Coding Task

This document contains the following topics:

1. How to set up API
2. How to use API
3. Approach used
4. Future scope

The requirement to use and test:

1. SQL Database
2. Python 3.x
3. Postman or any other similar tool

How to set up API

1. Extract the code and put it into a directory
2. In the root directory, execute “pip install -r requirements.txt”
3. In config.py, edit connection string for your database
4. In the root directory, execute “python setup.py” - To set up your database and sample data
5. In the root directory, “python app.py” - To run your API
6. Import Postman collection from postman collection folder for testing

How to use API

1. API has the following endpoints:
    a. api/v1/users/login - public endpoint - POST
        i. Takes the following parameters and generate JWT token for authentication

```
{
        "phone_number" : "number",
        "password": "password"
}
```

    b. api/v1/users/add - public endpoint - POST
        i. Takes the following parameters and creates a new user

```
{
        "name":"name",
        "phone_number": "number",
        "email": "email or empty string",
        "password": "password"
}
```

    c. api/v1/users/search/<search string> - secured endpoint - GET
        i. Takes <search string> as input param and returns user/ user list based on name and phone_number.
        ii. If exact name/phone number is found then similar will not be returned
        iii. If exact name/phone number is not found then similar will be returned as mentioned in task document
    d. api/v1/spams/add - secured endpoint - POST
        i. This will take the following parameters and register new spam

```
{
        "number" : "9896744563"
}
```

        ii. One user can report a number one time only
    e. api/v1/admin/sync - secured endpoint - GET
        i. This is only accessible to app admin. This is run update spam likelihood function manually. It not executed, this will run once every 24 hours

Secured endpoints are only accessible with JWT token issued by API. You need to pass it in the header of each request

Login credentials:

1. **Admin**
    a. Phone_number: 00000000
    b. Password: password
2. **User**
    a. Phone_number: 9896744563
    b. Password: password

Approach Used

1. The API is divided into 3 main layers
    a. Endpoints or controller
        i. This layer exposed endpoints to users
    b. Service layer
        i. This layer interacts with controllers and data access layer to perform required actions
    c. Data Access layer
        i. This layer contains the data definition and allows the service layer to perform operations on the database
2. Authentication: JWT Token is used as the authentication scheme
3. Authorization: JWT token is used as an authorization scheme
4. Scheduler: A scheduler is created which will execute specified actions at a specified period of time
5. A number is a spam or not is determined by the spam_likelihood variable which ranges from 0 to 100. The more the value of spam_likelihood, the more are the chances a number is a spam caller.

Future scope

1. A Logger service can be added for easy debugging on the production server