NAME : Shrishti Vishwakarma

CLASS : BVOC (First year) Sem 2

TITLE : Make login page that prevents Brute Force Attack (Secure coding)

INSTRUCTOR NAME : Shubham sir

TABLE OF CONTENT

INTRODUCTION

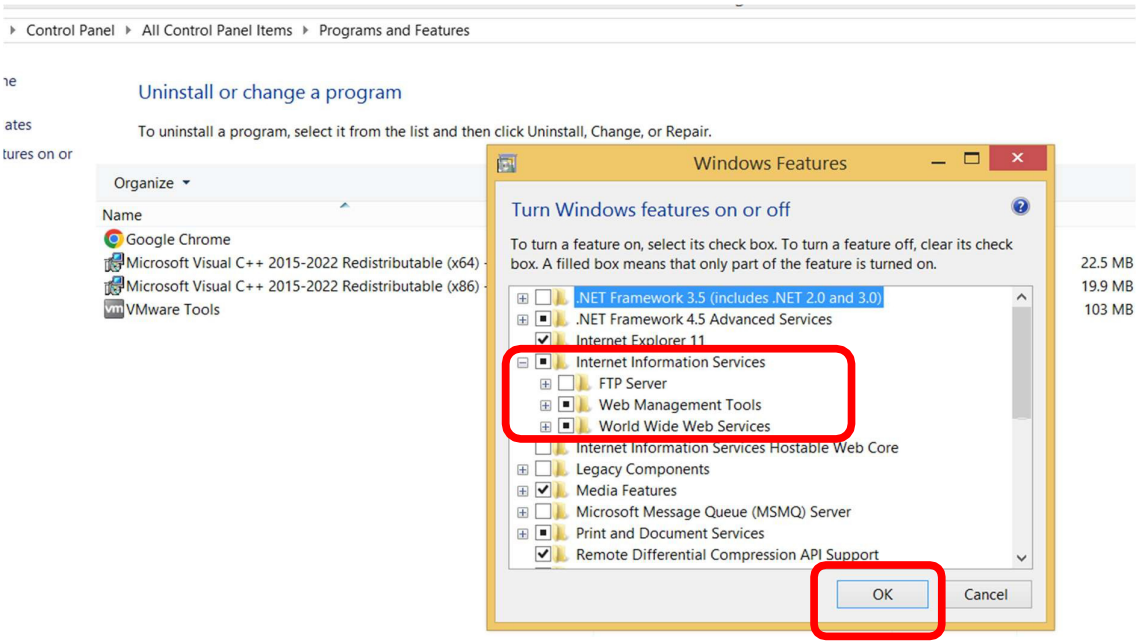
In today's digital landscape, secure user authentication is a critical component of any web application. One of the most common threats faced by login systems is Brute Force Attacks, where an attacker systematically tries many password combinations to gain unauthorized access.

This project demonstrates a secure login page built using Python (Flask), which includes multiple layers of protection against brute force attacks. The system tracks login attempts, introduces delays, and temporarily locks accounts after a certain number of failed login attempts, thereby significantly reducing the risk of unauthorized access.

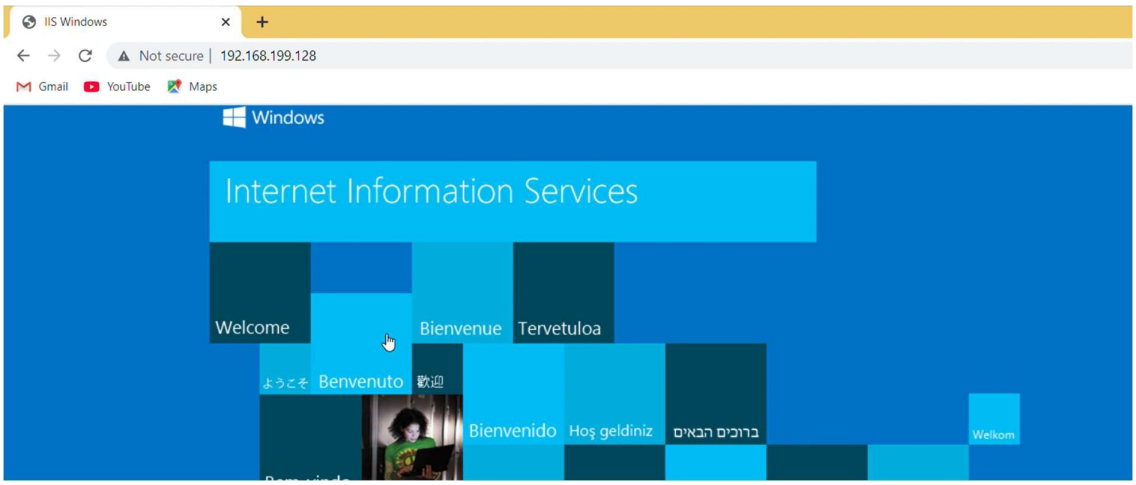
The application also uses secure password hashing techniques (bcrypt), and ensures proper session management, making it a strong foundation for secure user authentication in any modern web application.

Result And Screenshots

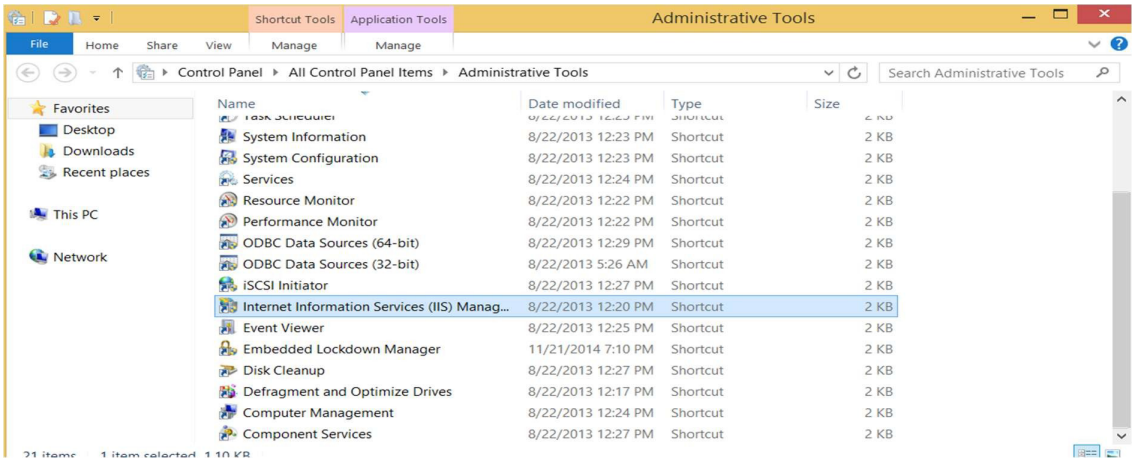
1) Firstly, we have to install **internet information services (IIS)** in windows 8.



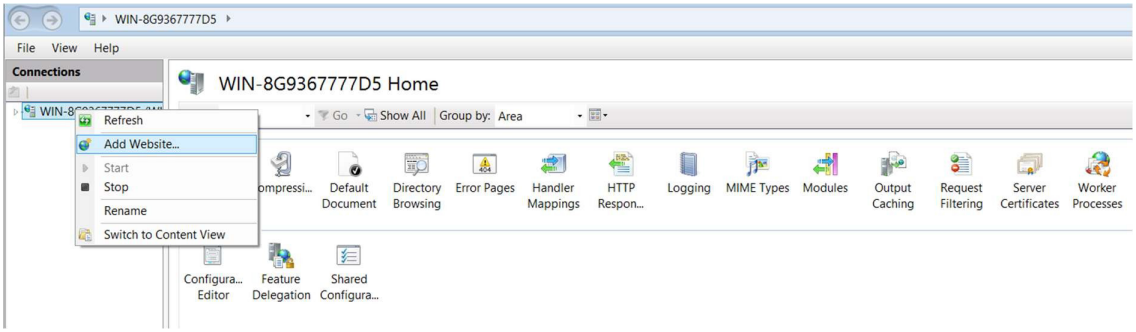
2) When Activate IIS And Enter Your Ip Address This Out Will Show.



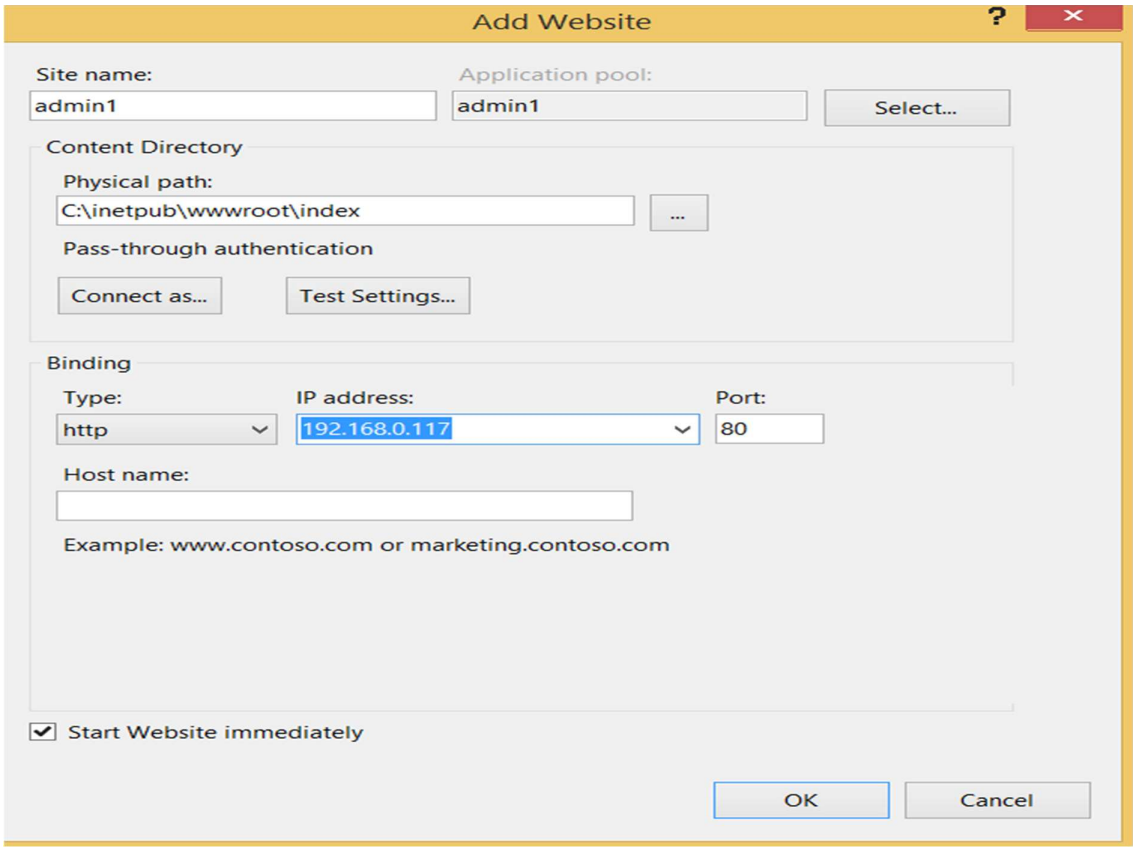
3) After installing go to control panel →Administrative tools→ select IIS manager.



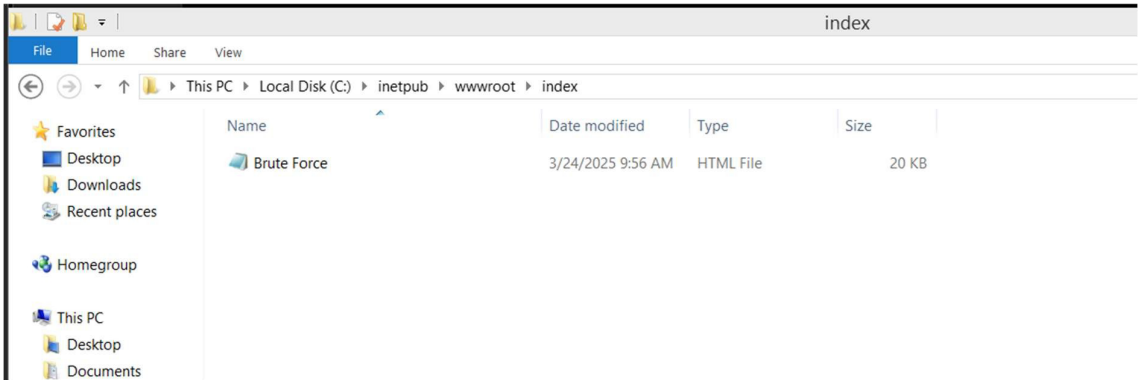
4) Selecting the IIS manager will redirect you to the manager interface and the in the connection panel we have to select the Add Website section.



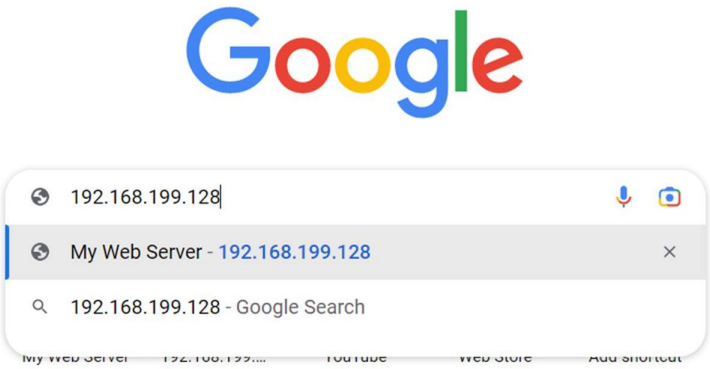
5) Add your web site name and the path which you want to save your directory also select the ip address and the port which host website.



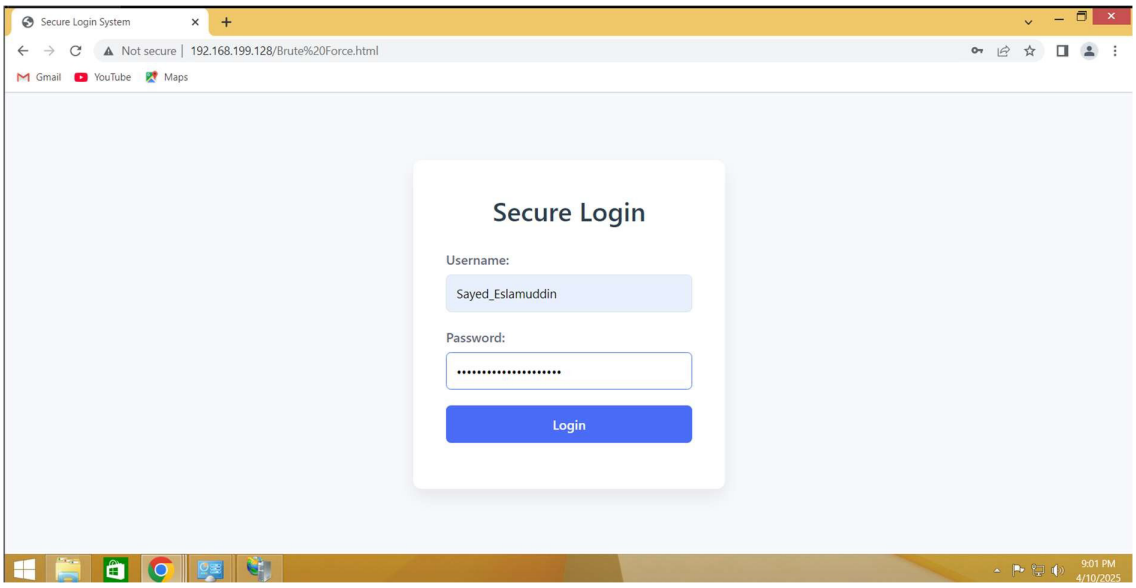
6) Now you have to create a html file which is saved in the path that you used to create the website.



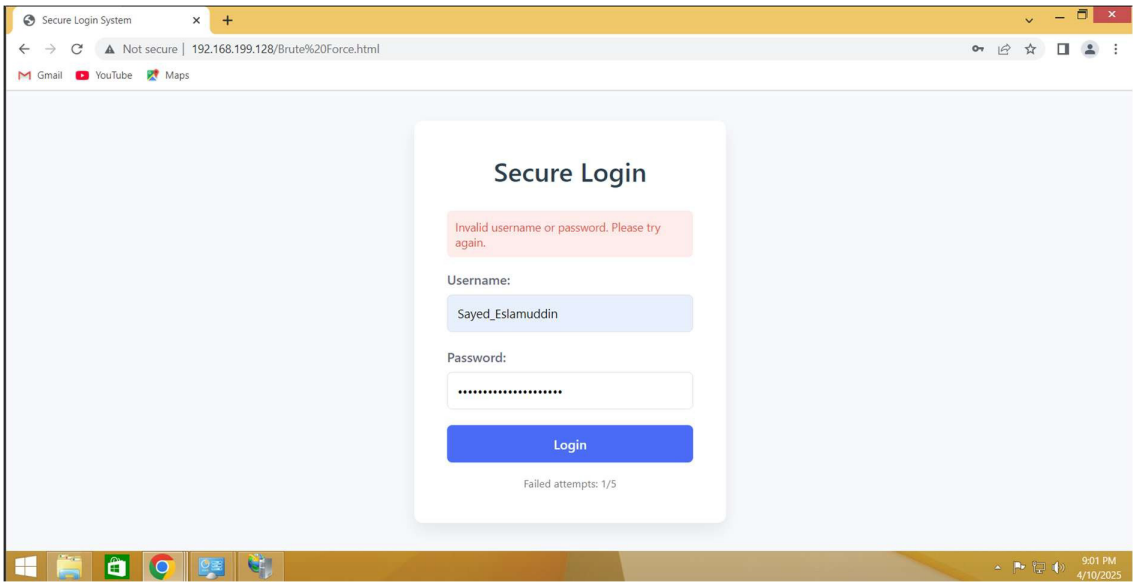
7) Go to your browser and search for your ip address



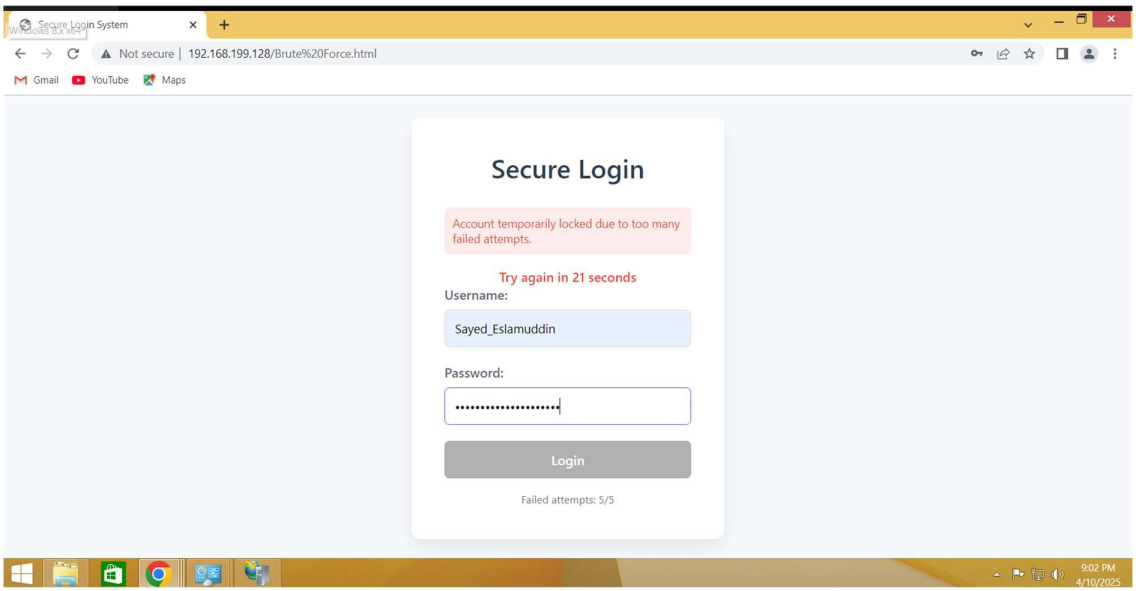
8) Final Output of Brute Force Attack Login Page



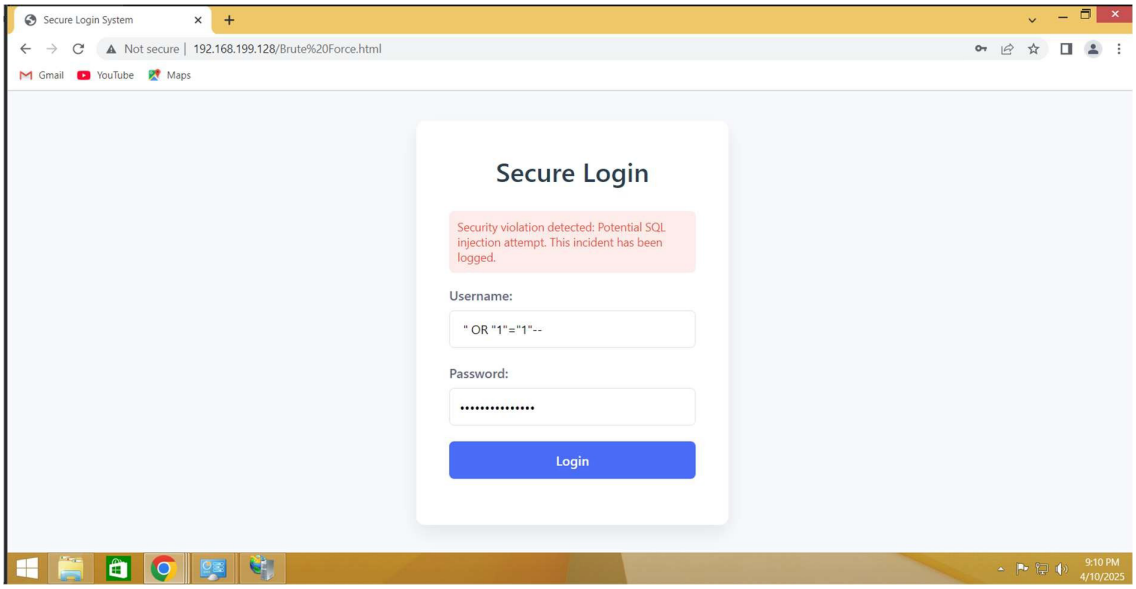
9) If You Enter Any Wrong Password Or User-Name.



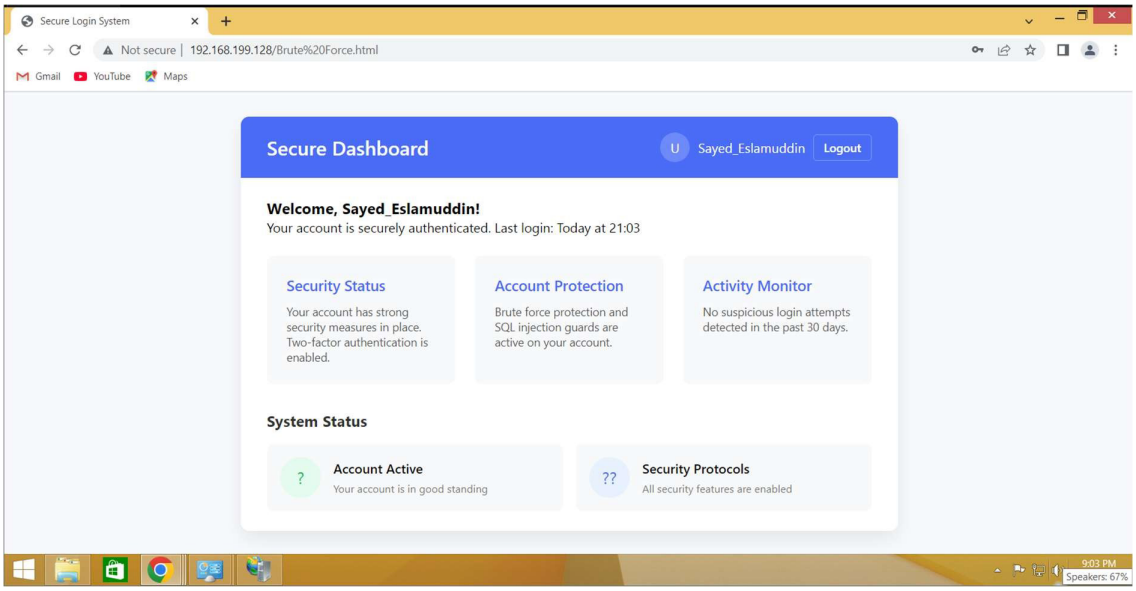
10) Is Only Give 5 Attempts If You Failed It Take 30 Sec To Reuse The Website



11) It Also Allow Injection Attack If Any Person Use SQL Injection Its Show Error Like This:



12) Final Out After Login:



TOOLS USED

1) windows 8.1

2) Windows 11(host)

3) VMware

4) Chrome browser

CONCLUSION

In this project, we successfully developed a secure login system capable of defending against brute force attacks. By implementing key security features such as login attempt tracking, account lockout mechanisms, password hashing using bcrypt, and proper session management, we significantly reduced the risk of unauthorized access.

this approach not only enhances user data protection but also demonstrates how **secure coding practices** can be integrated into everyday application development. As cybersecurity threats continue to evolve, building systems with layered defenses like these is essential for maintaining trust and integrity in web applications.