Professional Django OTP Integration Guide

Professional Step-by-Step Guide for Django OTP Integration

1. **Install and Configure Django**:
   - A virtual environment was created to ensure package dependencies are managed separately.
   - Django was installed using `pip install django`, and a new project was initiated with `django-admin startproject mysite`.
   - Basic configurations were set in `settings.py` including setting up the database and static files.

2. **Django OTP Integration**:
   - Two-factor authentication was added to the project by installing `django-otp` (`pip install django-otp`).
   - In `settings.py`, `django_otp` and `django_otp.plugins.otp_totp` were included in the `INSTALLED_APPS` section to enable Time-based One-Time Password (TOTP) functionality.

3. **Configuring URLs for OTP**:
   - The Django admin interface was secured by overriding the default admin site with `OTPAdminSite` from `django_otp.admin`. This ensures that all logins to the admin panel require an OTP token in addition to the username and password.
   - `urls.py` was updated to reflect the new OTP-secured admin site.

4. **Database Migrations**:
   - Migrations were applied using `python manage.py migrate` to ensure all required database tables were created.
   - This step ensured that all configurations, including OTP, were properly integrated into the database.

5. **Create a Superuser**:

- A superuser was created using `python manage.py createsuperuser`. This superuser account is necessary to access the Django admin panel.

- After setting up the superuser, access to the admin panel was secured with two-factor authentication (username/password and OTP).

6. **Setting Up OTP Devices**:

- After accessing the admin panel, the superuser was prompted to set up an OTP device, such as Google Authenticator or Authy.

- A QR code was generated for the OTP device, which is then used to scan and register the OTP token generator.

- The admin panel now requires an OTP from the configured device in addition to the username and password for login.

7. **Final Verification**:

- The system was thoroughly tested to ensure that OTP is functioning as intended. Each login attempt to the admin panel now requires an OTP token, confirming that two-factor authentication is successfully integrated.
