Web Vulnerability

In this project, we propose a methodology to leverage Machine Learning (ML) for the detection of web application vulnerabilities. Web applications are particularly challenging to analyses, due to their diversity and the widespread adoption of custom programming practices. ML is thus very helpful for web application security: it can take advantage of manually labelled data to bring the human understanding of the web application semantics into automated analysis tools. We use our methodology in the design of Mitch, the first ML solution for the black-box detection of Cross-Site Request Forgery (CSRF) vulnerabilities. Mitch allowed us to identify 35 new CSRFs on 20 major websites and 3 new CSRFs on production software.

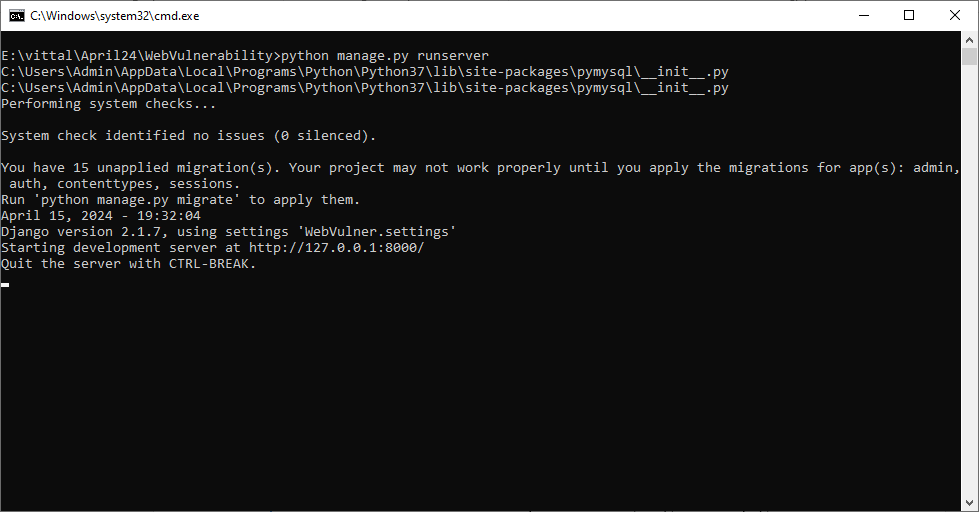
This project consists of two modules

1. Admin Module: admin can login to system using username and password as admin and admin. After login admin can activate new registered user account. Admin can view all CSRF list, view users, view POST and GET request
2. New User Sign up: user can sign up with the application
3. User Login: once account activated then user can login to system and then enter any URL along with depth value to scan URL to detect vulnerability and then apply mitch process to identify URL as vulnerable or not. User can train ML algorithms on different methods and then calculate accuracy and other metrics.

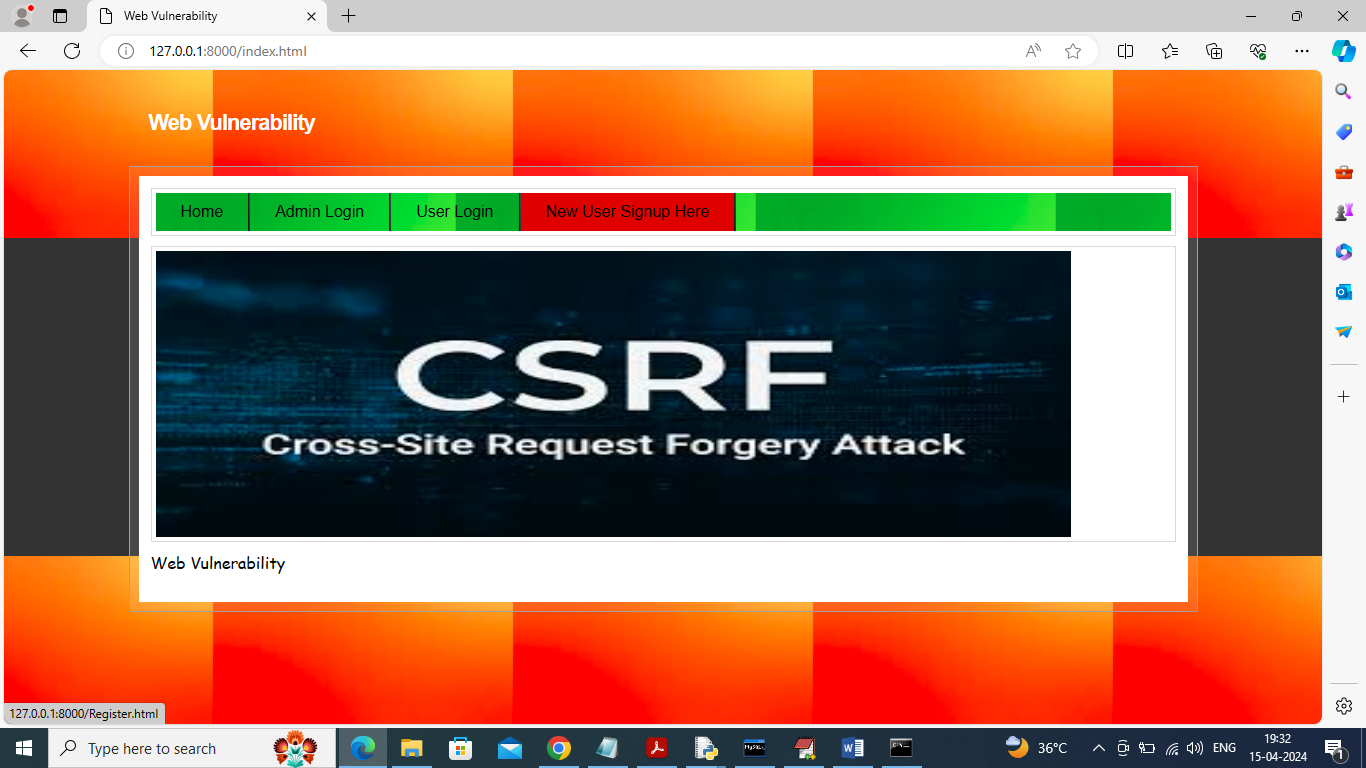
To run project install python 3.7.2 and then install all packages given in requirements.txt file. Install MYSQL database and then open MYSQL console and then copy content from ‘database.txt’ file and paste in MYSQL console to create database

SCREEN SHOTS

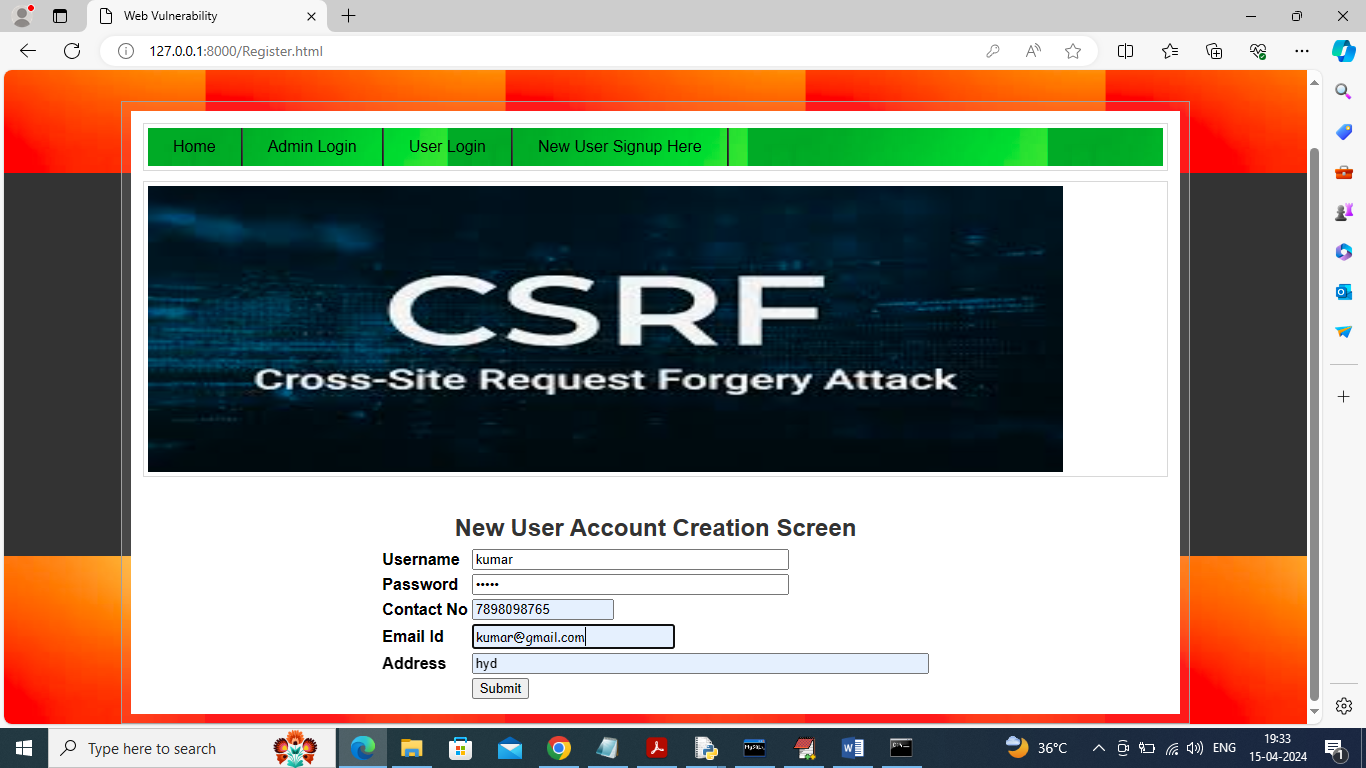
To run project double click on ‘run.bat file to start python server and get below page



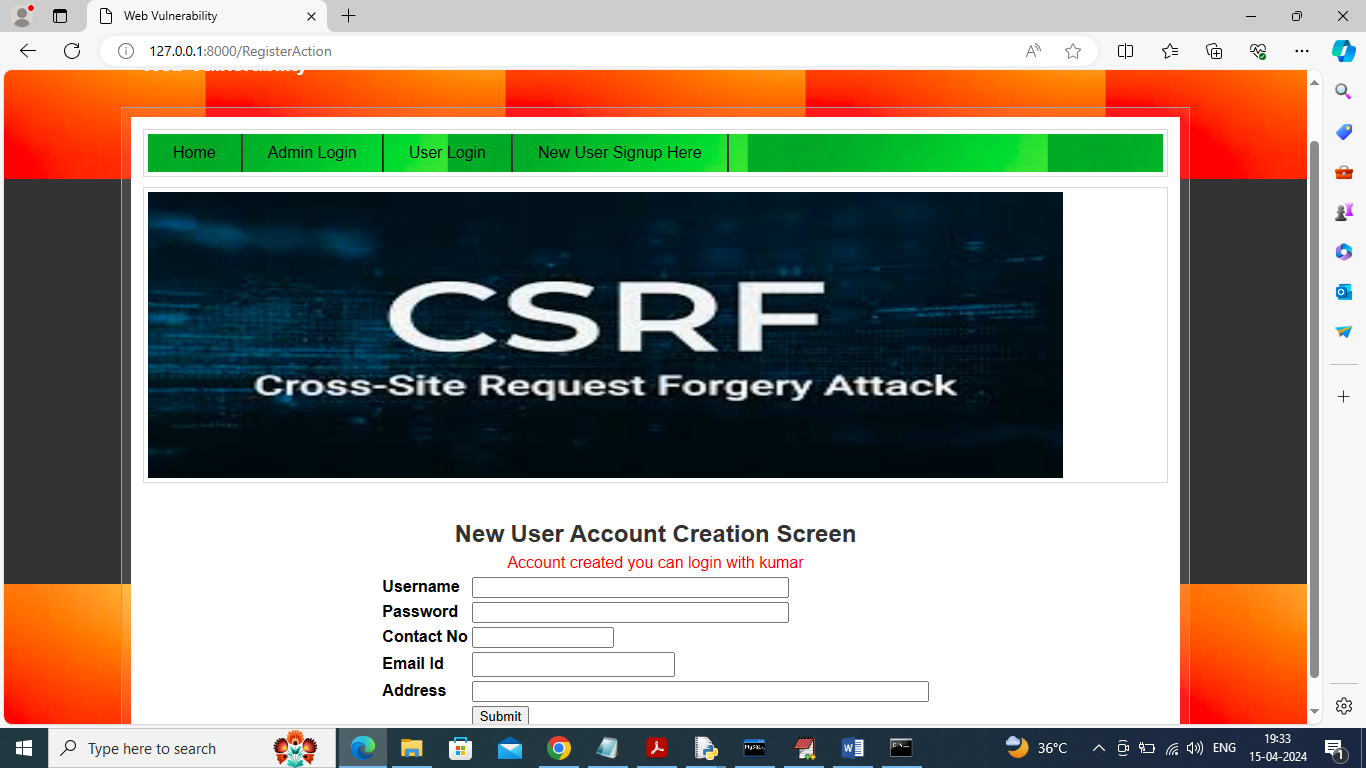
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



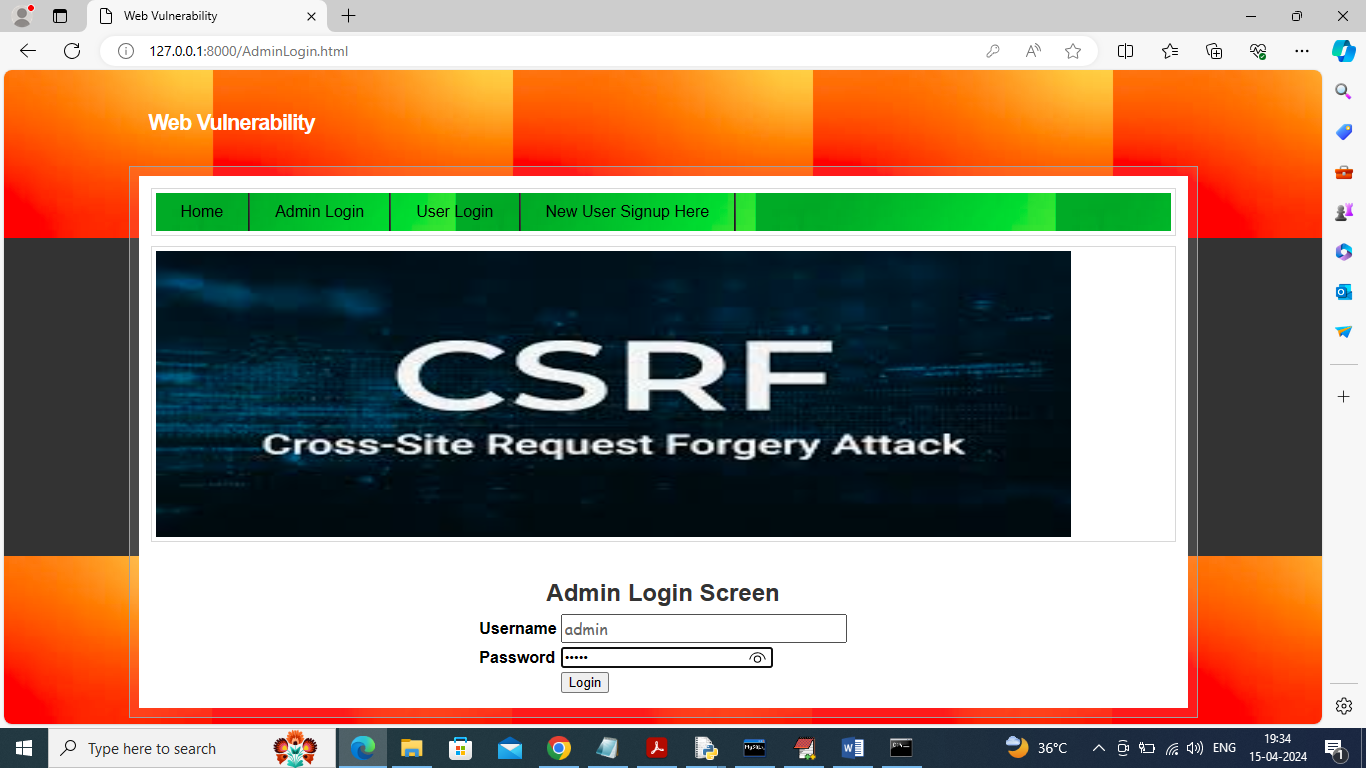
In above screen click on ‘New User Sign up’ link to get below page



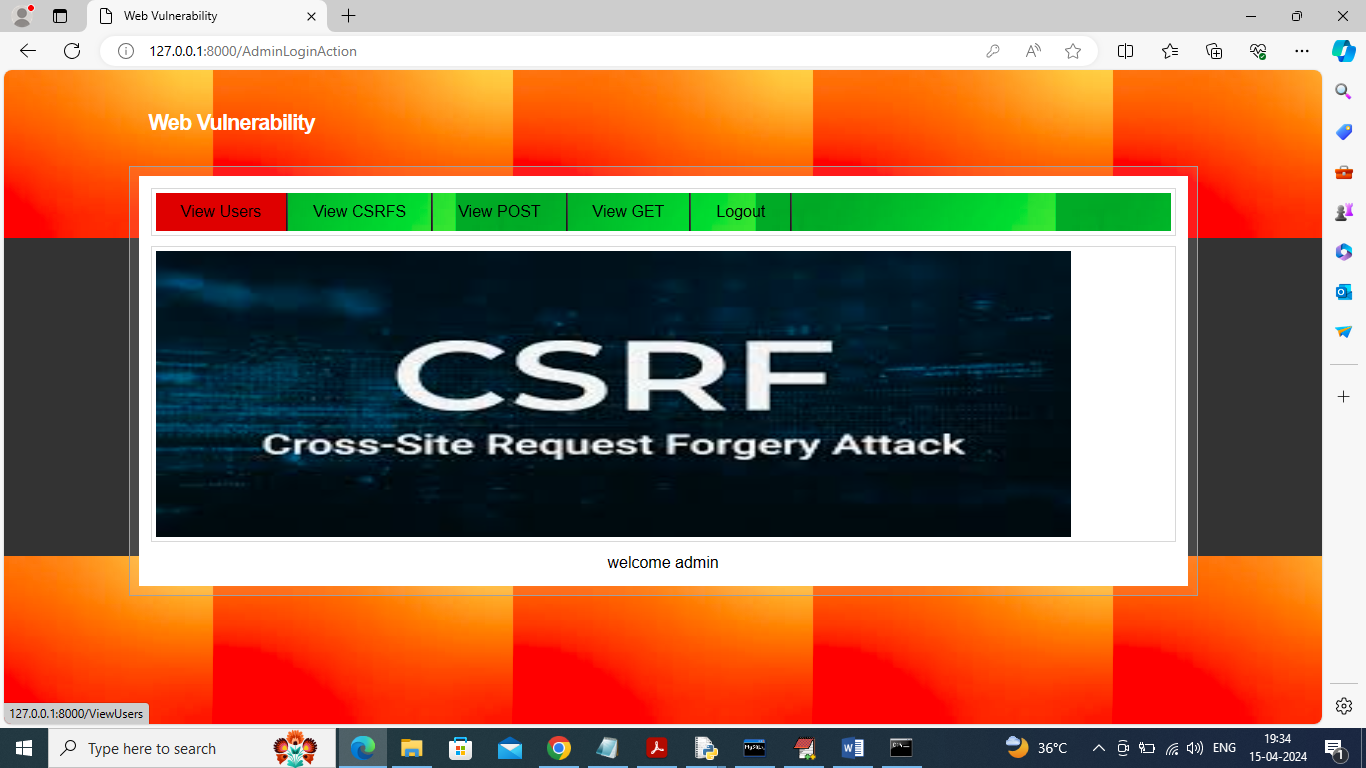
In above screen user is entering sign up data and then press button to get below page



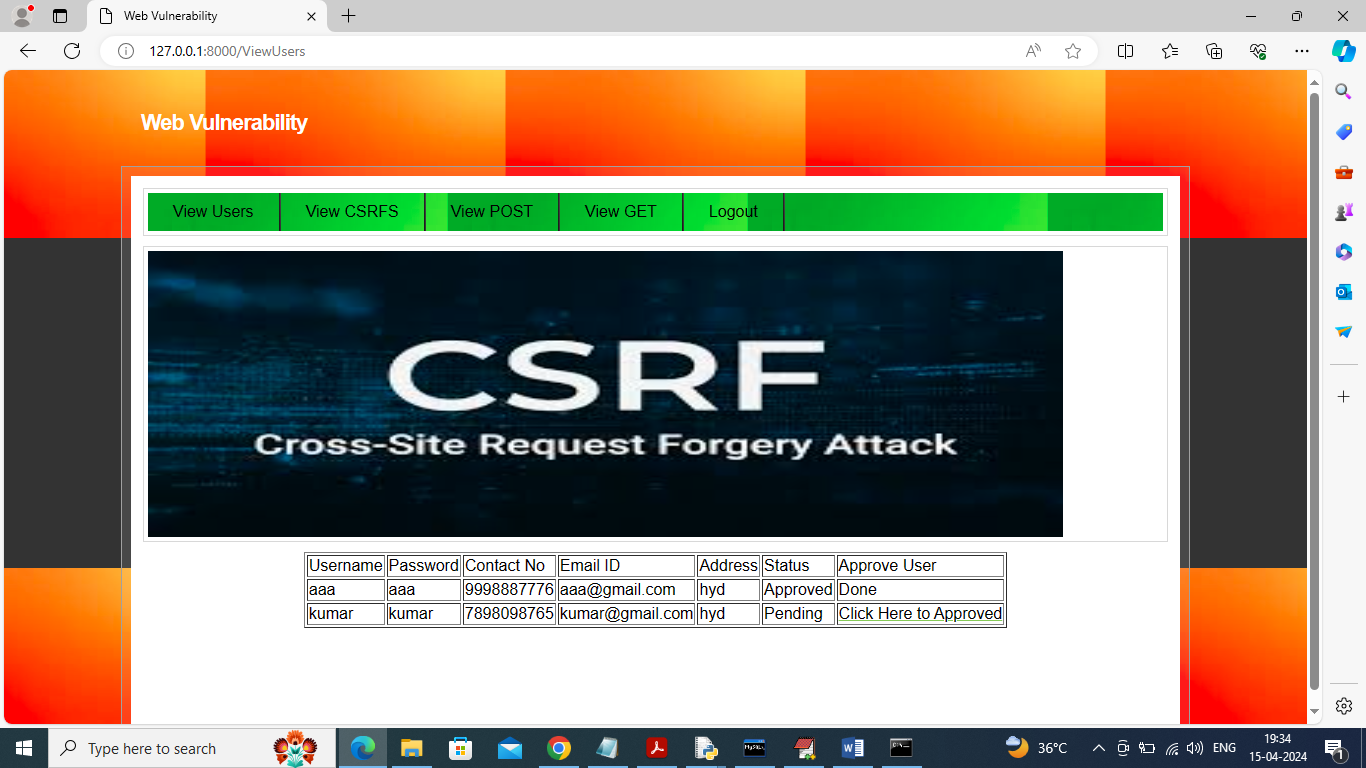
In above screen user account created and now login as admin to activate user account



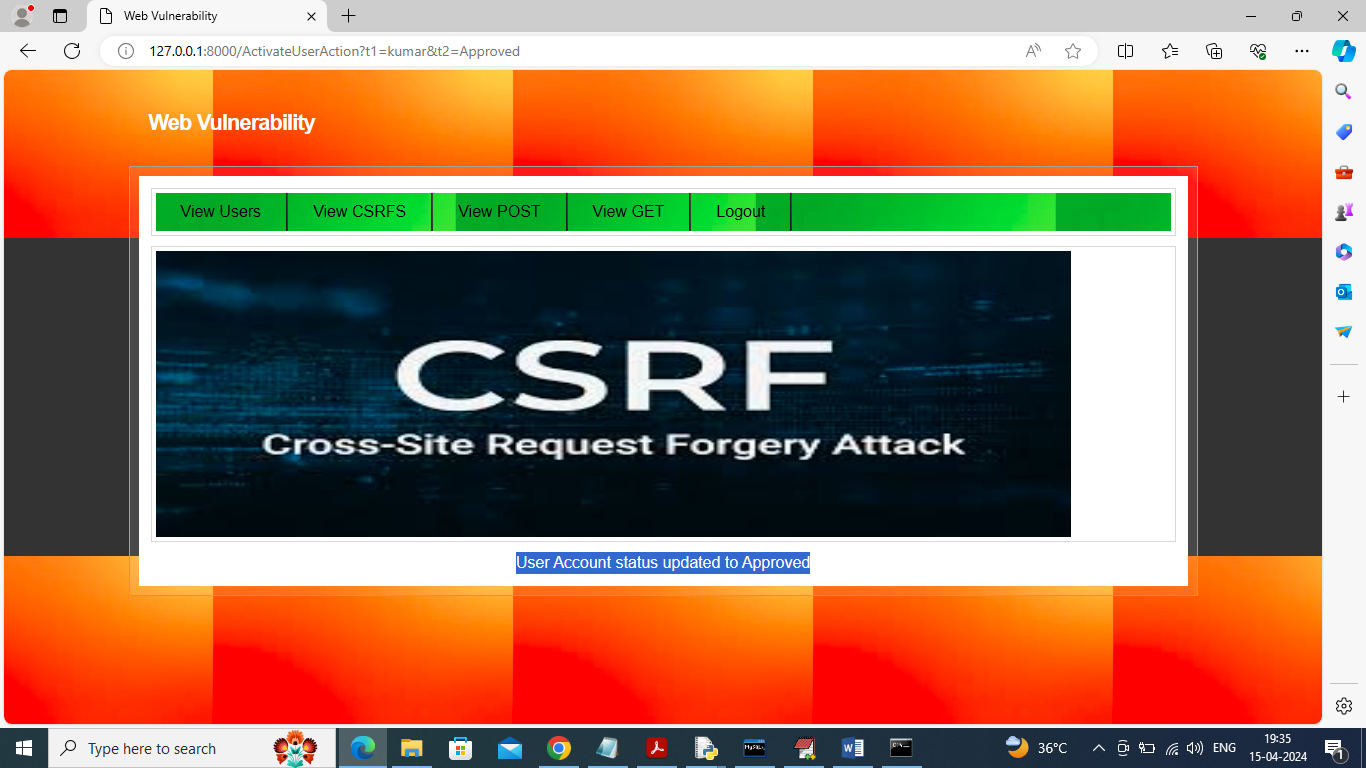
In above screen admin is login and after login will get below page



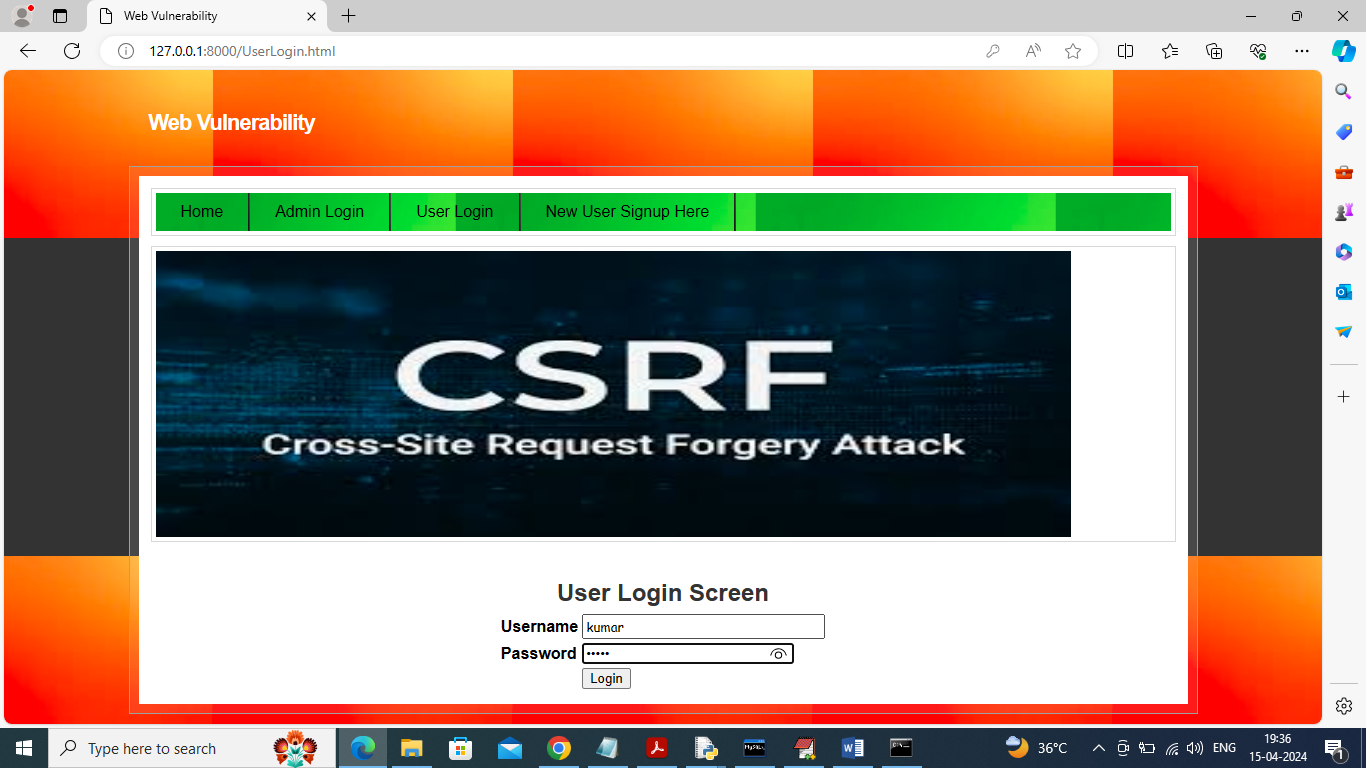
In above screen admin can click on ‘View Users’ link to get below page



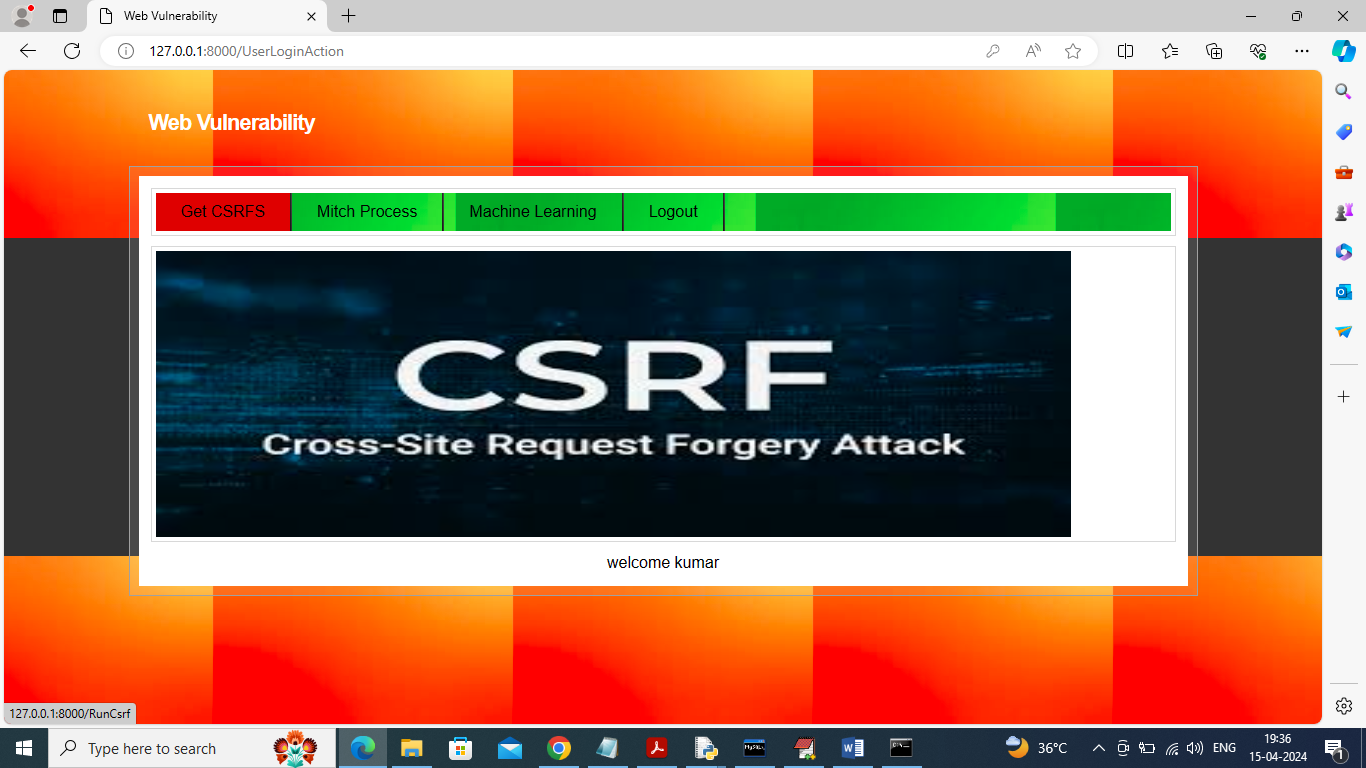
In above screen admin can view list of accounts and can click on ‘Click Here to Approved’ link on pending accounts to approve users and get below page



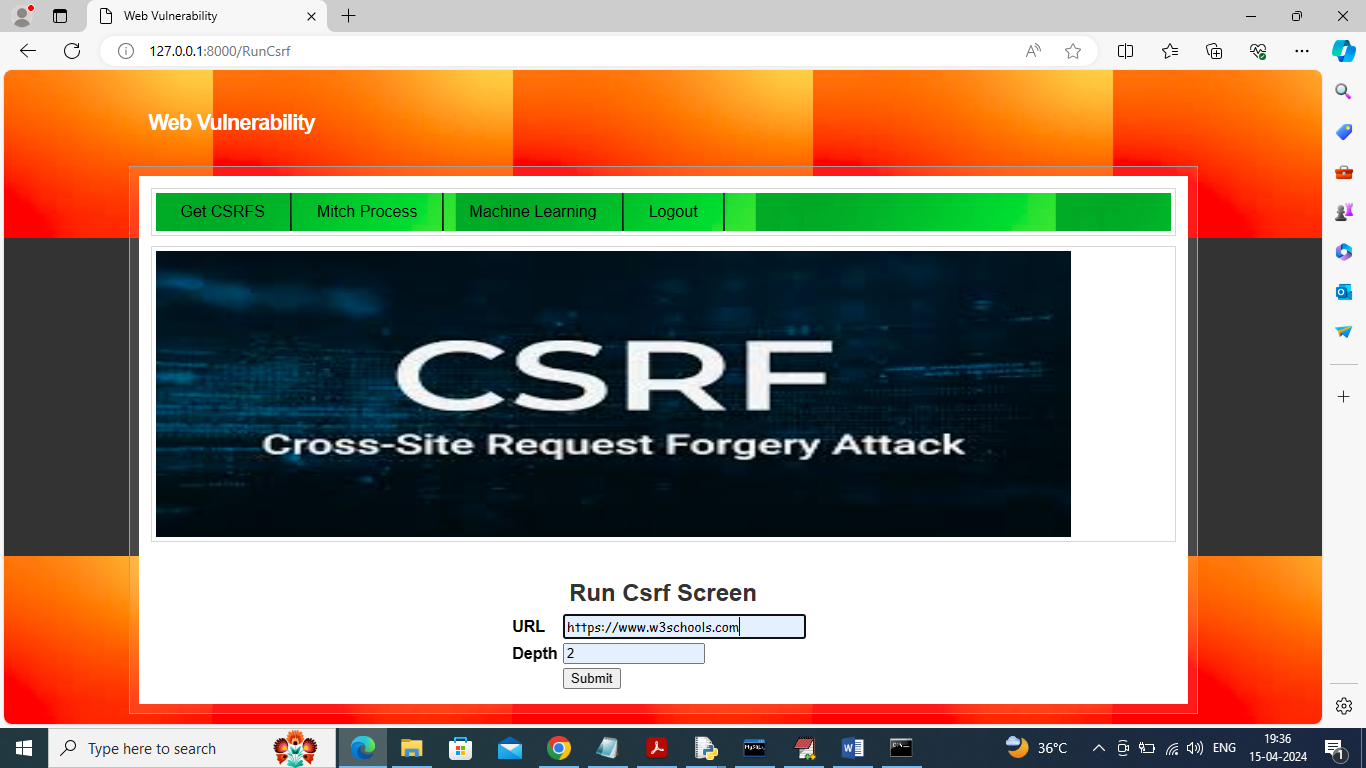
In above screen user account approved and now logout and login as user



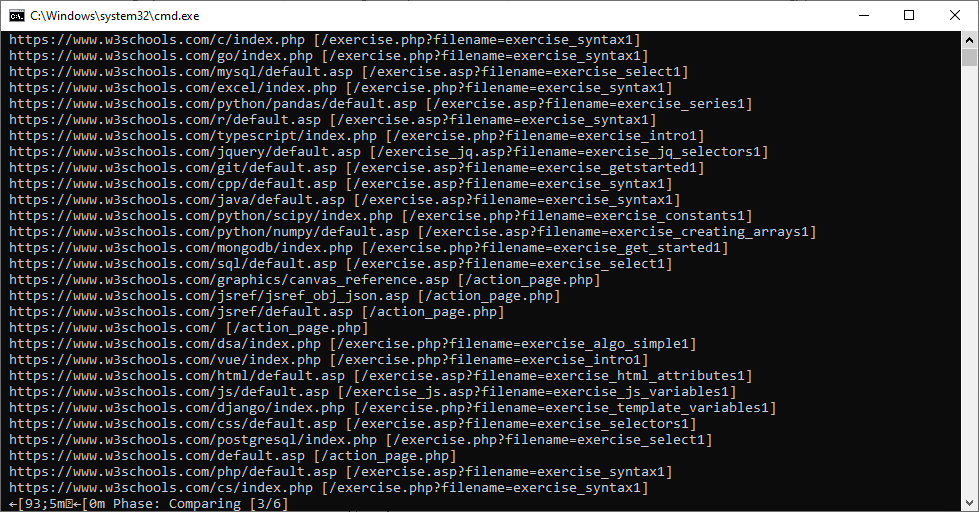
In above screen user is login and after login will get below page



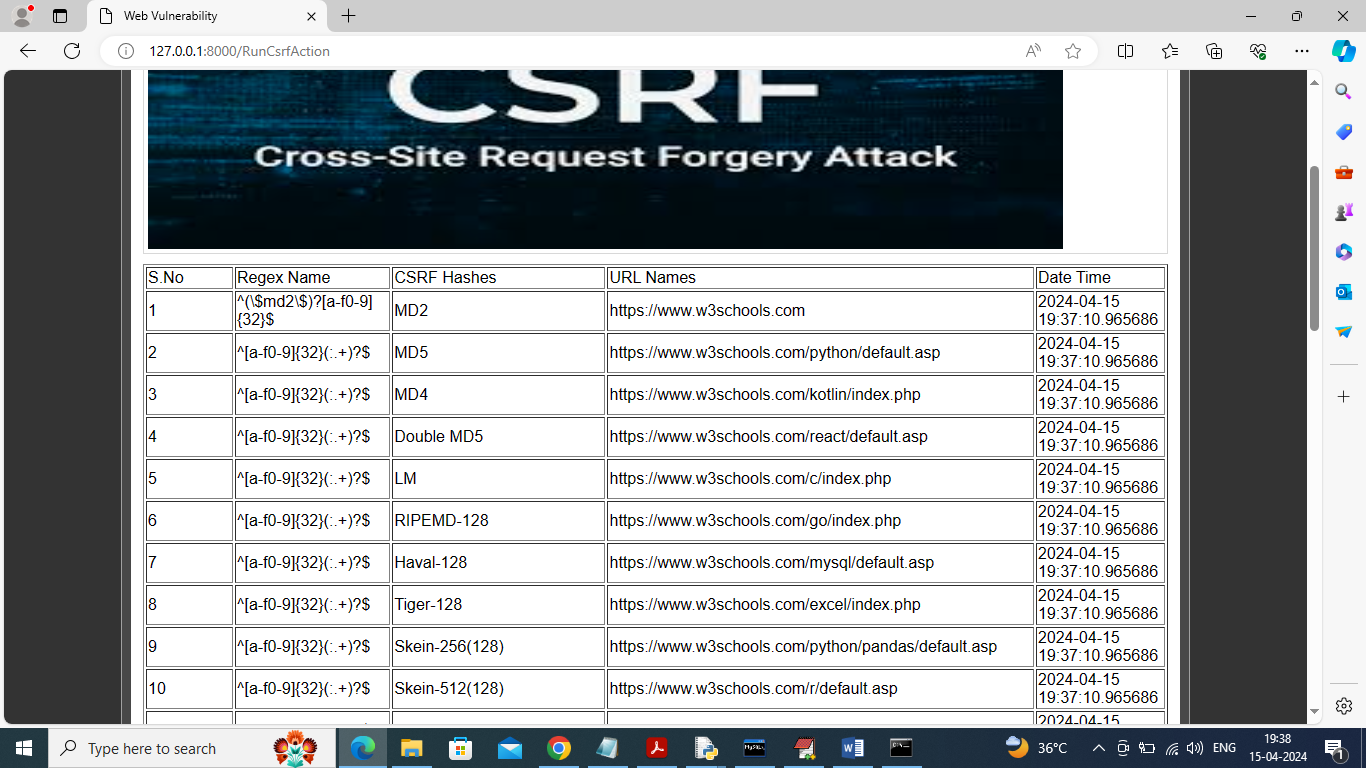
In above screen user can click on ‘Get CSRFS’ link to get below page



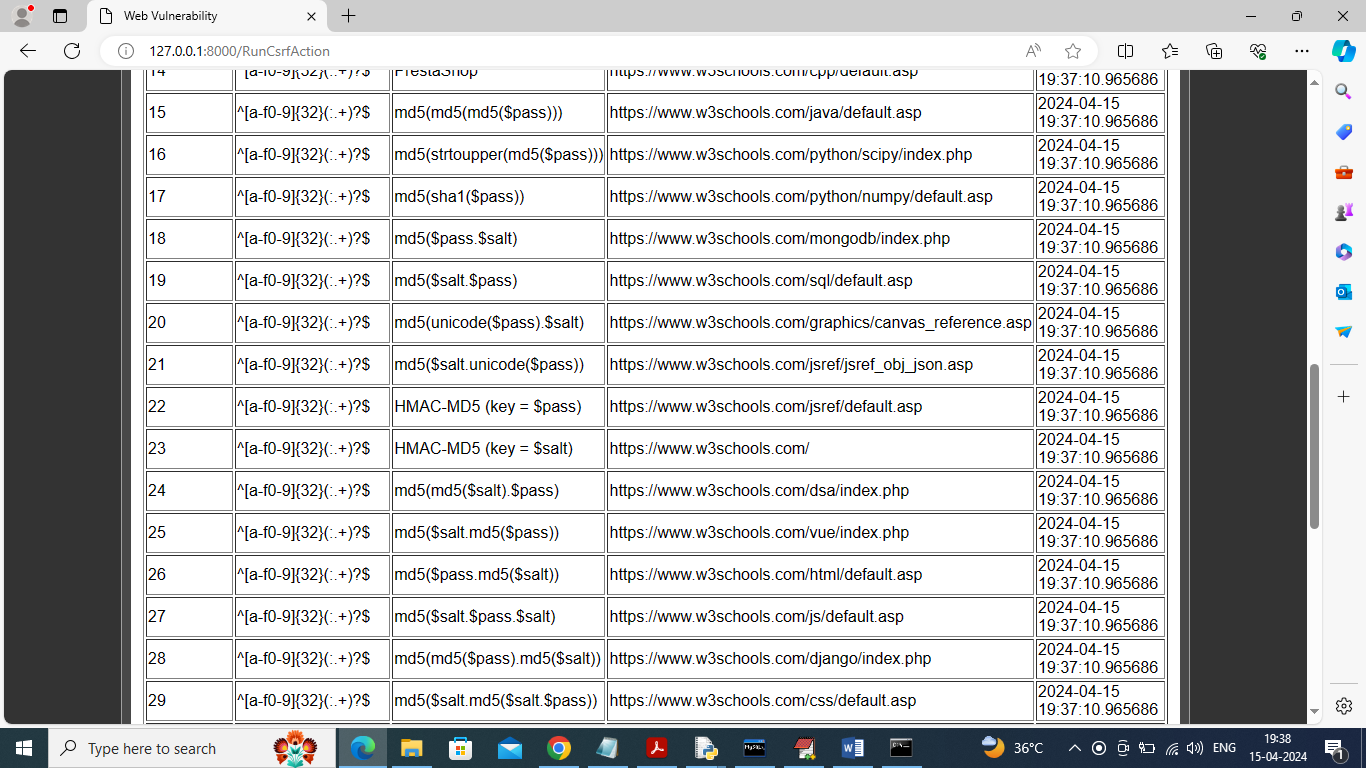
In above screen enter URL and depth value and then click on button to get below URL scanning output



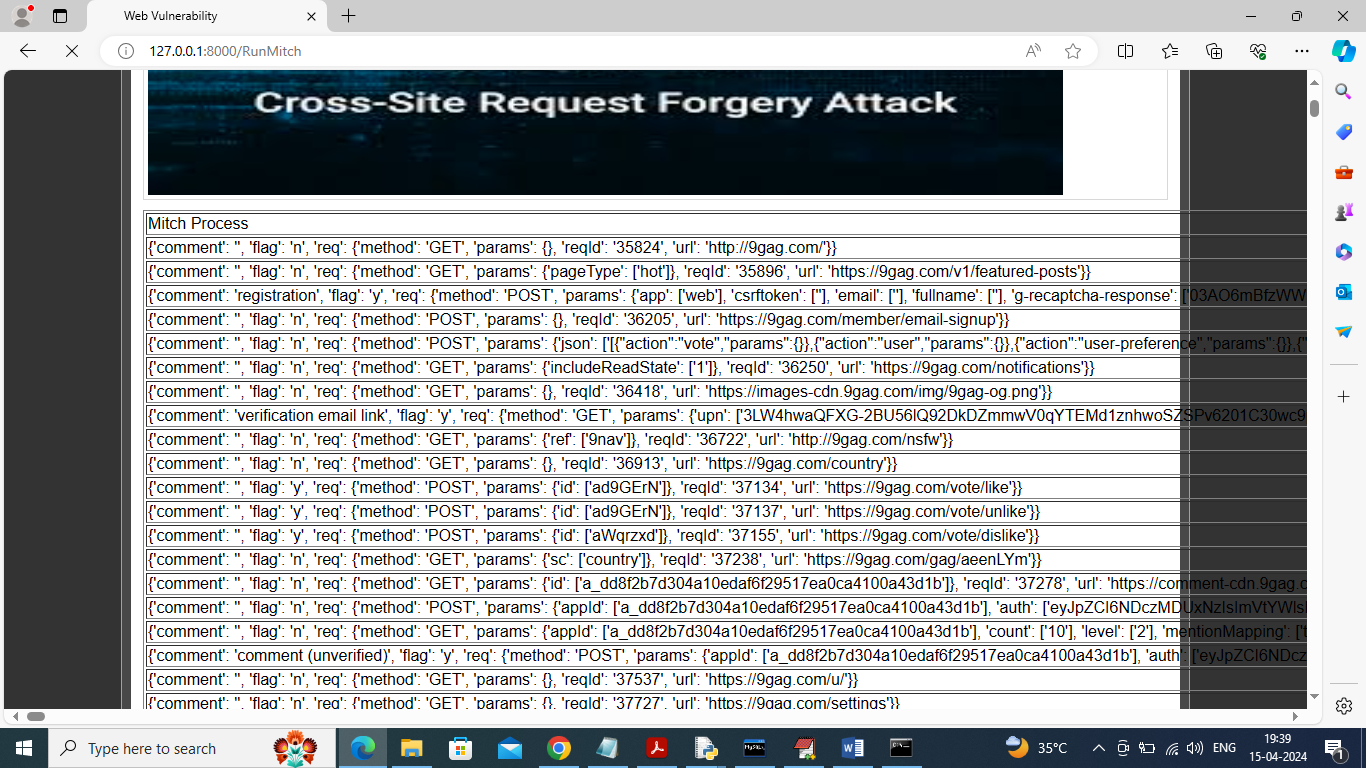
In above screen can see all scanned URL and then will get below page



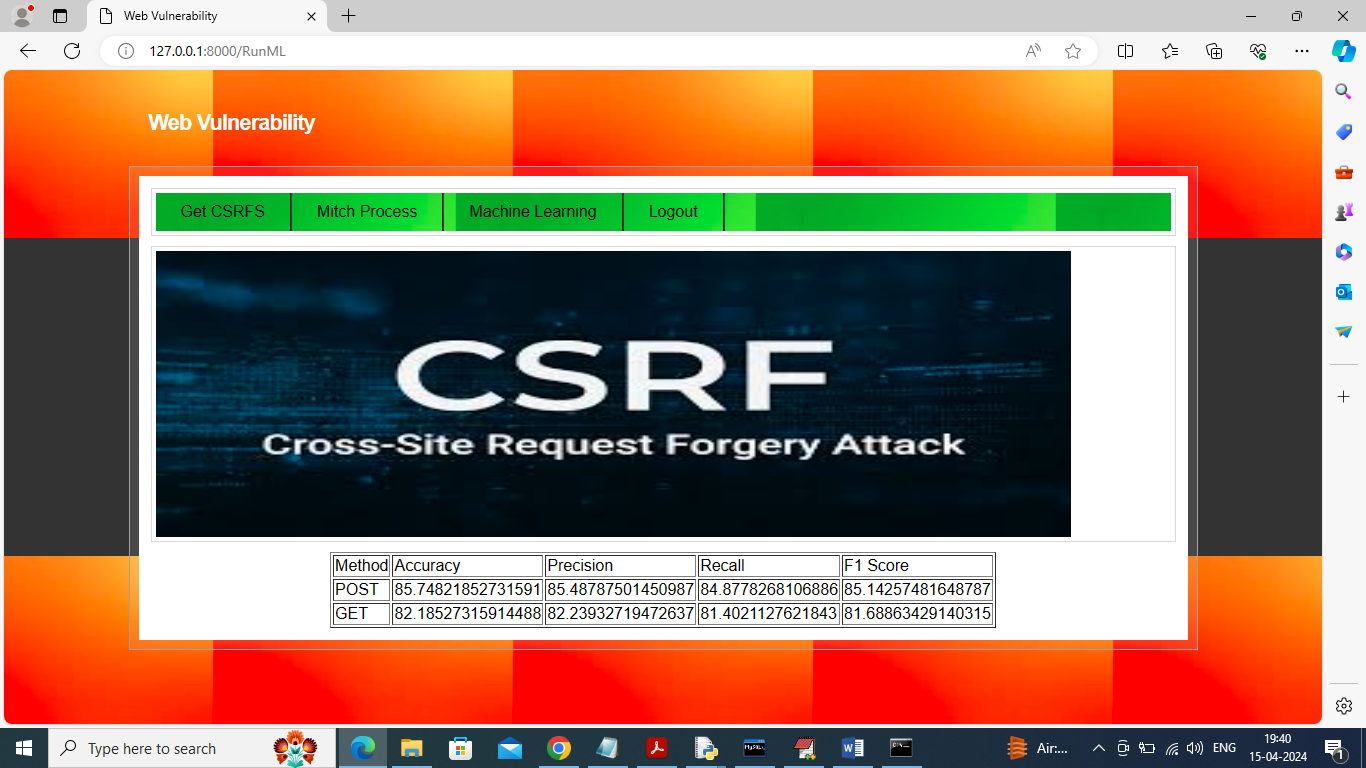
In above screen can see all CSRF list obtained from given URL and scroll down to view all details



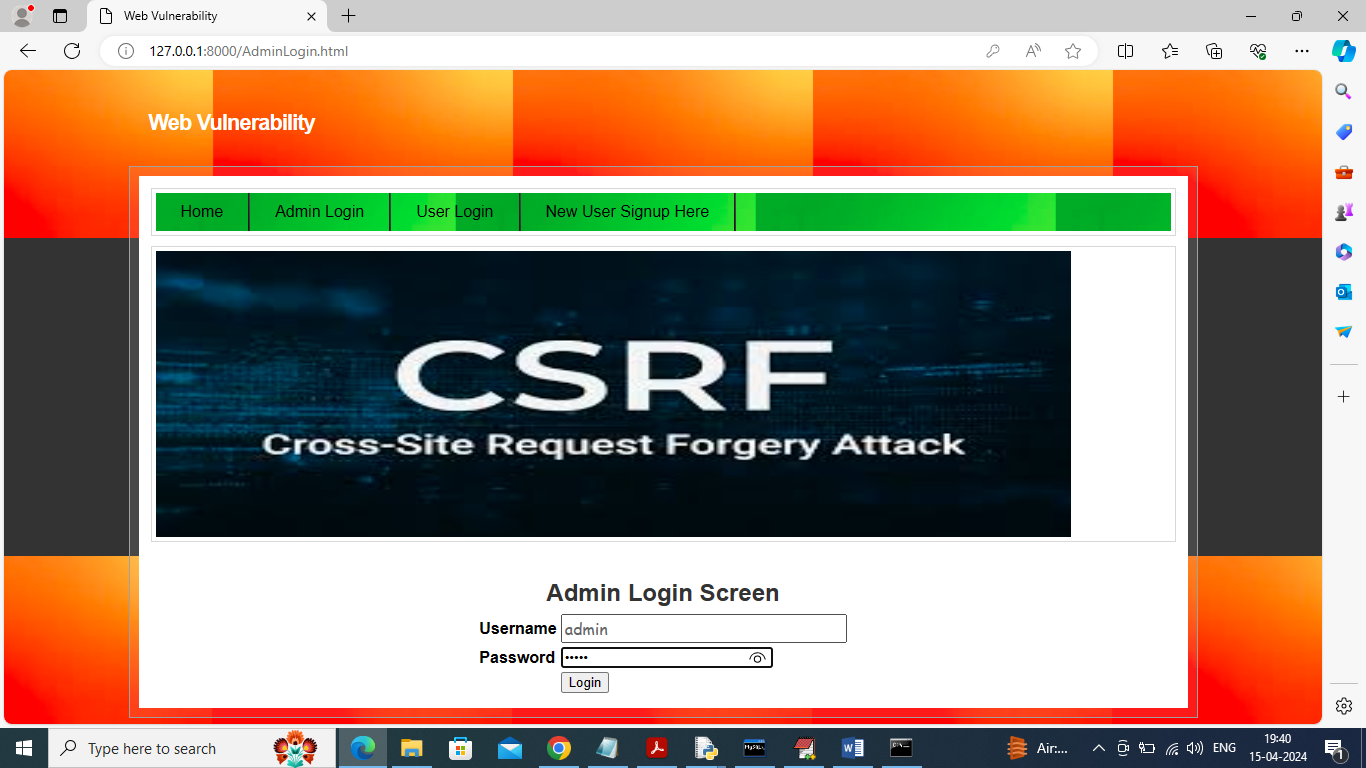
Now user can click on ‘Mitch Process’ link to run mitch and get below output



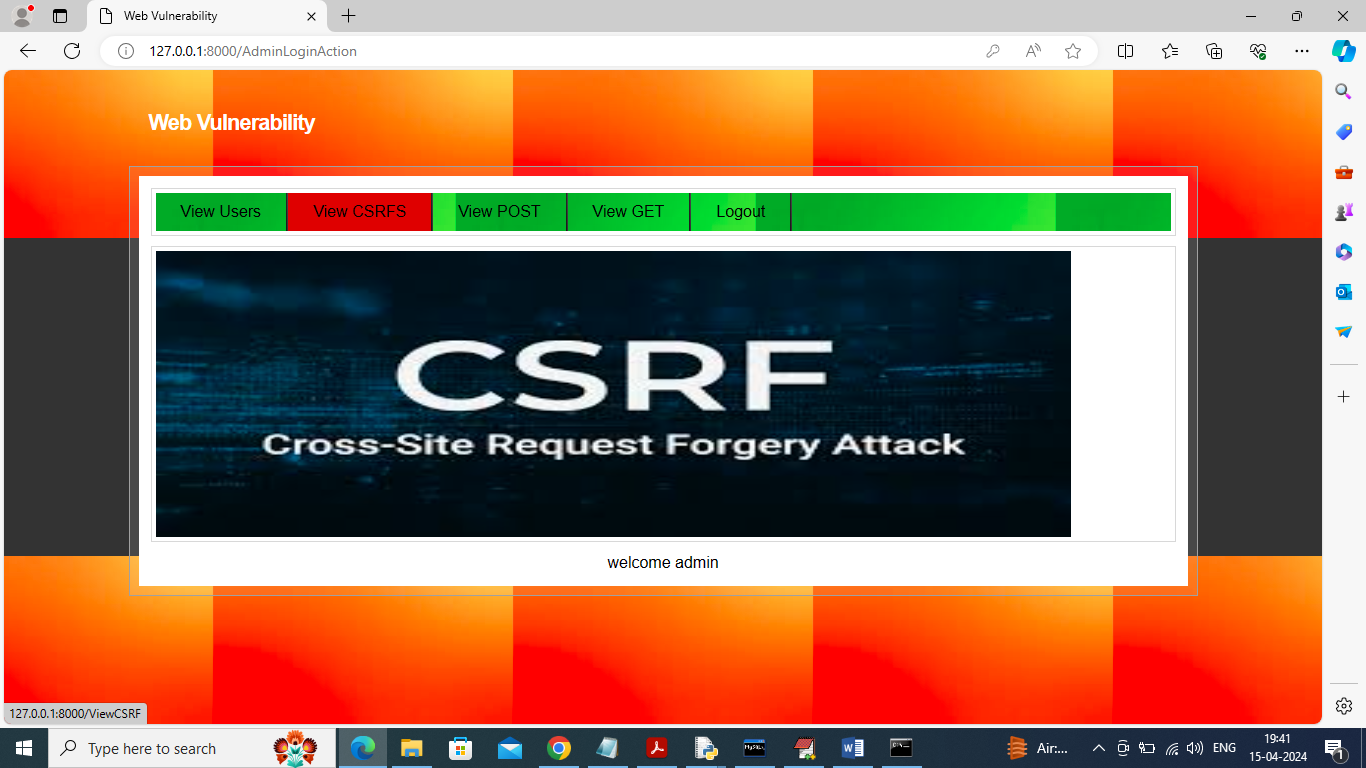
In above screen can see all MITCH process and now click on ‘Machine Learning’ link to train ML algorithm and get below output



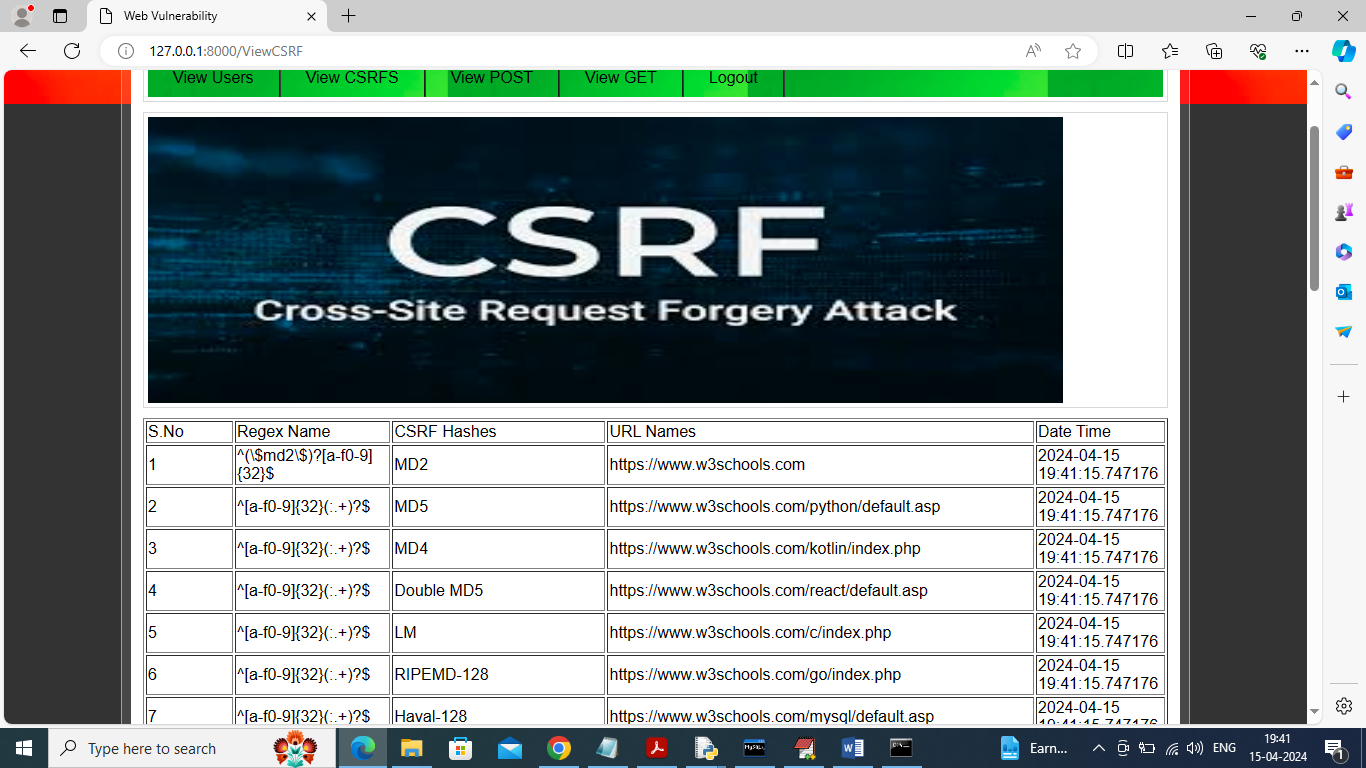
In above screen can see ML accuracy on both GET and POST methods and now logout and login as admin to view other process



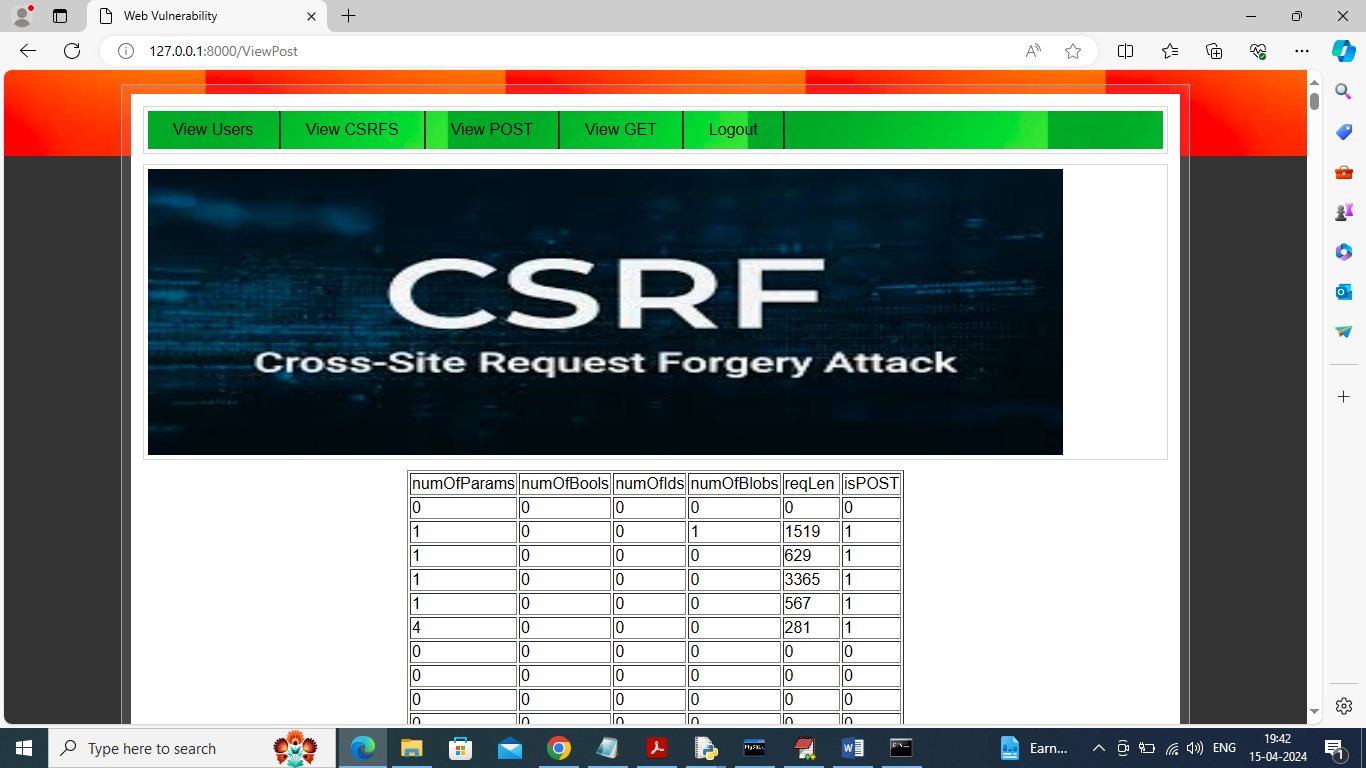
In above screen admin is login and after login will get below page



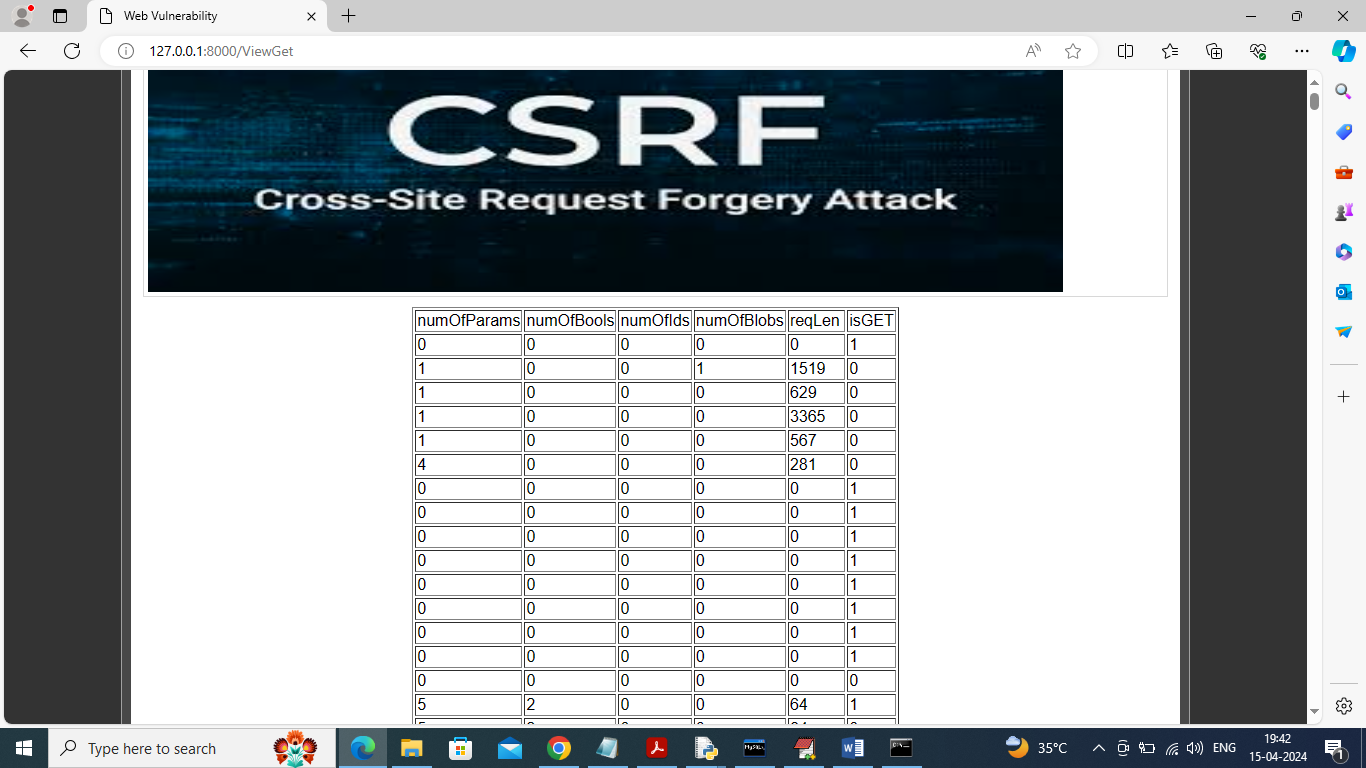
In above screen admin can click on ‘View CSRFS’ link to view all past CSRFS list and get below page



In above screen admin can view list of CSRF list and now click on ‘View Post’ link to view all post request



In above screen can see all POST request data and now click on ‘View Get’ link to get all get request data



In above screen can see list of all GET request and similarly by following above screens you can run all modules of the project