**Assignment 3 – Secure Session Management**

As per the requirements mentioned for Assignment 3, we have implemented the following:

Step 1 is accomplished using Django Web Framework.

Step 2, 3, & 4 are accomplished using Django User Authentication and session management.

Step 5 & 6 are accomplished using User RBAC and Django User Authentication.

1) For **User Authentication:** we are using Django API *"django.contrib.auth"* .

*user = authenticate(username=form.cleaned\_data['username'],* password=form.cleaned\_data['password'])

Also all the views require the user to login to the application. We implemented this using *"@login\_required"* decorated provided by django.

*@login\_required(login\_url='/accounts/login/')*

In case, the user is not logged in, the user is redirected to the login page.

2) We implemented **Authorization (Role Based Access Control)** for three types of users (ADMIN, Doctor and Patient).

where, patient can view only list of doctors.

doctors can view only list of patients.

Admin can view both list of doctors and patients.

We implemented this by fetching records from database based on the

- type or profile(role) of the logged in user (Admin/Patient/Doctor)

- type of the users stored in the database (Patient/Doctor)

3) We used **Session Management** for performing the following activities:

# set the universal user email

*request.session['user\_email']=curr\_user.email*

# set the universal user username

*request.session['user\_username']=username*

The username and email Id of the user are stored in session to be used on all the web application pages.

***\*\* Text marked in Red represent code snippets.***