Incident Response Automation

In propose work we are developing an online tool which will scan and monitor all network log data to detect all cyber-attacks and then can isolate such attacking system from the network to minimize further spread of attacks to other system. This application will detect all network attacks by employing Wireshark network attack detection API. Identifying and resolving such cyber-attack is known as Incident Response Automation.

Incident response is the process of identifying, investigating and resolving security incidents and breaches isolating the affected systems from further damage, minimize the damage and recover the systems.

Incident response in Cyber security is a structured process an organization uses to handle a data breach or cyber-attack, aiming to minimize damage and restore systems. It involves identifying an attack, containing its spread, and recovering from the incident to reduce the risk of future attacks. This process is often guided by an Incident Response Plan (IRP) that outlines procedures for different types of cyber-attacks.

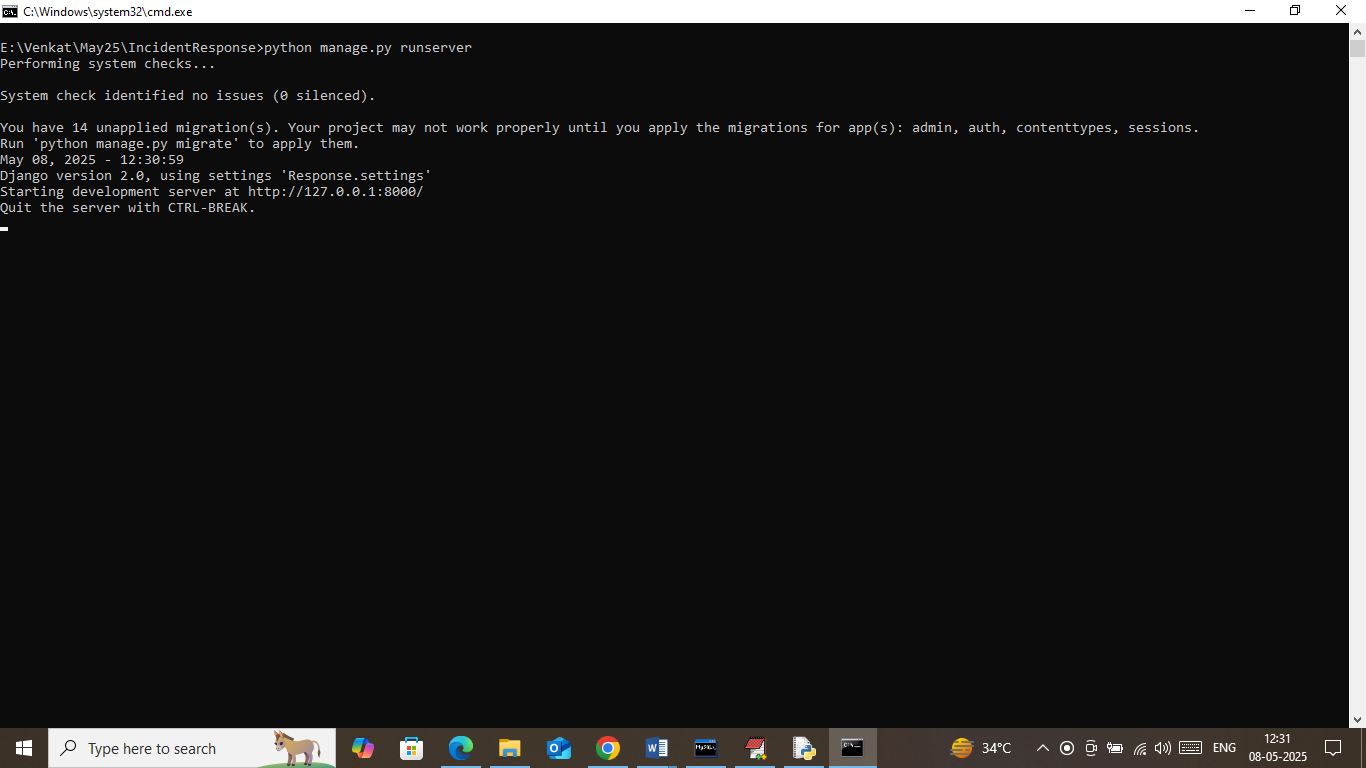
To implement cyber-attack automation process we have designed following modules

1. New User sign up: user can sign up with the application
2. User Login: user can login to system
3. Data Collection & Incident Detection: using this module user can upload network log data and then apply scanning API to detect all abnormal network activities and then generate report with different alerts
4. Alert Analysis: this module analyse all network traffic data file and then system will scan all packets to detect malicious activities and then generate detail graph on different attacks happened from different IP and PORT.

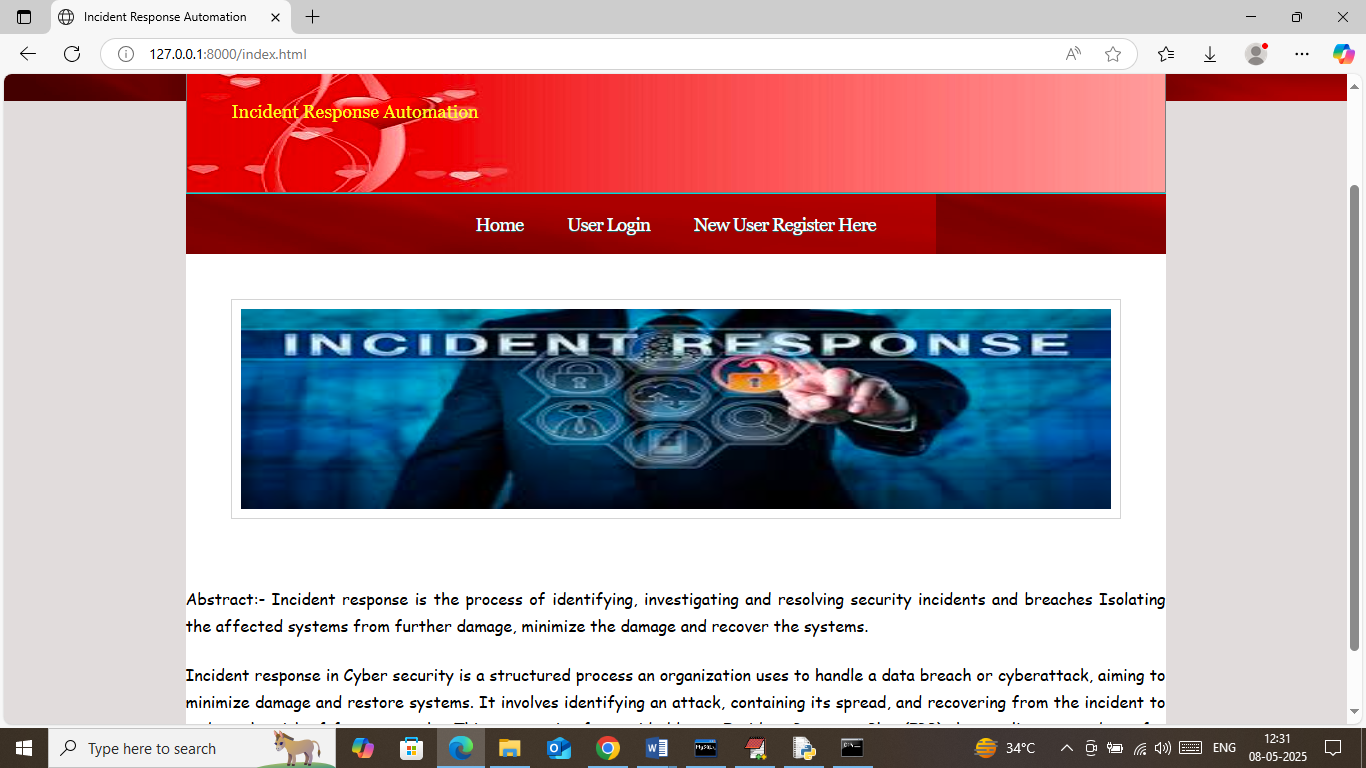
To run project install python 3.7.2 and then install all packages given in requirements.txt file and then install MYSQL and then copy content from database.txt file and paste in MYSQL console to create database

SCREEN SHOTS

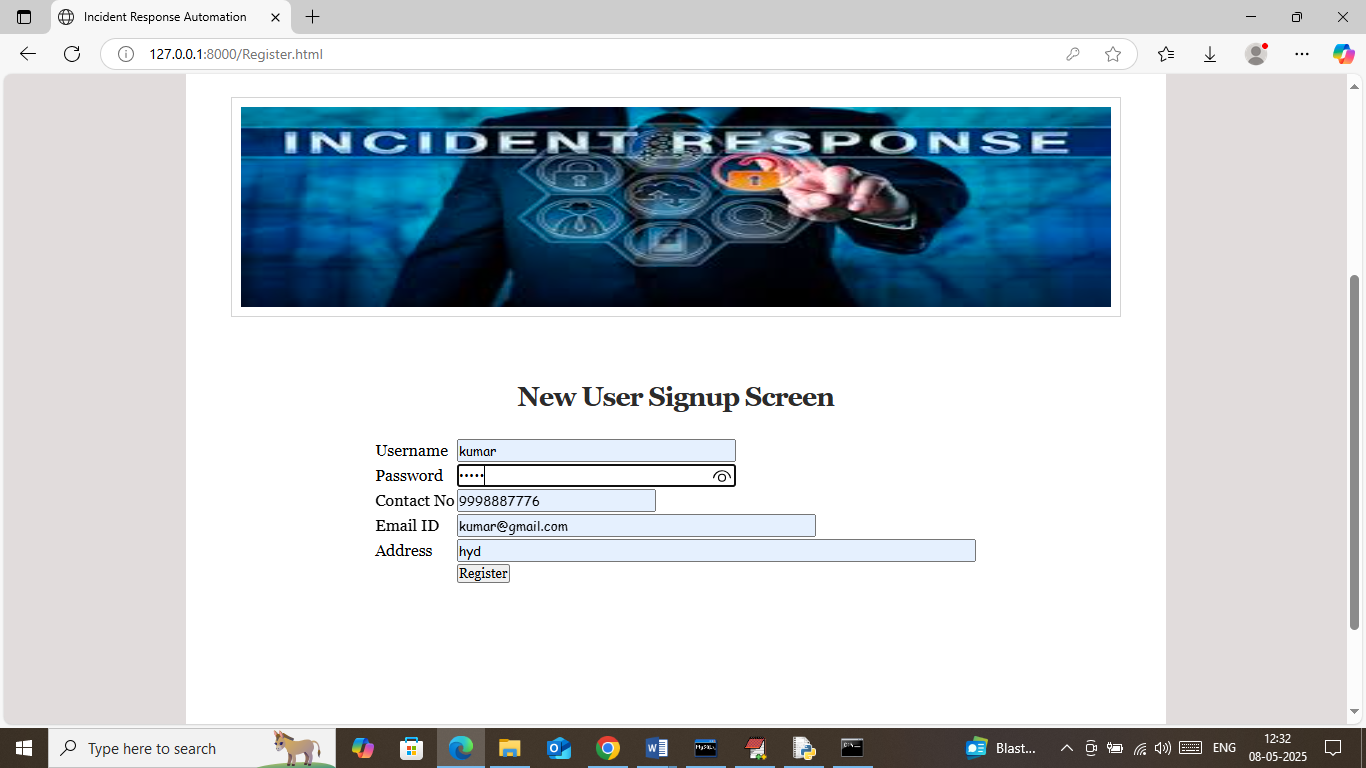
To run project double click on ‘run.bat’ file to get below page



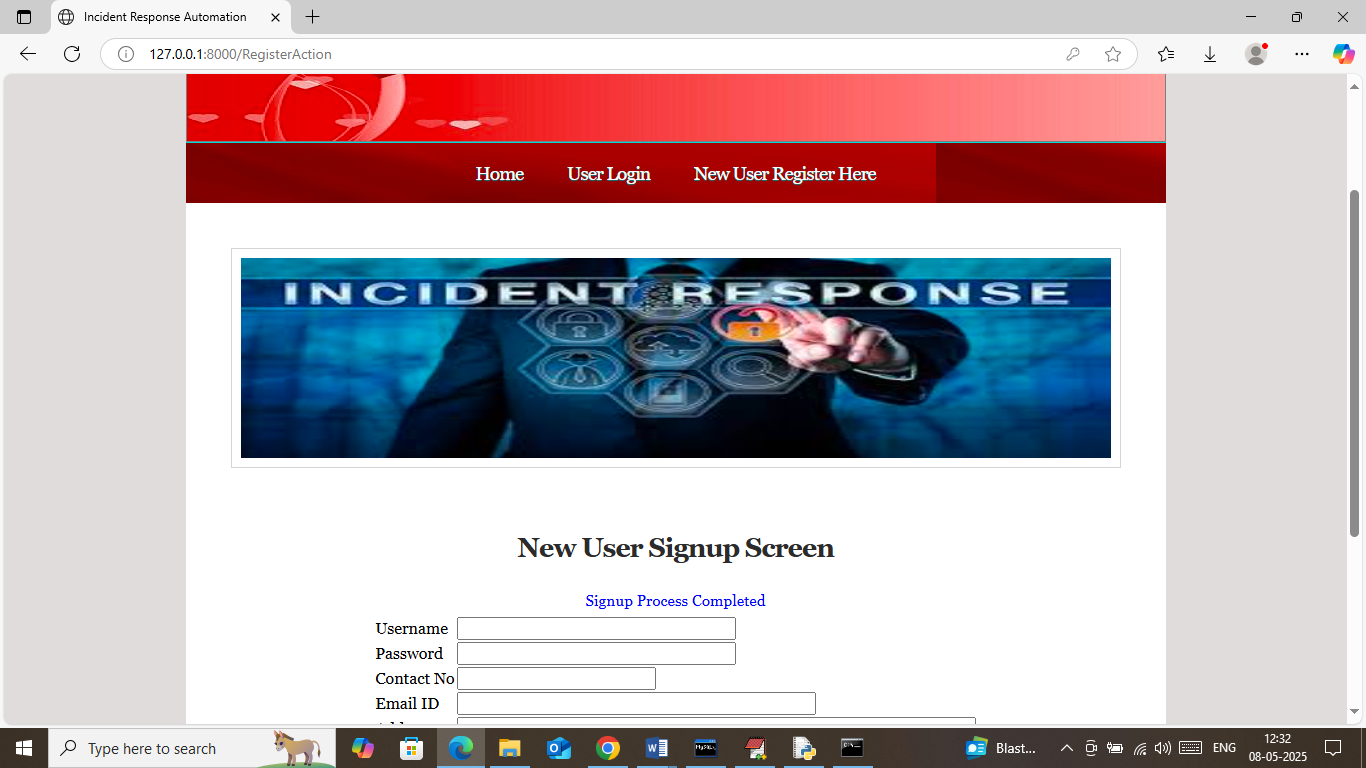
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and then press enter key to get below page



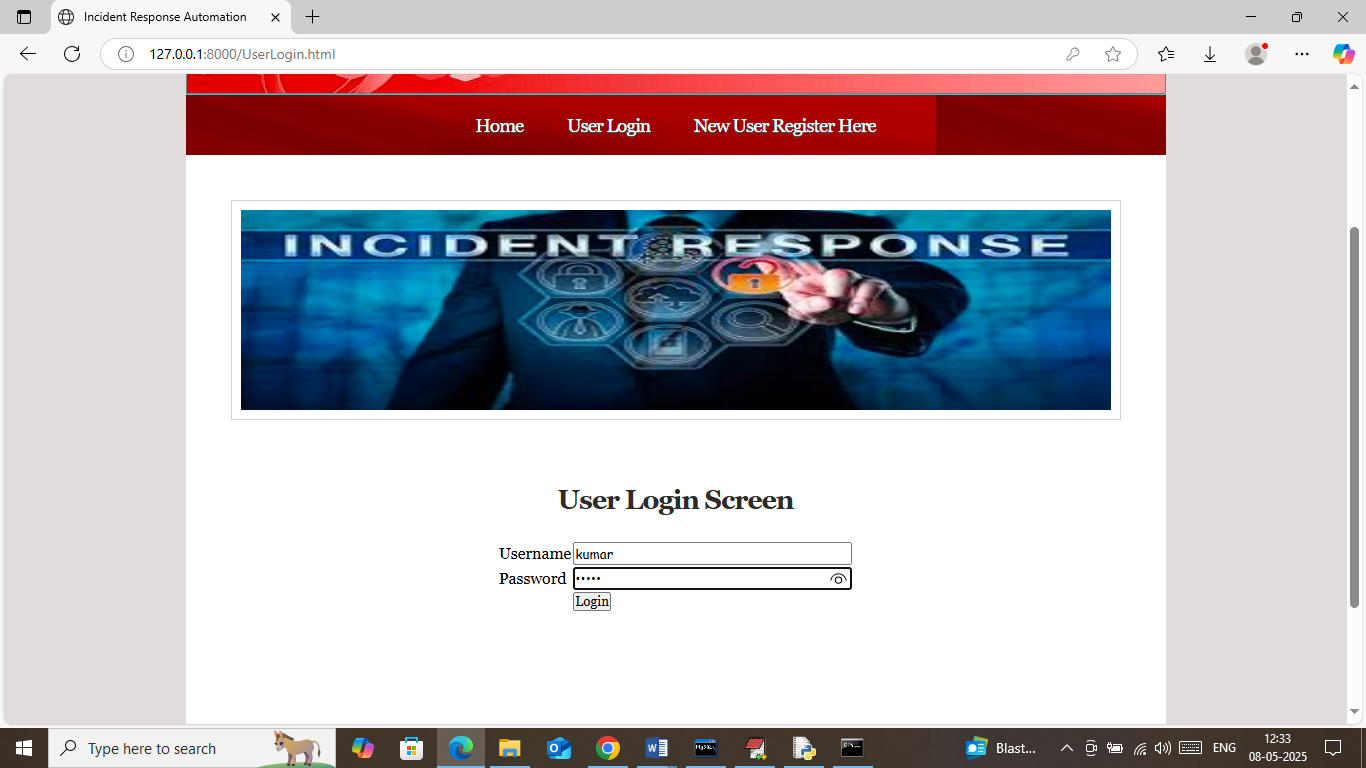
In above screen click on ‘New User Register’ link to get below page



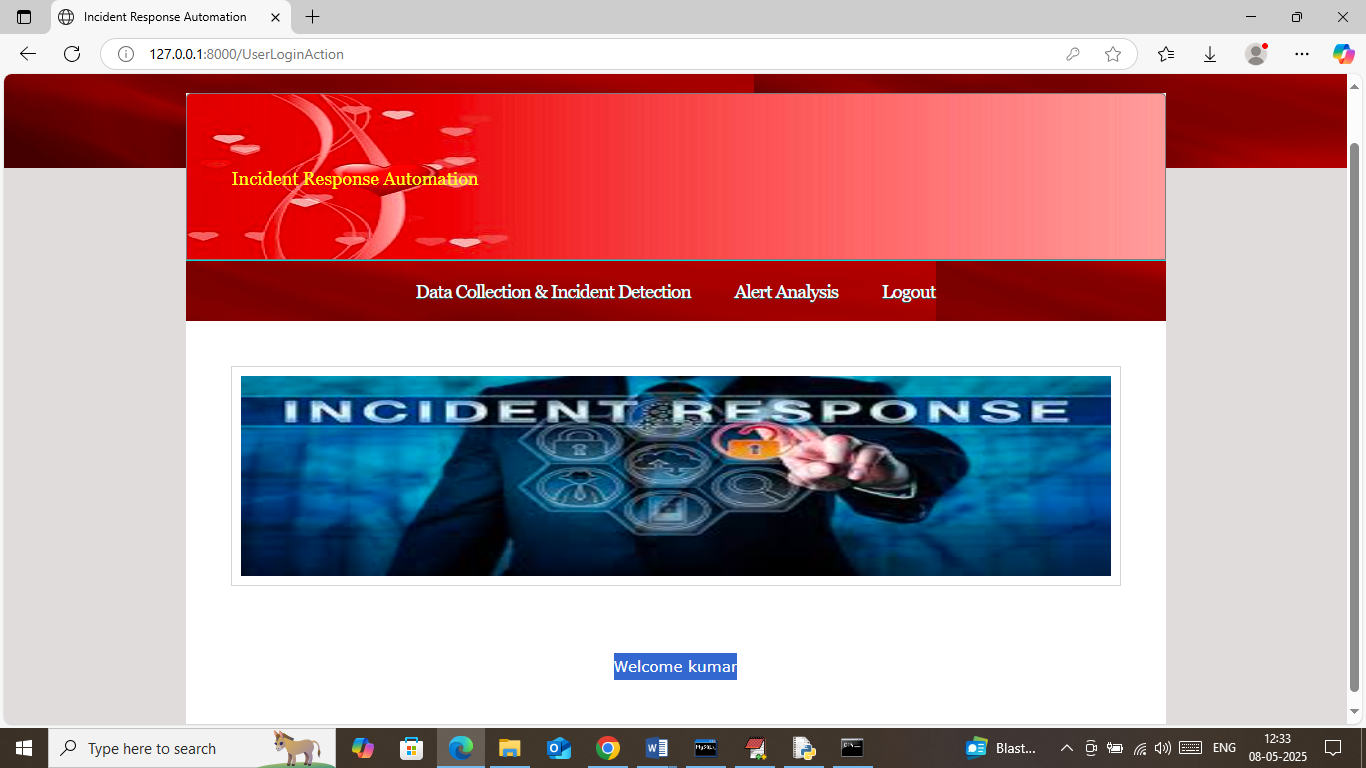
In above screen user is entering sign up details and then press button to get below page



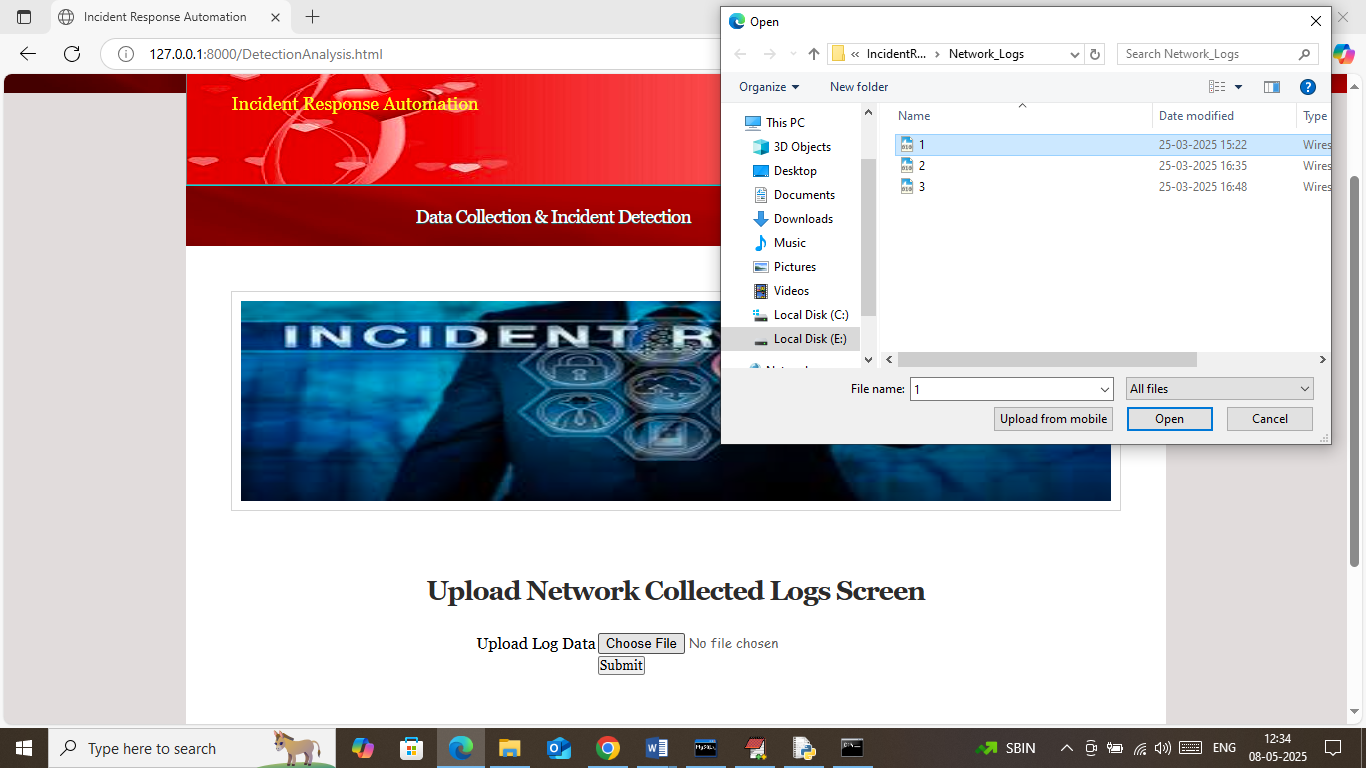
In above screen sign up task completed and now click on ‘User Login’ link to get below page



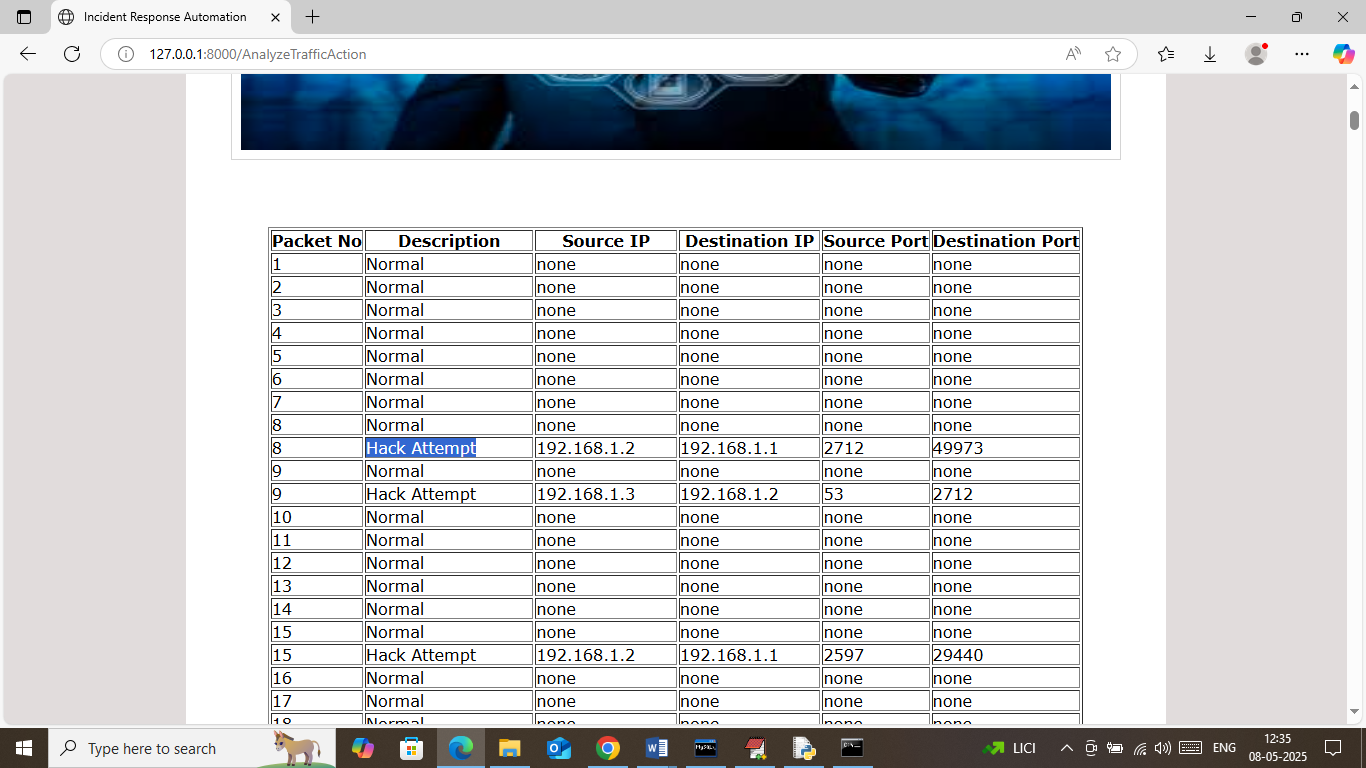
In above screen user is login and after login will get below page



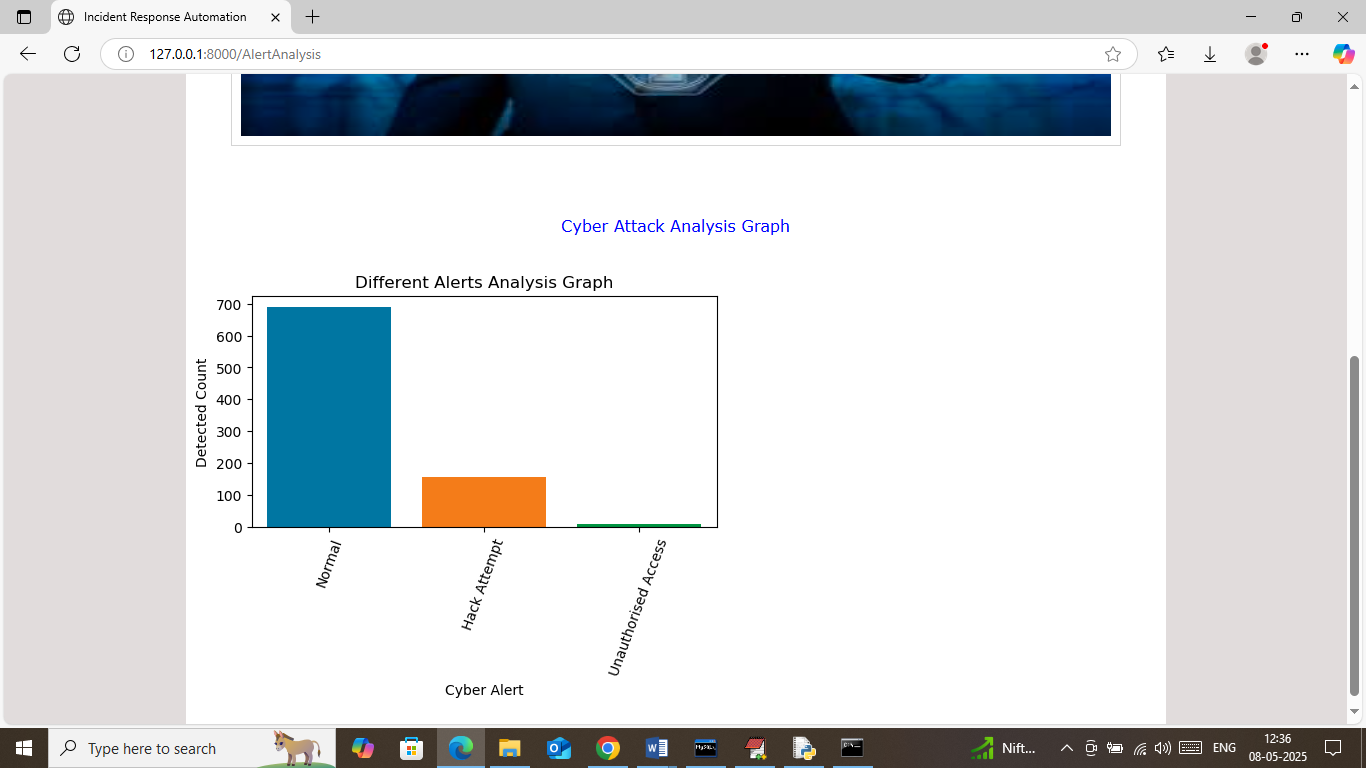
In above screen user can click on ‘Data Collection & Incident Detection’ link to upload network log data and then analyse data to detect cyber attacks



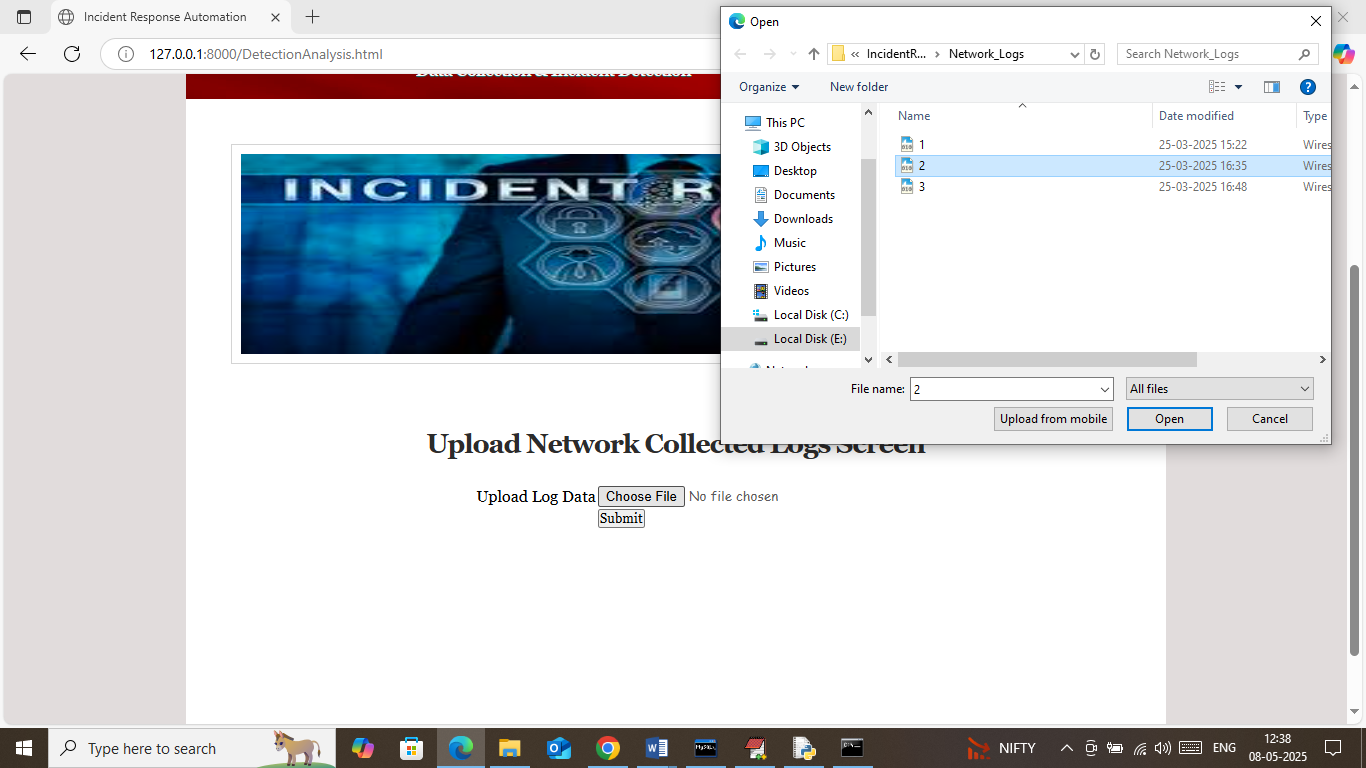
In above screen selecting and uploading network log data and then click on buttons to get below report



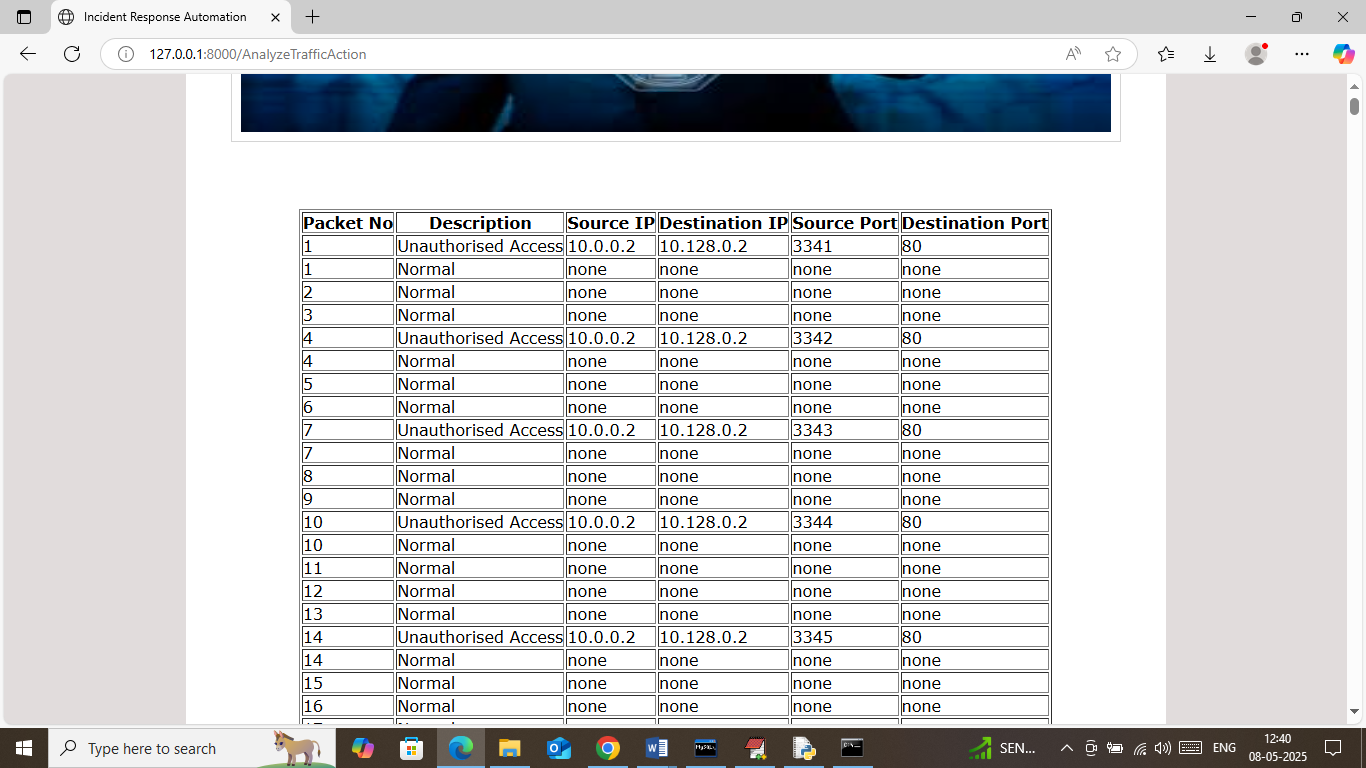
In above screen can see reports generated from log data where displaying different attack names happening from different IP and port no and now click on ‘Alert Analysis’ link to get below page



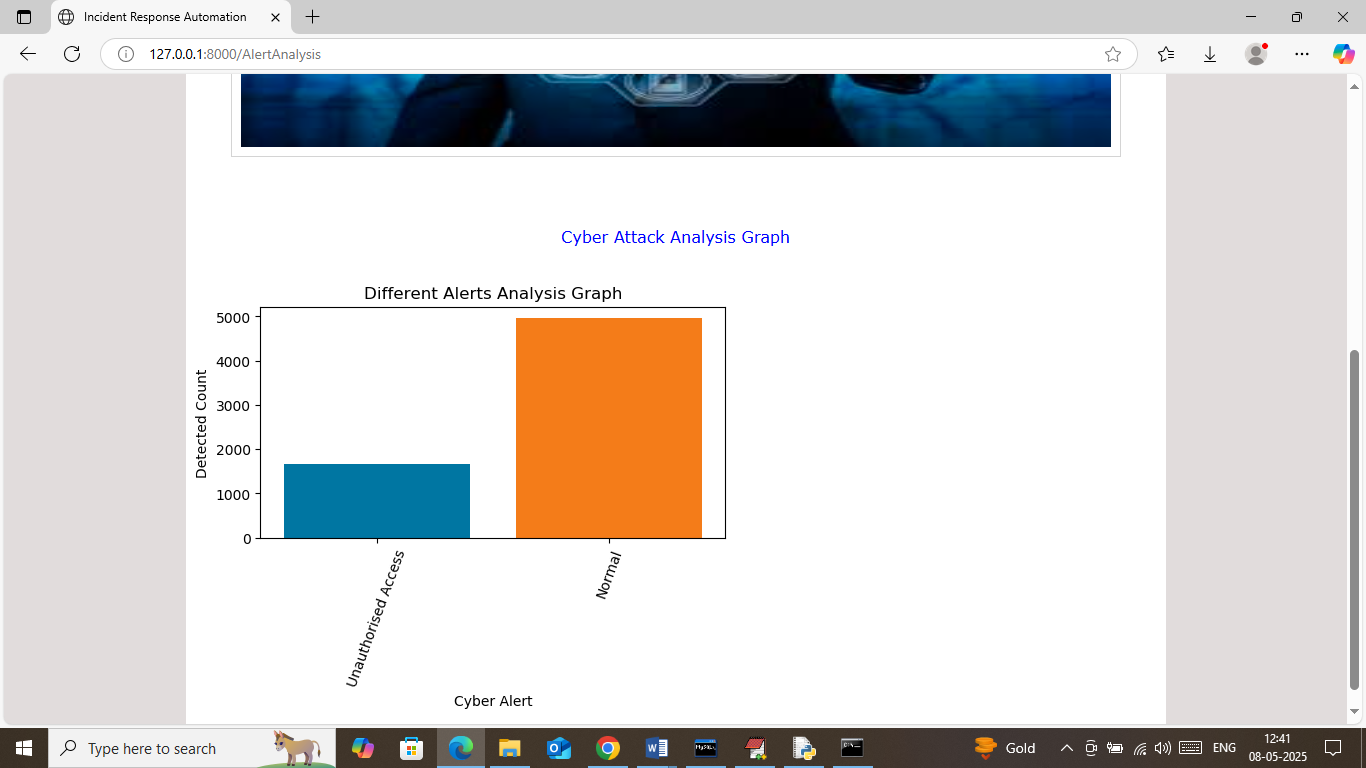
In above alert analysis graph where x-axis represents type of activities and y-axis represents activity count. Similarly you can upload and test any other log file and below is another log output



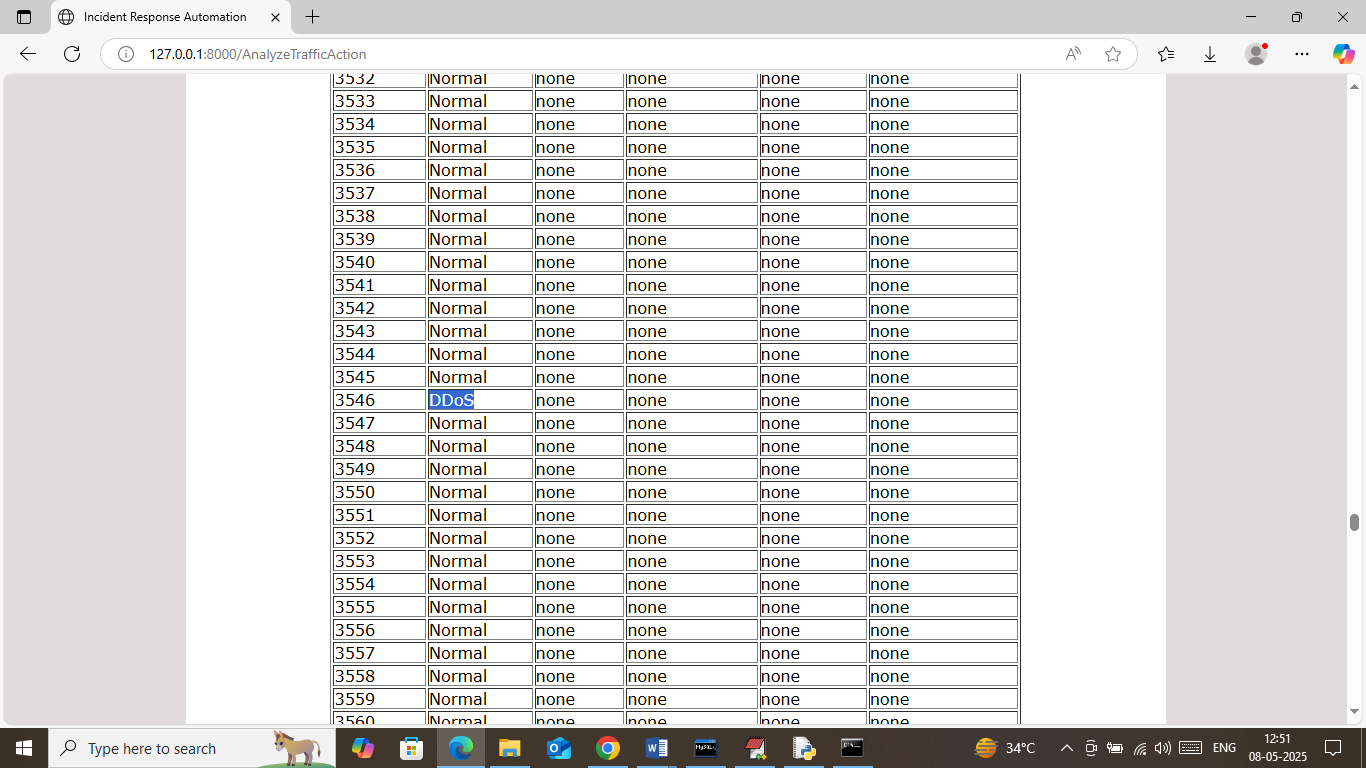
In above screen uploading another log data and then press button to get below page



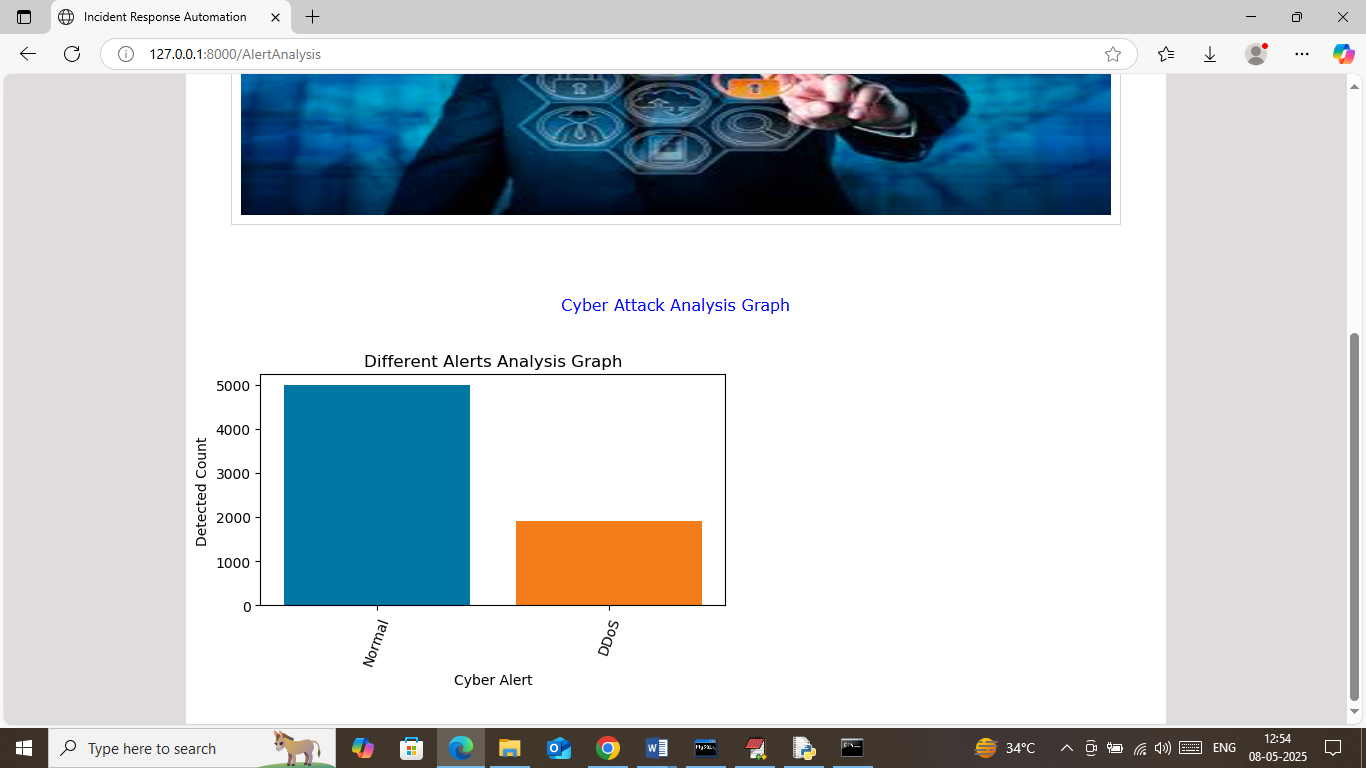
In above screen can see detected normal and attack packets and now click on Analysis Alert to get below page



In above graph can see type of detected attacks



In above screen DDOS attack detected



In above analysis graph can see number of DDOS and normal traffic detected from network log data

Similarly you can upload and test any other network log data