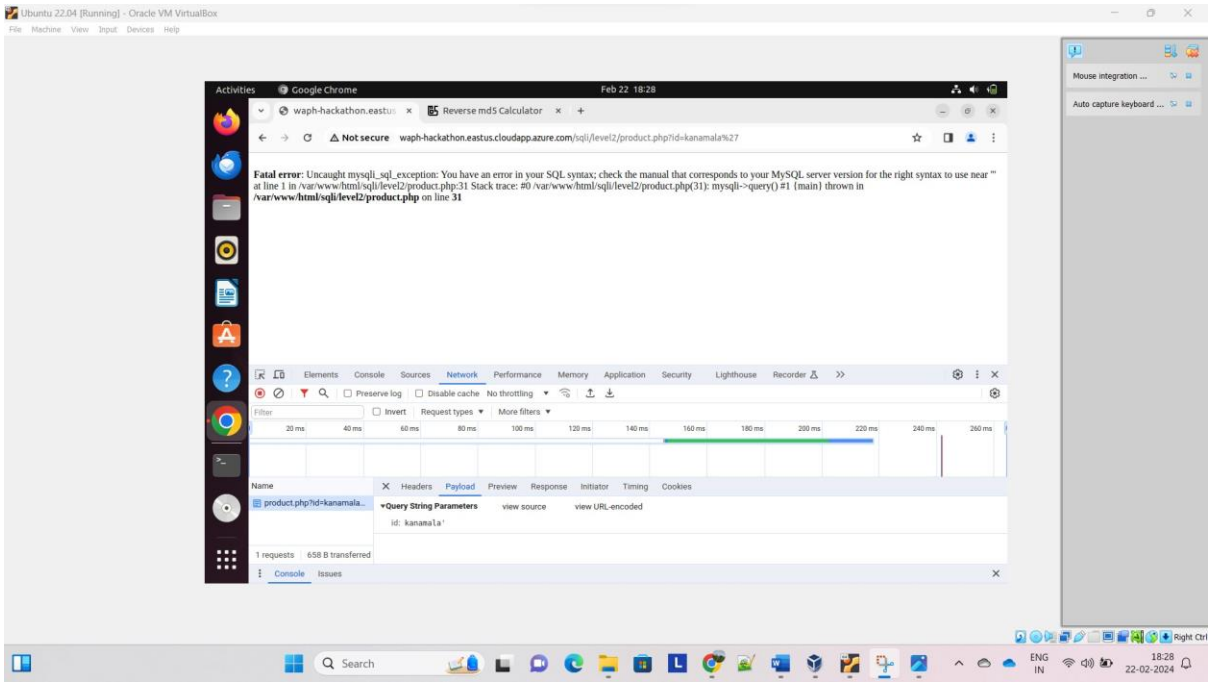
- As per the understanding from the lecture level 1 is bit difficult.
- The aim is same that we need to do the SQL injection but in the different level of security.
- So, to bypass the security and to login successfully I have used the “kanamala “ or 1=1 limit 1 ; #”.
- The 1=1 will always makes the condition true and “limit 1” to make the number of rows to 1 and rest same as level 0.

Back end SQL string guess: "SELECT * FROM users WHERE username=? AND password = md5("whatever")";



Level 2a: Detecting SQLi Vulnerabilities

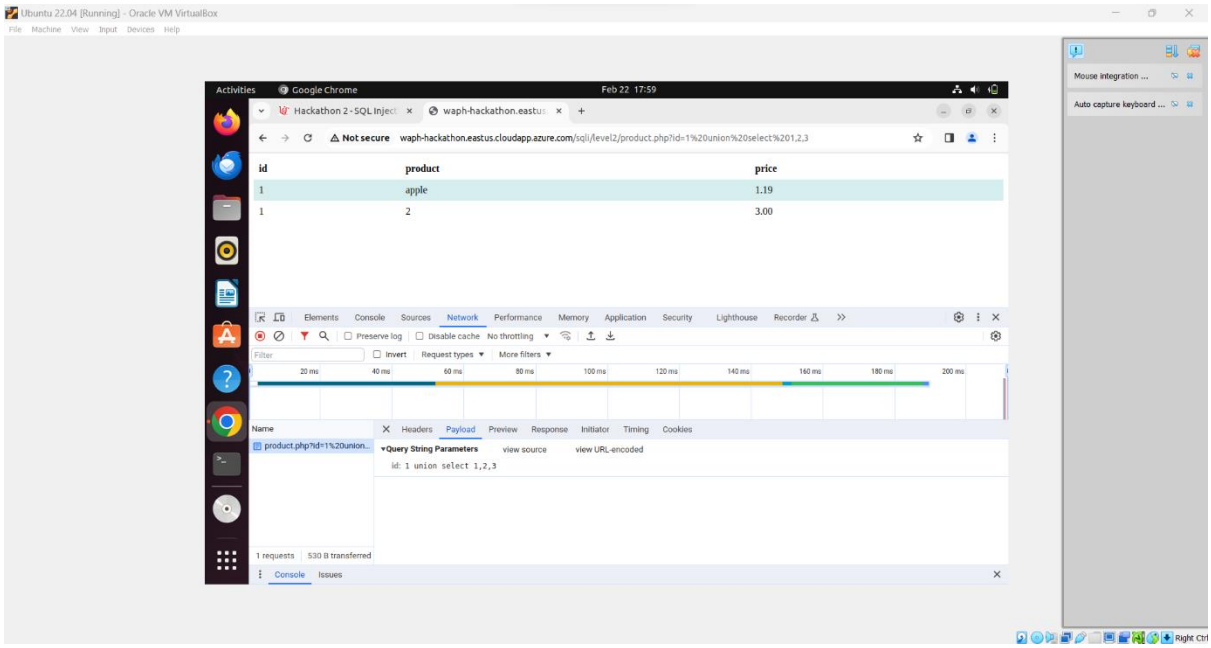
- In this level 2 section a we need to find the possibility of vulnerability.
- To achieve this I have followed the trail and error method where I have gave the multiple inputs and checked for vulnerability.
- Then I have found a vulnerability at line 31 of the code. Only vulnerability found for the multiple inputs.
- Finally the vulnerability along the SQL injection was placed below.



Level 2b: Exploiting SQLi to Access Data

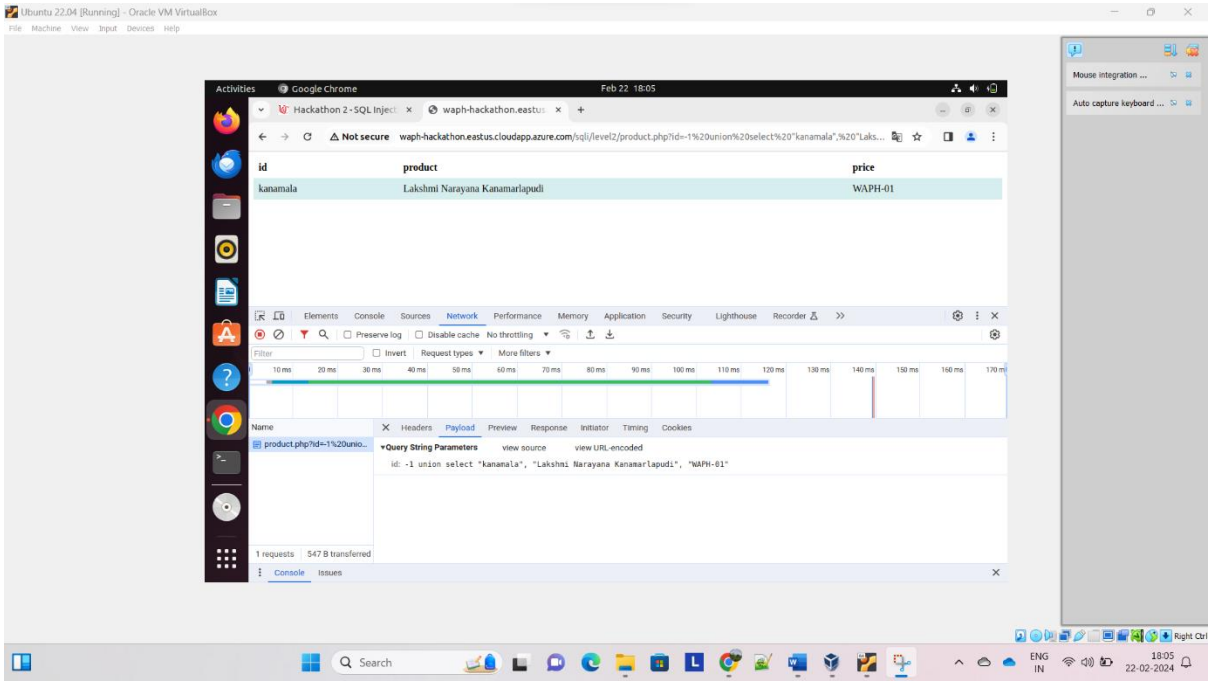
Level 2b-i: Identify the Number of Columns

- The main aim of the task is to find the number of columns in the database table.
- To find this I have tried to many possibilities but I have found only one successful attempt.
- Where to exploit the table for finding the columns I have tried to combine my input with the original output.
- So, I have used the following SQL string “union select 1,2,3. And the screenshot was attached below.



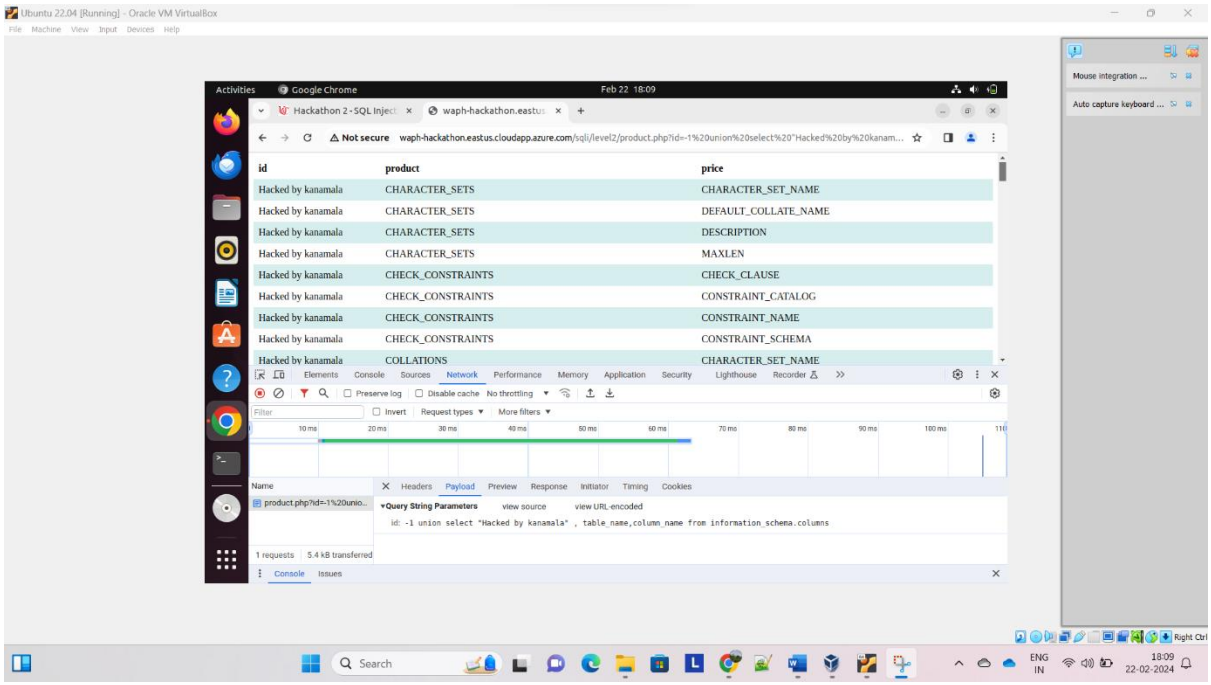
Level 2b-ii: Display Your Information

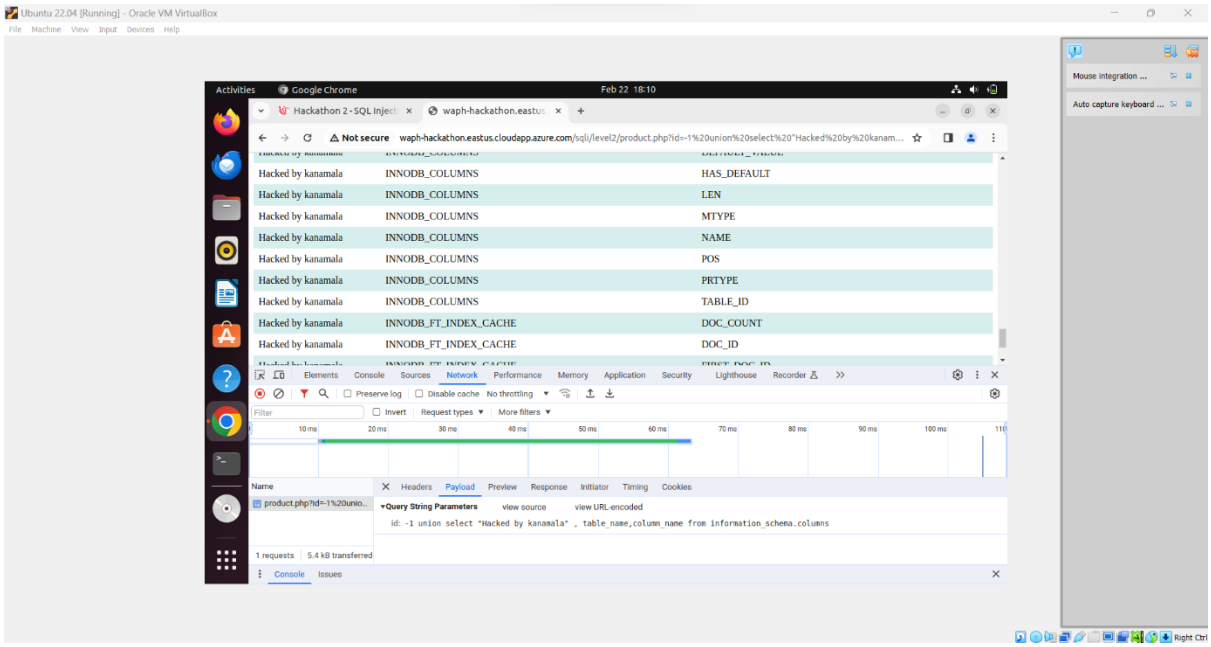
- This task is a subtask of level 2 where we need to print the information like university username , name and section of the course.
- To perform this type of SQL injection I have used the same union and select as in the “level-2b-I”.
- I have used following SQL string “-1 union select “kanamala”, “Lakshmi Narayana Kanamarlapudi”, “WAPH-01”” to exploit and print the desired output.
- The output was mentioned below.

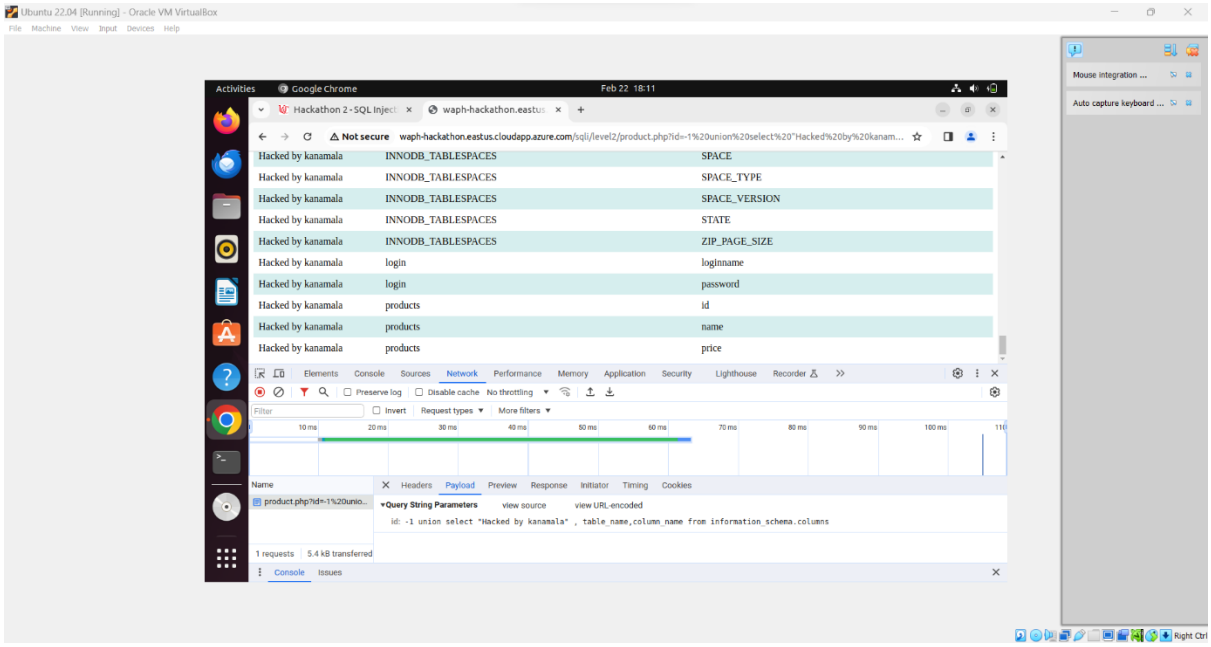


Level 2b-iii: Display the Database Schema

- The aim of the task is to display the database scheme which is nothing but displaying the table names along with the columns names.
- To achieve this I have used a SQL string which is liked printes a message first then it will retrieved information related to the table names and column names from the Database schema.
- The SQL string “-1 union select “Hacked by kanamala”, table_name,column_name from information_schema.columns” along with the output has been placed below.



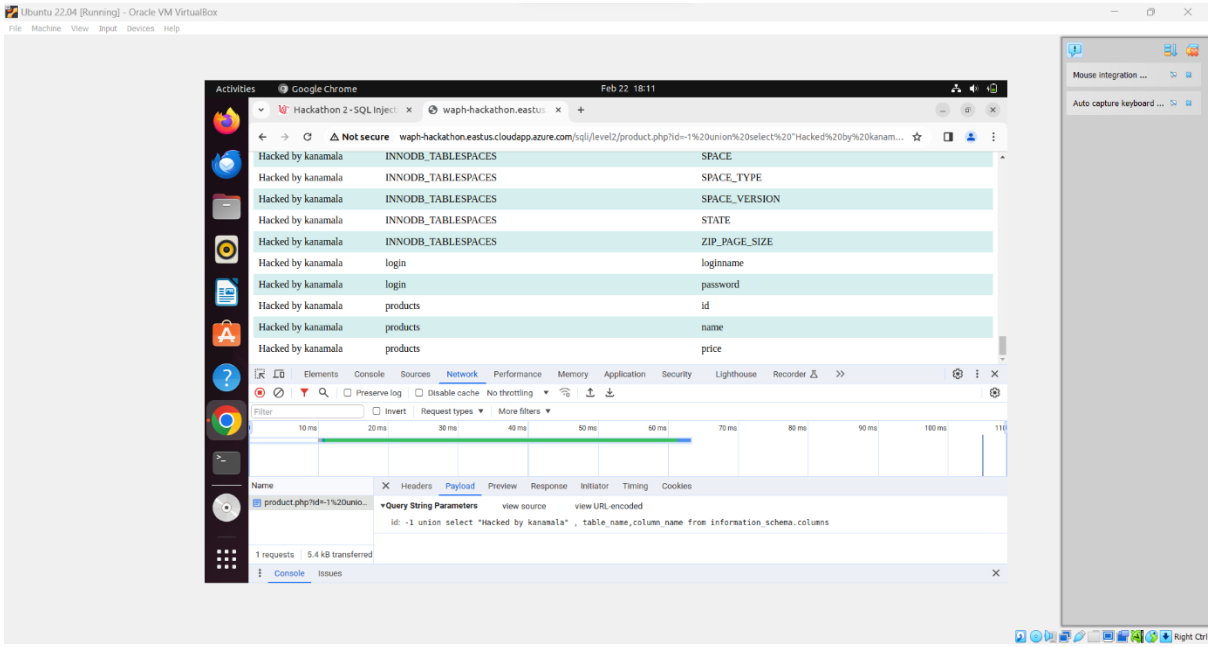




Level 2b-iv: Display Login Credentials

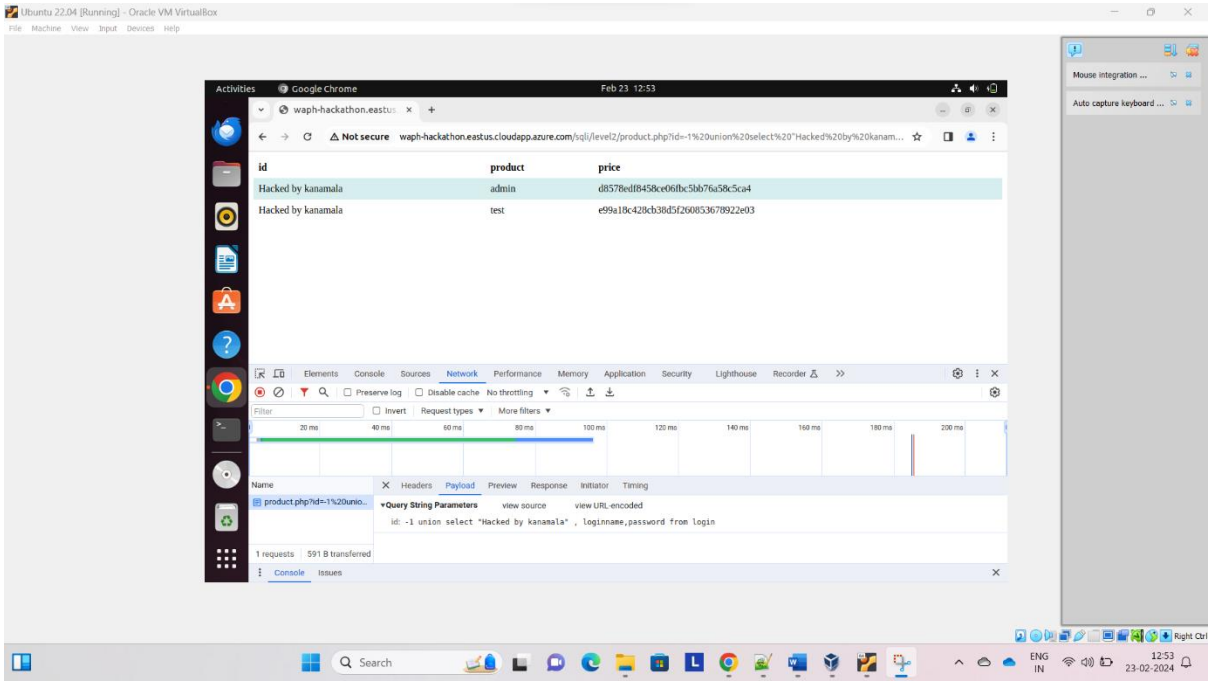
Table and columns that store usernames and passwords:

- Here we have revealed the table name and column name which stores the loginname and passwords.
- SQL string : “-1 union select “Hacked by kanamala”, table_name,column_name from information_schema.columns”.



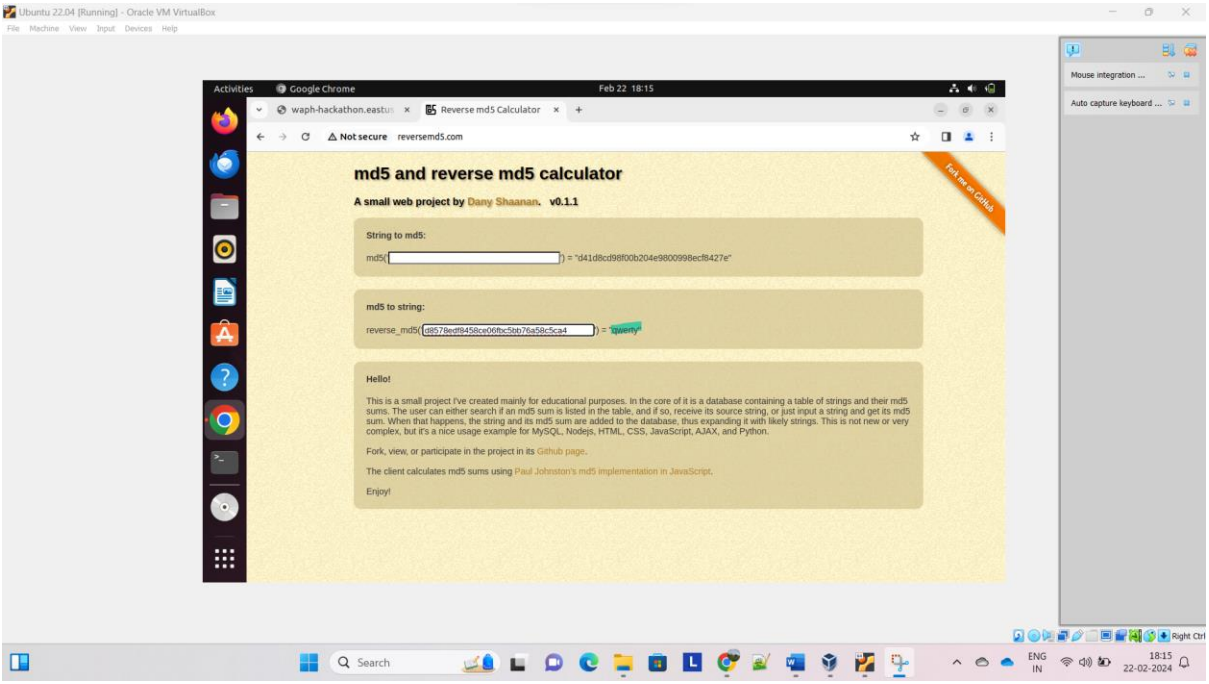
Usernames and passwords:

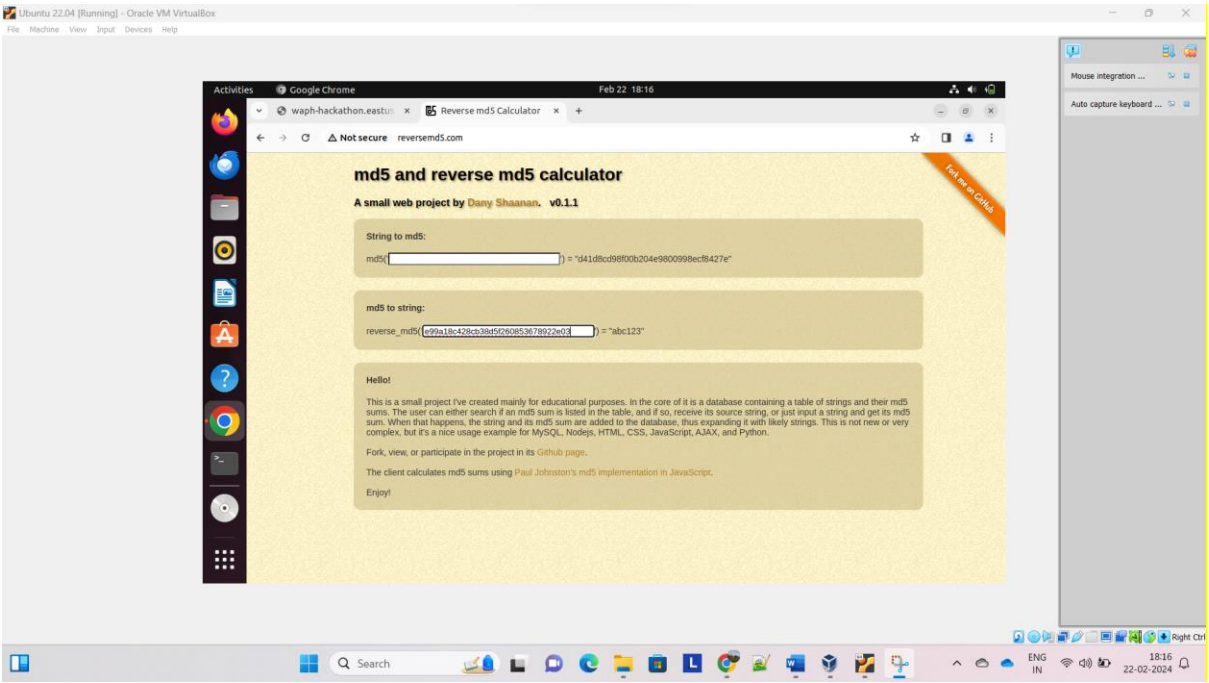
- For this task we need to display usernames and passwords that are available.
- The related information we need retrieve from the login table.
- To achieve this I have used the following SQL string “-1 union select “Hacked by kanamala”, loginname,password from login” .
- The output screenshot was attached below.



Reveal hashed password values:

- Here we need decode the password which are encrypted using the md5.
- To achieve this I have used the online tool. The out screenshot was placed below.





Level 2c:

- Here we need to login to the system using the password which we found.
- The logins are done successfully and the output screenshots are attached below.