USER MANUAL

IDE to be used for running the server is VS code and IDE for running the main application is Jupyter Notebook.

I. PRELIMINARY STEPS TO SETUP THE APPLICATION:

1. First, install the following packages in python: keras, tensorflow, opencv, numpy, pandas, matlablib, openpyxl, apachelogs by following the required instructions.
2. Install Xampp server which enables to run a webpage having a front-end and back-end on the local machine.
3. Create a database in the Xampp Mysql server and connect it to the front-end application (Webpage).

II. STEPS TO RUN THE APPLICATION:

1. Before running the main application, the model has to be trained which in turn creates model.h5, dictionary.pickle, model.json files which are required in the testing phase.
2. Apache server and Mysql server has to be started in the Xampp control panel.
3. All the executable files are kept in the directory Xampp/htdocs/final_codes.
4. Open any browser and type the URL localhost/final_codes/home.php which opens the main page of the website. The users can login, create account, post, etc. only if the input data or the user is valid/benign.

6tt68

III. USAGE OF THE APPLICATION:

1. Once the home.php is rendered on the screen, click the appropriate user button by choosing either user login or admin login.
2. User login:
    - Login with the appropriate credentials for an existing user or register to the portal for a new user account. On successful login, the user is navigated to the welcome page and for an unsuccessful login (attempt to SQLi attack), the user is alerted and blocked.
    - Once the user lands on welcome page, he/she can perform their desired actions by choosing the respective links in the navigation bar. For every attempt to perform attacks in search fields/post fields, the user is alerted and blocked.
    - 'Your account' in the navbar provides all the details of the user logged in.
3. Admin login:
    - Login with the appropriate admin credentials. Admin has the control to perform log analysis by clicking the same in the rendered page. Once the log analysis is performed, admin can view the attack statistics on the screen.