**Authentication System Documentation**

**Overview**

This authentication system is designed to provide user registration, login, logout, and profile management functionalities for your Django project. It ensures security using Django’s built-in features like hashed passwords and CSRF protection.

**Features**

1. **User Registration**:
   * Allows new users to create accounts.
   * Validates data like username, email, and password.
2. **User Login**:
   * Authenticates users with valid credentials.
   * Redirects to the profile page after successful login.
3. **User Logout**:
   * Logs the user out and clears their session.
   * Redirects to the login page or homepage.
4. **Profile Management**:
   * Enables authenticated users to view and edit their profiles.
   * Supports updating fields like email, bio, and profile picture.

**Authentication Process**

**1. Registration**

* **URL**: /register/
* **View**: register\_view in views.py
* **Form**: UserRegisterForm (extends UserCreationForm to include an email field).
* **Template**: register.html
* **Flow**:
  + User submits the registration form.
  + Valid form data creates a new user.
  + On successful registration, the user is redirected to the login page.

**2. Login**

* **URL**: /login/
* **View**: Django’s built-in LoginView (django.contrib.auth.views.LoginView).
* **Template**: login.html
* **Flow**:
  + User submits the login form with their username and password.
  + Valid credentials log the user in and redirect them to /profile/.
  + If next is passed as a query parameter (e.g., /login/?next=/profile/), the user is redirected there after login.

**3. Logout**

* **URL**: /logout/
* **View**: Django’s built-in LogoutView (django.contrib.auth.views.LogoutView).
* **Template**: logout.html (optional confirmation page).
* **Flow**:
  + User clicks the logout button.
  + Session is cleared, and the user is redirected to the login page.

**4. Profile Management**

* **URL**: /profile/
* **View**: profile\_view in views.py
* **Form**: ProfileUpdateForm (custom form for updating user details).
* **Template**: profile.html
* **Flow**:
  + Authenticated user accesses /profile/.
  + The user can view their details and submit updates.
  + The system handles POST requests to update the user's email, bio, and profile picture.

**How Users Interact**

**Registration:**

1. Visit the registration page (/register/).
2. Fill in the form with:
   * Username
   * Email
   * Password (confirmed twice)
3. Click "Register."
4. If successful, they are redirected to the login page.

**Login:**

1. Visit the login page (/login/).
2. Enter their username and password.
3. Click "Login."
4. They are redirected to /profile/ or the page they were trying to access.

**Logout:**

1. Click the logout button or visit /logout/.
2. Session is cleared, and they are redirected to the login page.

**Profile Management:**

1. Log in and visit /profile/.
2. Edit fields like email, bio, and profile picture.
3. Submit the changes.
4. Updates are reflected in their profile.

**Instructions for Testing**

**1. Test Registration**

* Navigate to /register/.
* Submit the form with valid data.
* Confirm the user is created in the database.
* Test invalid data (e.g., missing fields, short password) to ensure validation errors are displayed.

**2. Test Login**

* Navigate to /login/.
* Log in with valid credentials and confirm redirection to /profile/.
* Test invalid credentials to ensure proper error messages are shown.
* Test the next parameter by trying to access a protected page directly (e.g., /profile/).

**3. Test Logout**

* Log in and then visit /logout/.
* Confirm the session is cleared by attempting to access /profile/.

**4. Test Profile Management**

* Log in and navigate to /profile/.
* Update fields like email or bio and submit.
* Confirm changes are reflected in the database.
* Test invalid inputs (e.g., unsupported file format for profile picture).

**Security Features**

1. **CSRF Protection**:
   * All forms include {% csrf\_token %} to prevent CSRF attacks.
   * Verified using Django’s middleware.
2. **Password Security**:
   * Passwords are hashed using Django’s built-in hashing algorithms.
   * Strong password requirements are enforced with AUTH\_PASSWORD\_VALIDATORS.
3. **Session Security**:
   * Session data is cleared on logout.
   * Use SESSION\_COOKIE\_SECURE and CSRF\_COOKIE\_SECURE in production to enforce secure cookies.
4. **Brute-Force Protection**:
   * Integrate third-party tools like django-axes to limit login attempts (optional).

**Code Overview**

**Views**

* **register\_view**: Handles user registration and redirects to the login page on success.
* **profile\_view**: Displays and updates user profile information.

**Forms**

* **UserRegisterForm**: Extends UserCreationForm to include an email field.
* **ProfileUpdateForm**: Custom form for updating profile fields like email and bio.

**Templates**

* register.html, login.html, logout.html, and profile.html provide user interfaces for authentication functionalities.

**URL Patterns**

Defined in urls.py:

python

Copy code

urlpatterns = [

path('register/', register\_view, name='register'),

path('login/', LoginView.as\_view(), name='login'),

path('logout/', LogoutView.as\_view(), name='logout'),

path('profile/', profile\_view, name='profile'),

]

## Comment System

### Features:

- Users can view all comments on a blog post.

- Authenticated users can:

- Add a new comment to any post.

- Edit their own comments.

- Delete their own comments.

### Permissions:

- Only the author of a comment can edit or delete it.

- Anyone can view comments on a post.

### URL Patterns:

- `/post/<int:pk>/`: View and add comments to a post.

- `/comment/<int:pk>/edit/`: Edit a comment.

- `/comment/<int:pk>/delete/`: Delete a comment.