Screenshots of Project Operations

Initial admin credentials are inserted directly to the User and Role repositories on startup: username **- "admin",** password **- "admin",** role **- "ADMIN"**.

New roles and users can be added only by ADMIN users. This provides a security layer that prevents non-ADMIN users from assigning the role ADMIN to any new user.

1. Application is able to add roles dynamically in the database. Here "**name**" specifies a role which can be assigned to a user that will be used for authentication purposes while interacting with the API.
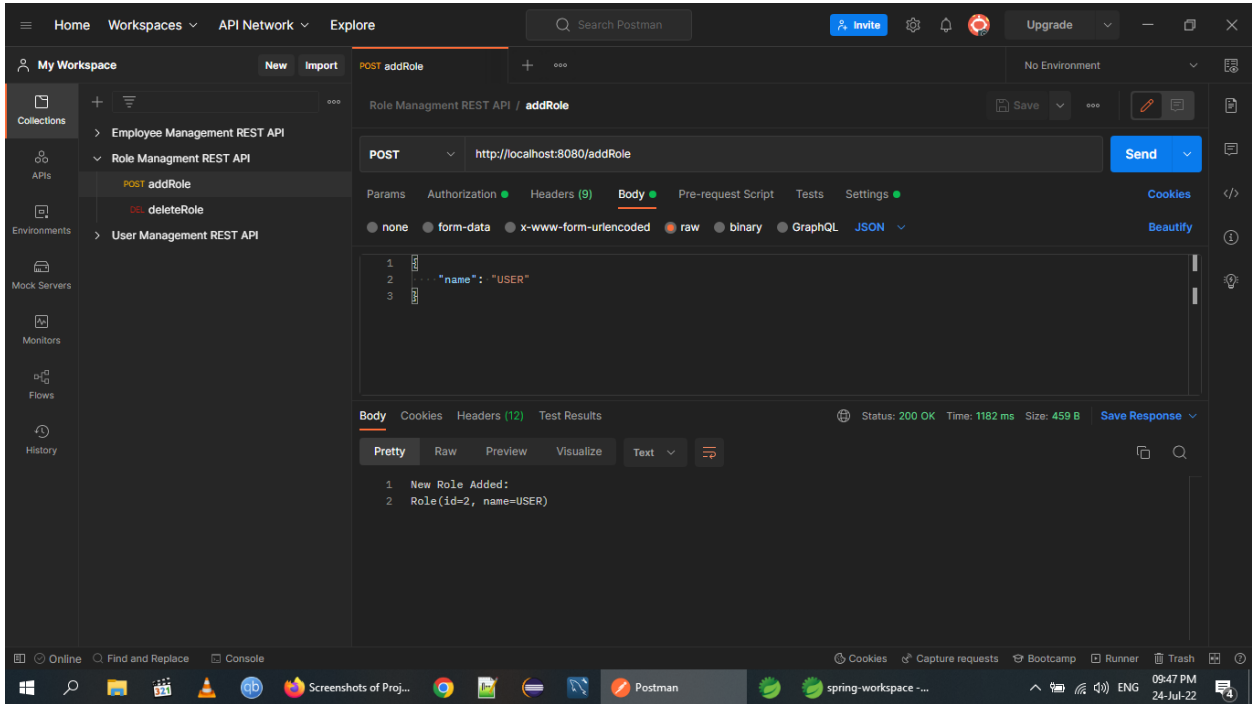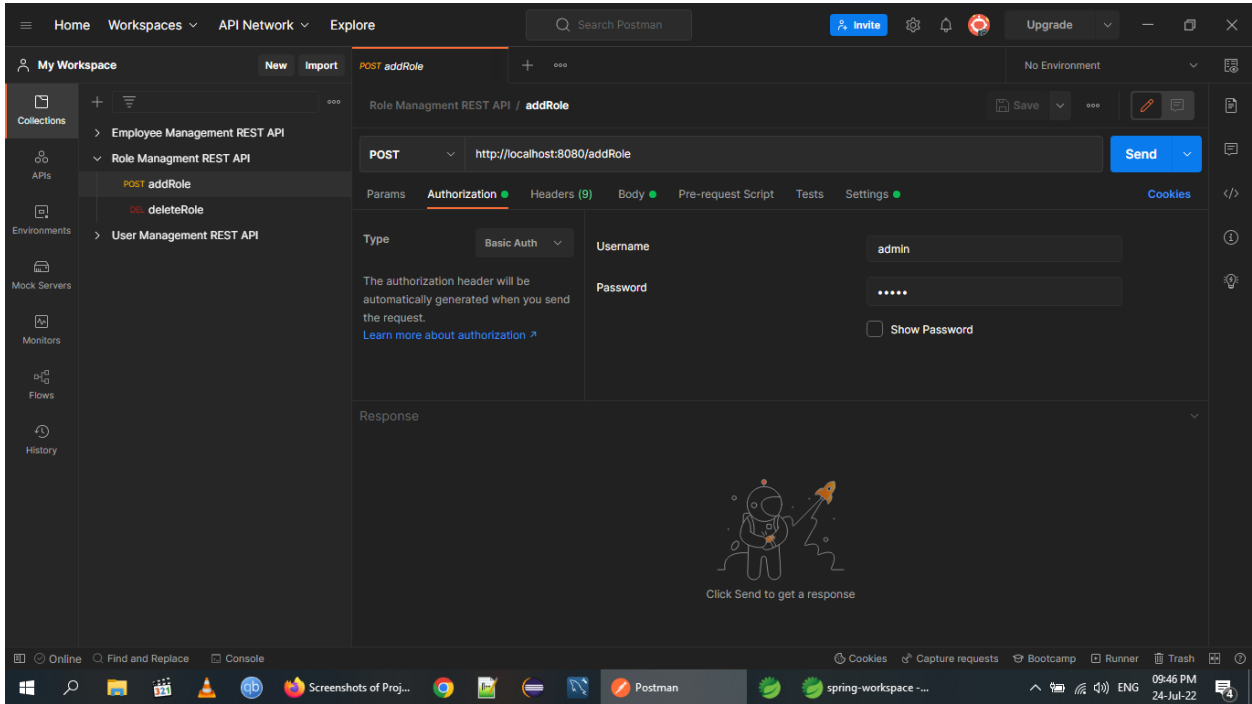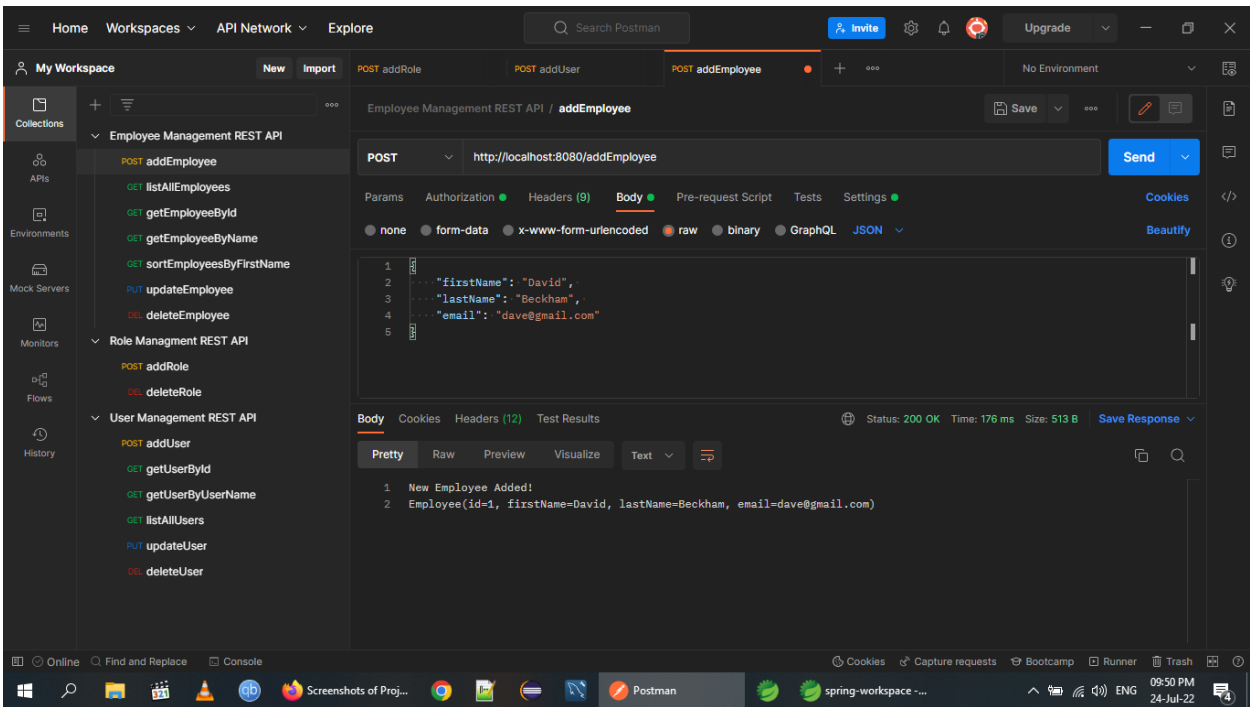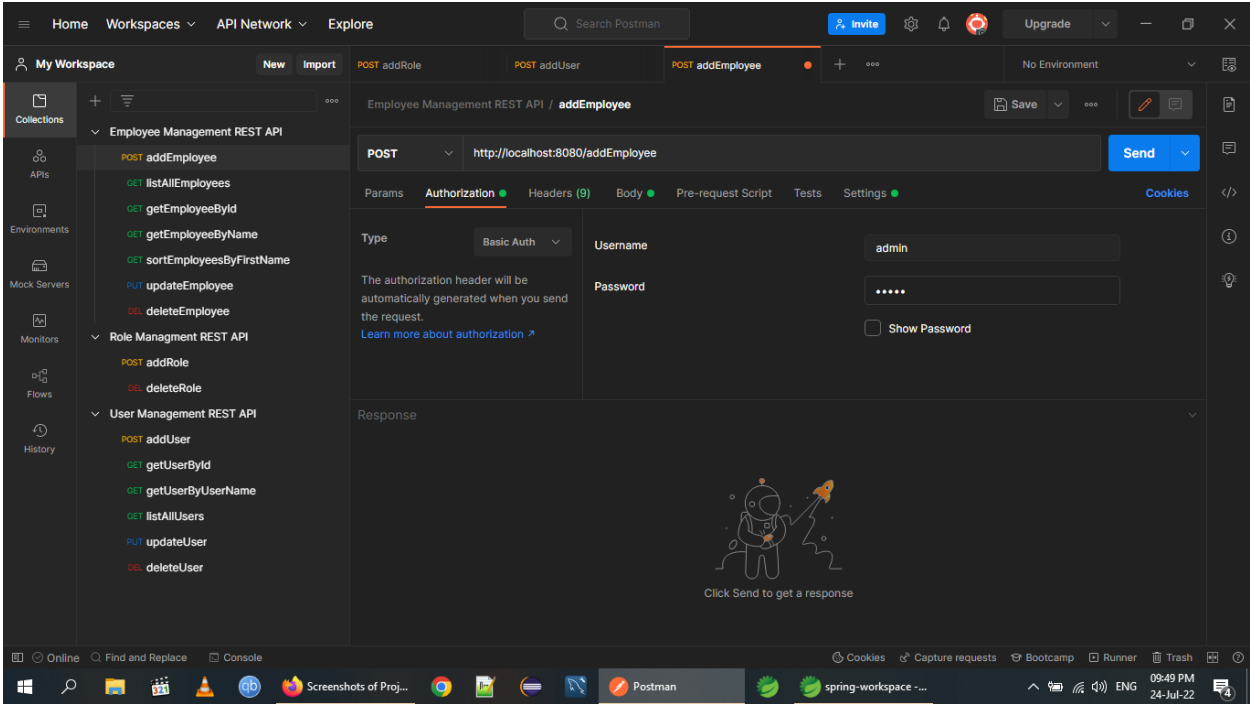
2. Application is able to add Users in the database which can be used for authentication purposes.
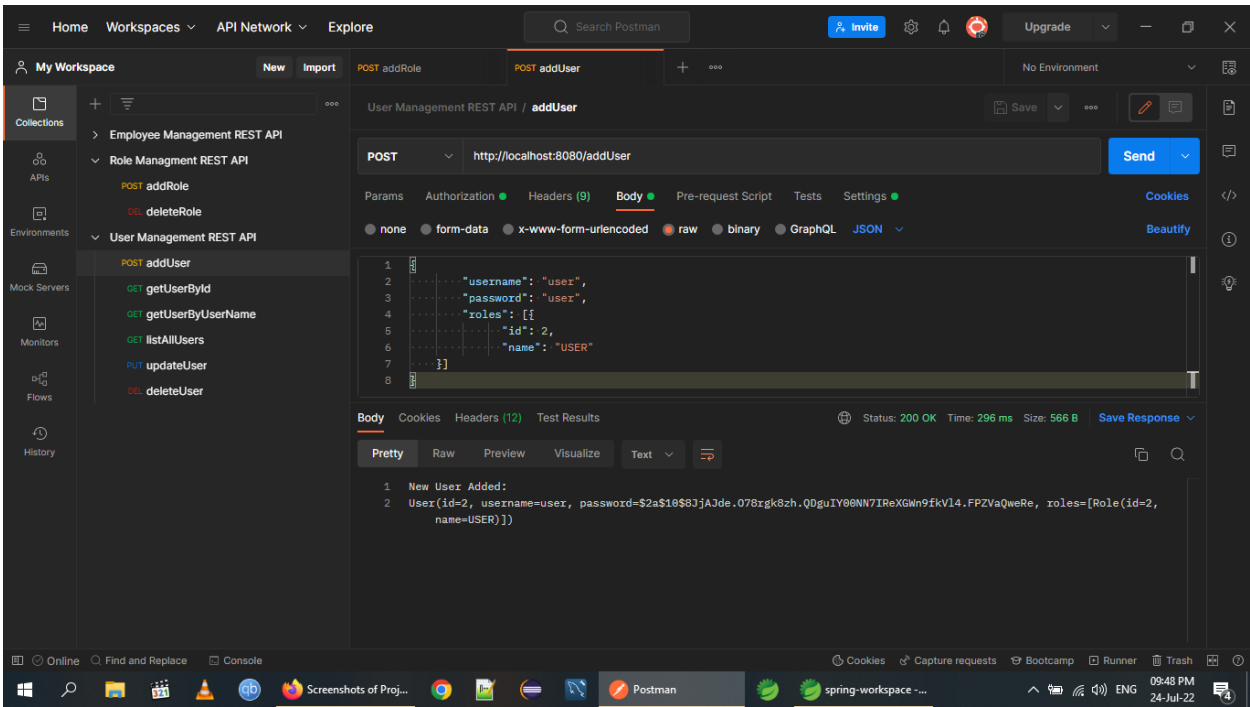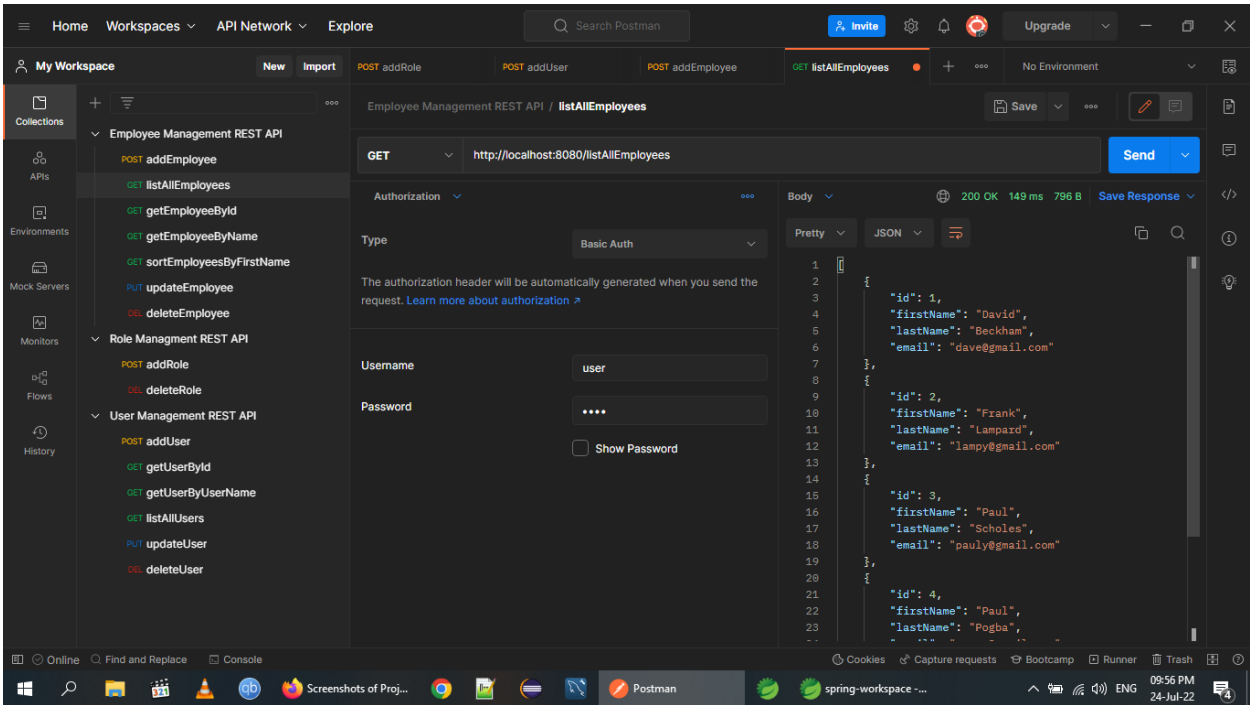

3. Application shows **Error: 403: Forbidden** when **non-ADMIN** user tries to add an employee.
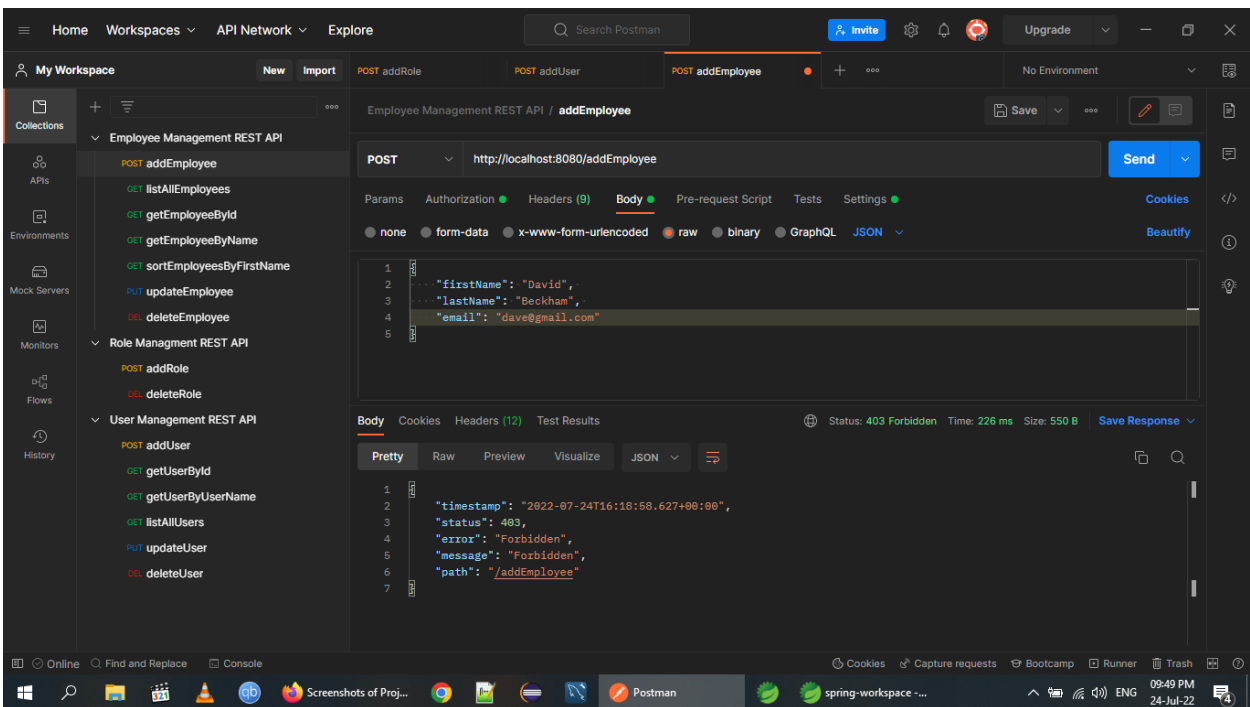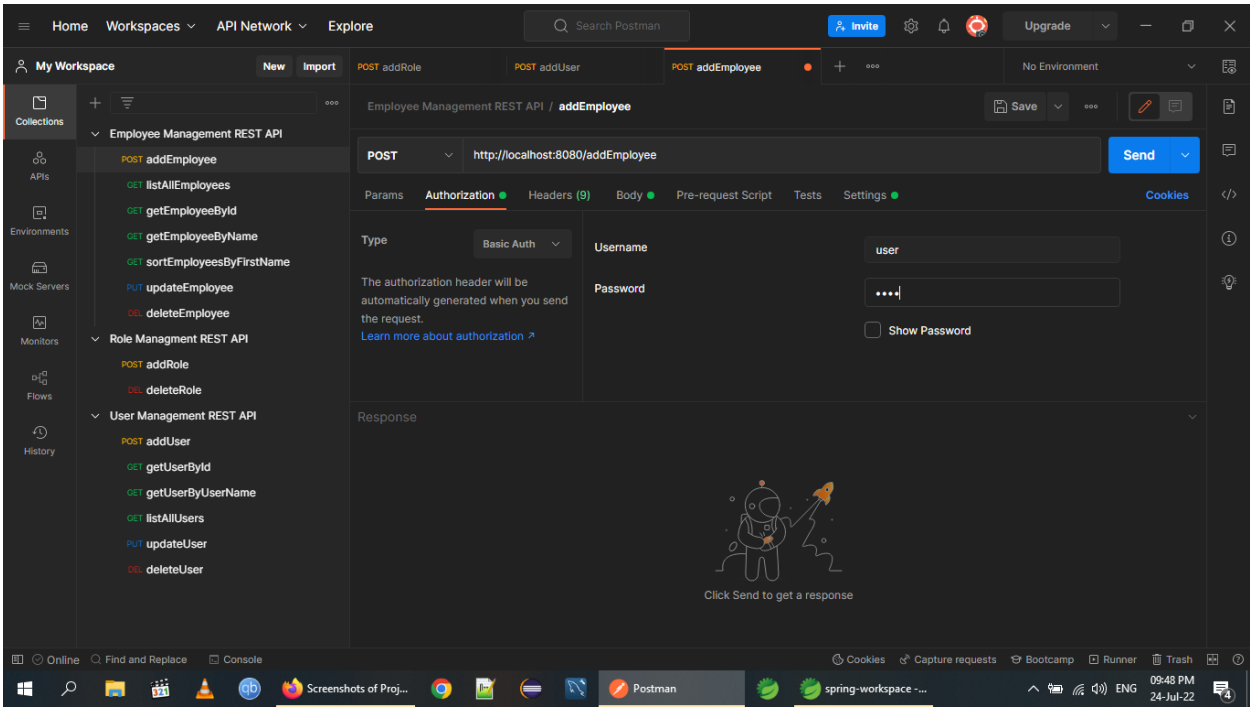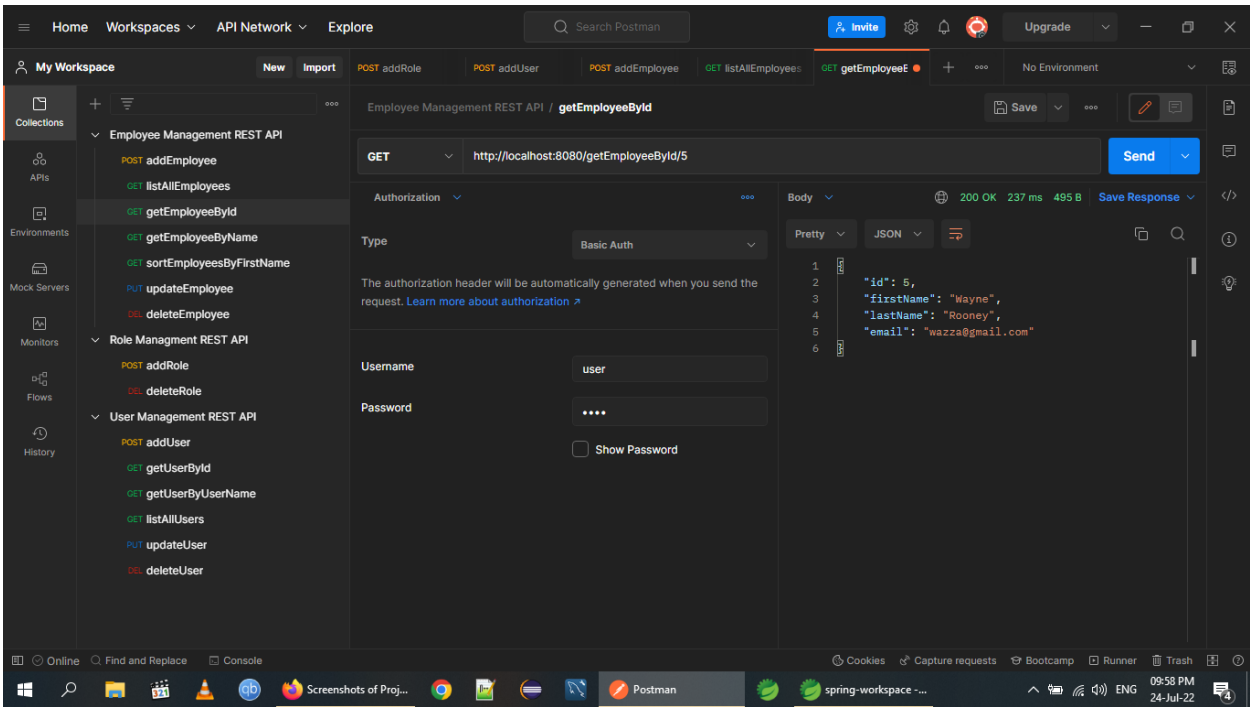
4. Application is able to add employees data in the database if and only if the authenticated user is **ADMIN**.
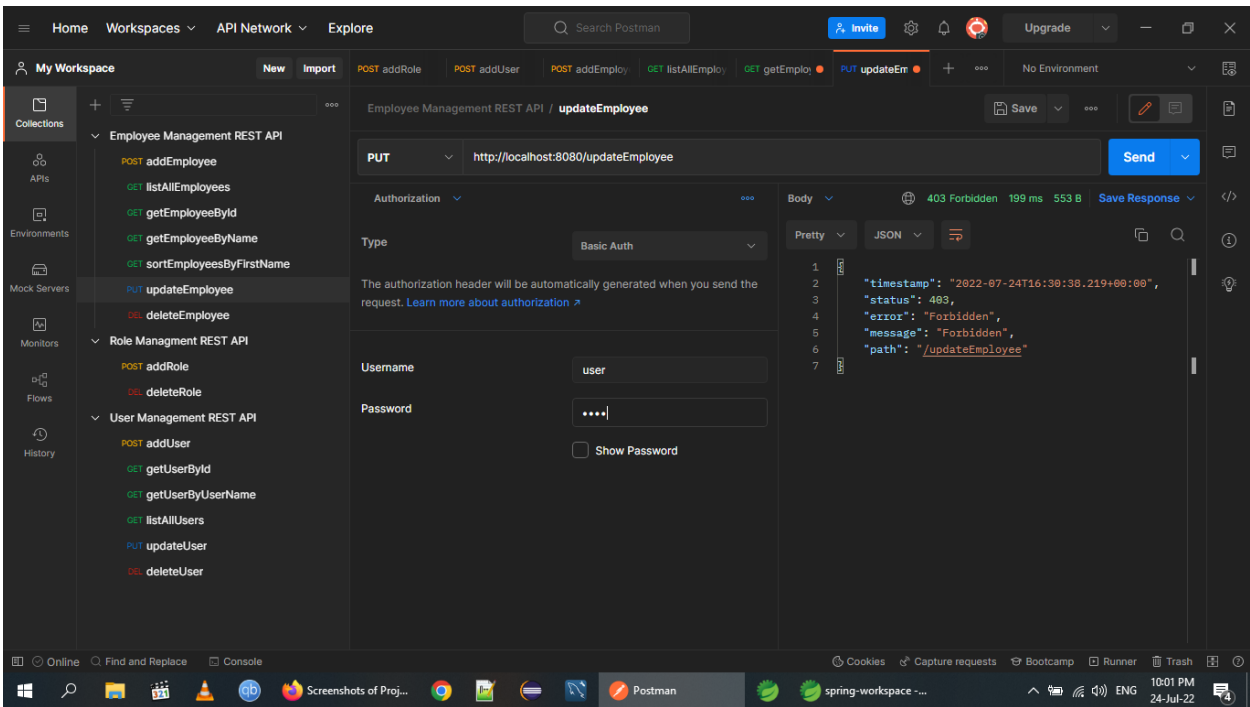

5. Application provides an endpoint to list all the employees stored in the database.
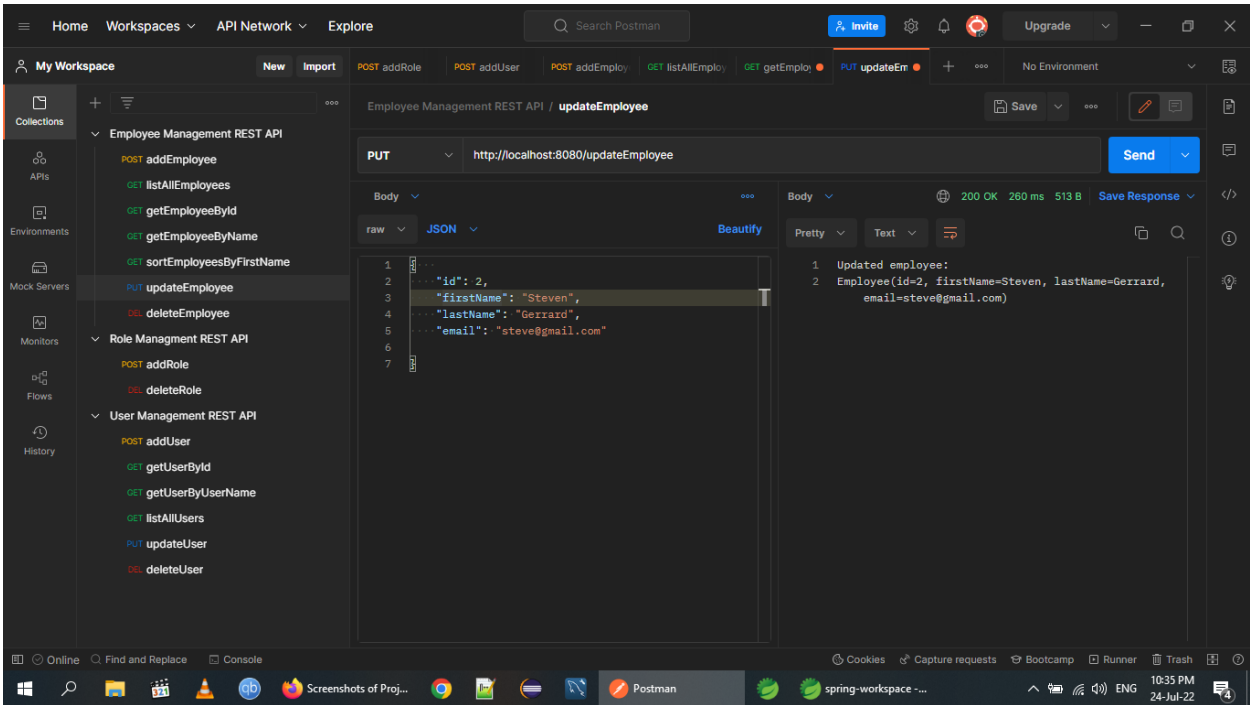
6. Application provides an endpoint to fetch an employee record specifically based on the ID of that employee.
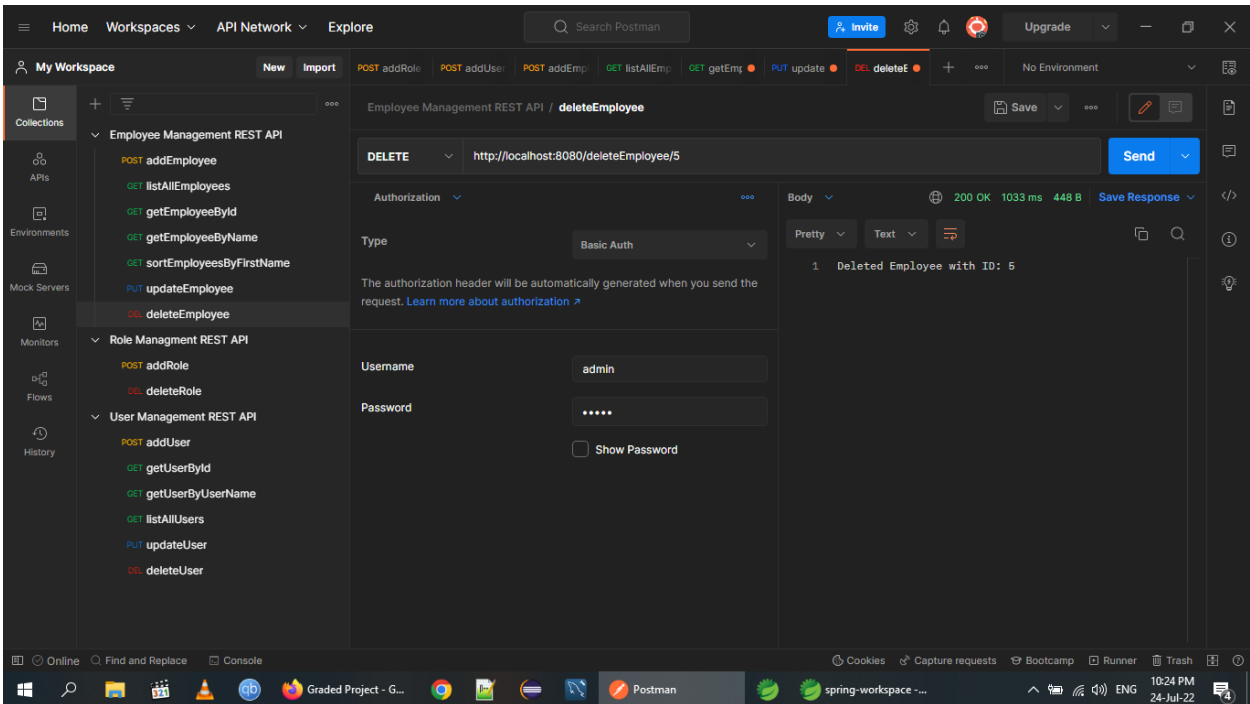

7. Application provides an endpoint to update an existing employee record with the given updated json object. Update privilege not granted to **non-ADMIN** users.
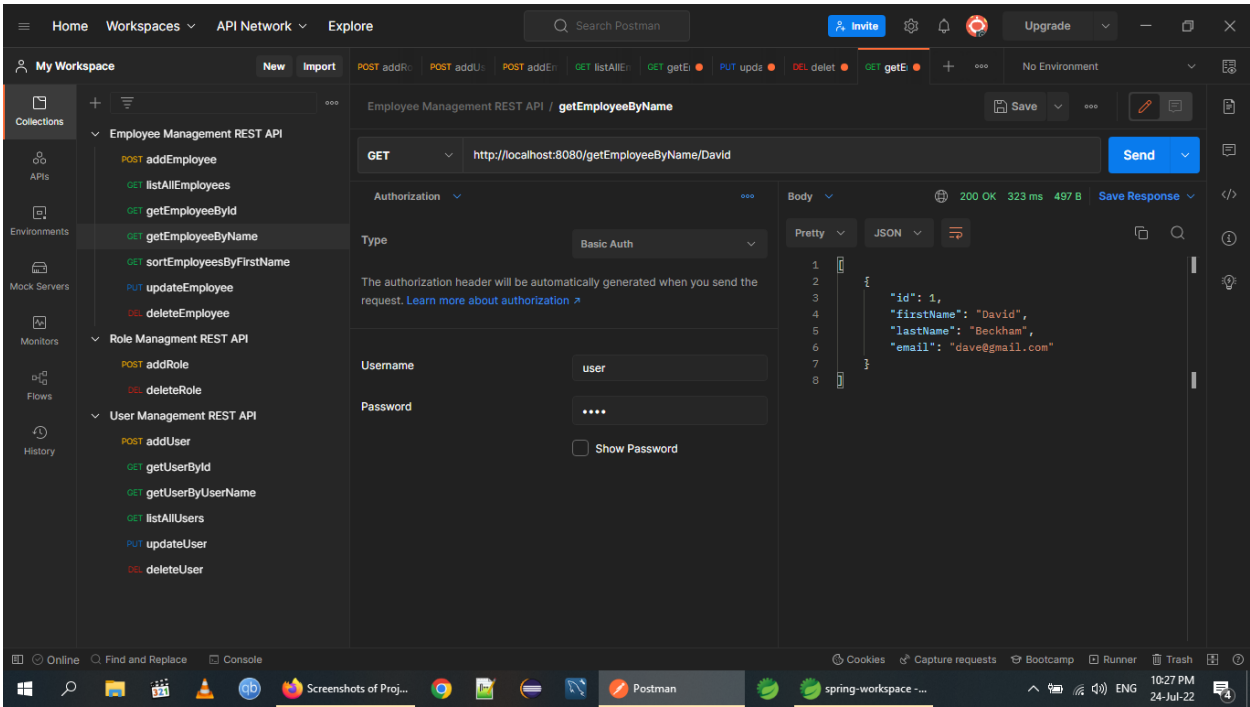
8. Only **ADMIN** users can perform updates to employees' records.

9. Application provides an endpoint to delete an existing employee record based on the ID of the employee. Only **ADMIN** users are privileged to perform Delete operations.

10. Application provides an endpoint to fetch an employee by their first name.
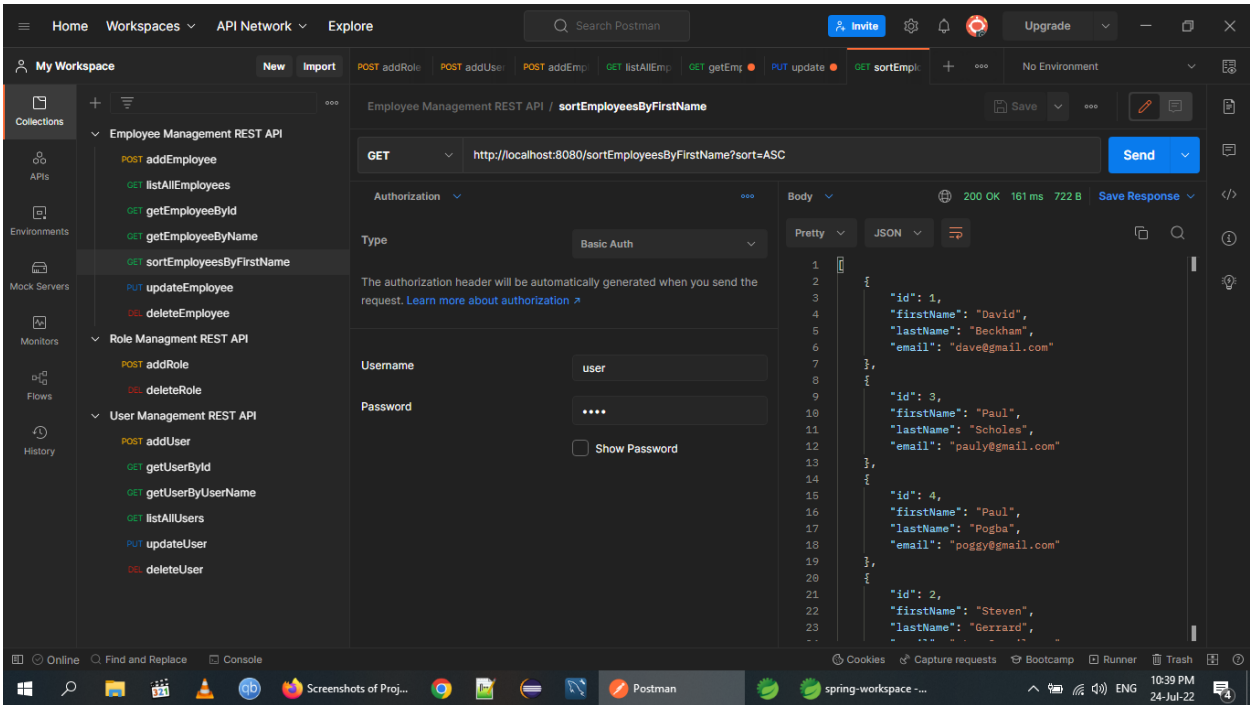

11. When more than one record is found with the same first name, the application lists them all.
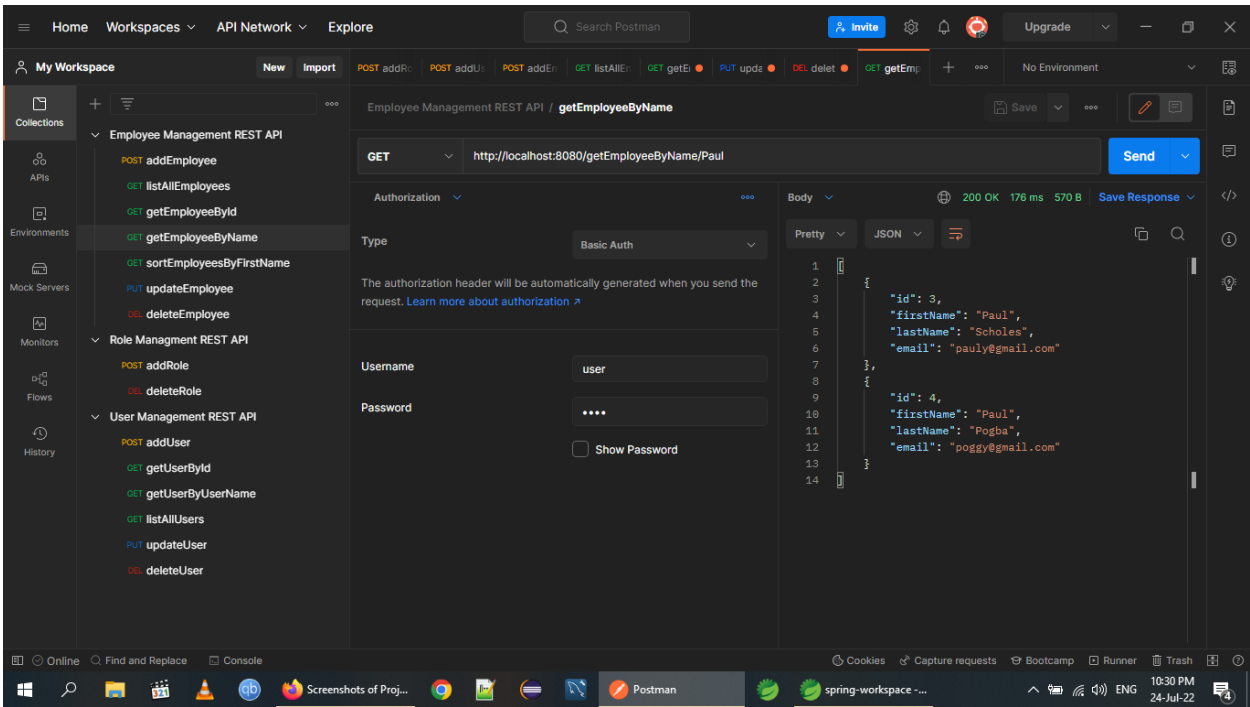
12. Application is able to list all employee records sorted on the basis of their first name.

    a.   In Ascending order

    b.   In Descending order

****