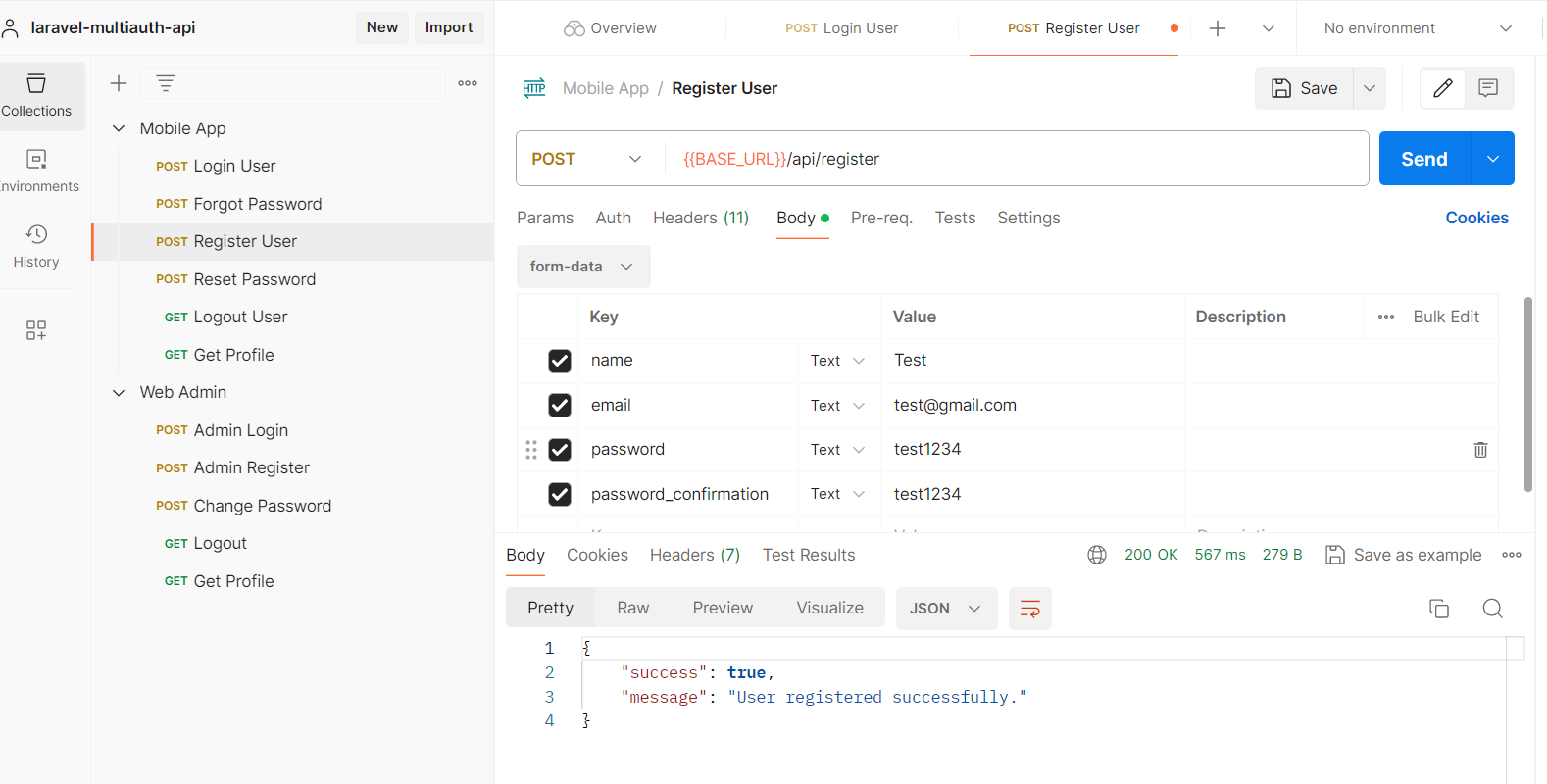
**API Document**

We have implemented multi auth (Web Admin and App users) token-based authentication (using Laravel Sanctum). So, to start with accessing user APIs, first we need to register user using “Register User” API, then we need to get the access token using “Login User” API with same credentials of registered user.

**API - Register User:**



**API Endpoint**: <http://localhost:8000/api/register>

**Method**: POST

**Headers**:

Accept: application/vnd.api+json

Content-Type: application/vnd.api+json

**Body Form Data:**

name: "Test"

email: "test@gmail.com"

password: "test1234"

password\_confirmation: "test1234"

**Response**:

{

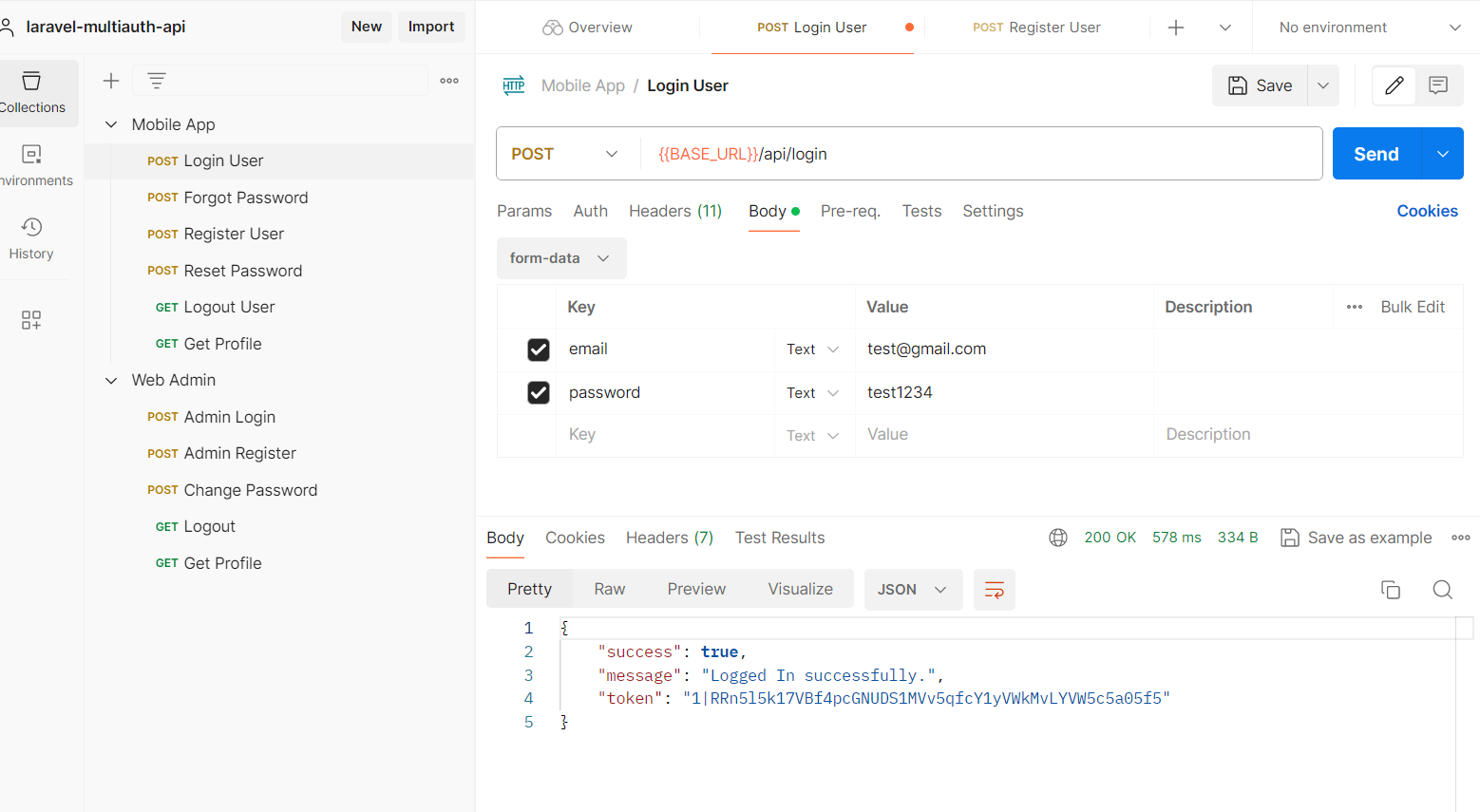
    "success": **true**,

    "message": "User registered successfully."

}

Once user get registered, we should use login API to get access token.

**API - Login User:**



**API Endpoint**: <http://localhost:8000/api/login>

**Method**: POST

**Headers**:

Accept: application/vnd.api+json

Content-Type: application/vnd.api+json

**Body Form Data:**

email: "test@gmail.com"

password: "test1234"

**Response**:

{

    "success": **true**,

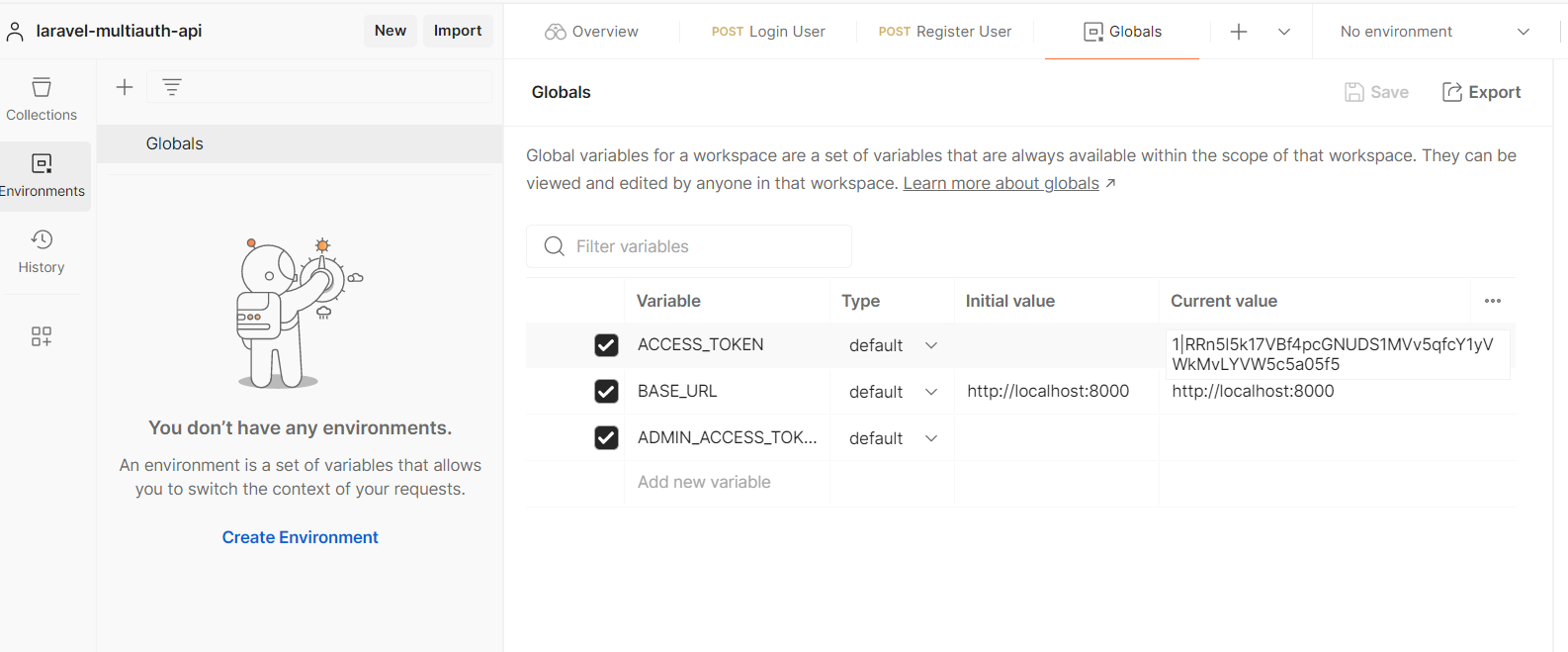
    "message": "Logged In successfully.",

    "token": " 1|RRn5l5k17VBf4pcGNUDS1MVv5qfcY1yVWkMvLYVW5c5a05f5"

}

We need to use this yellow highlighted token to access other API endpoints.

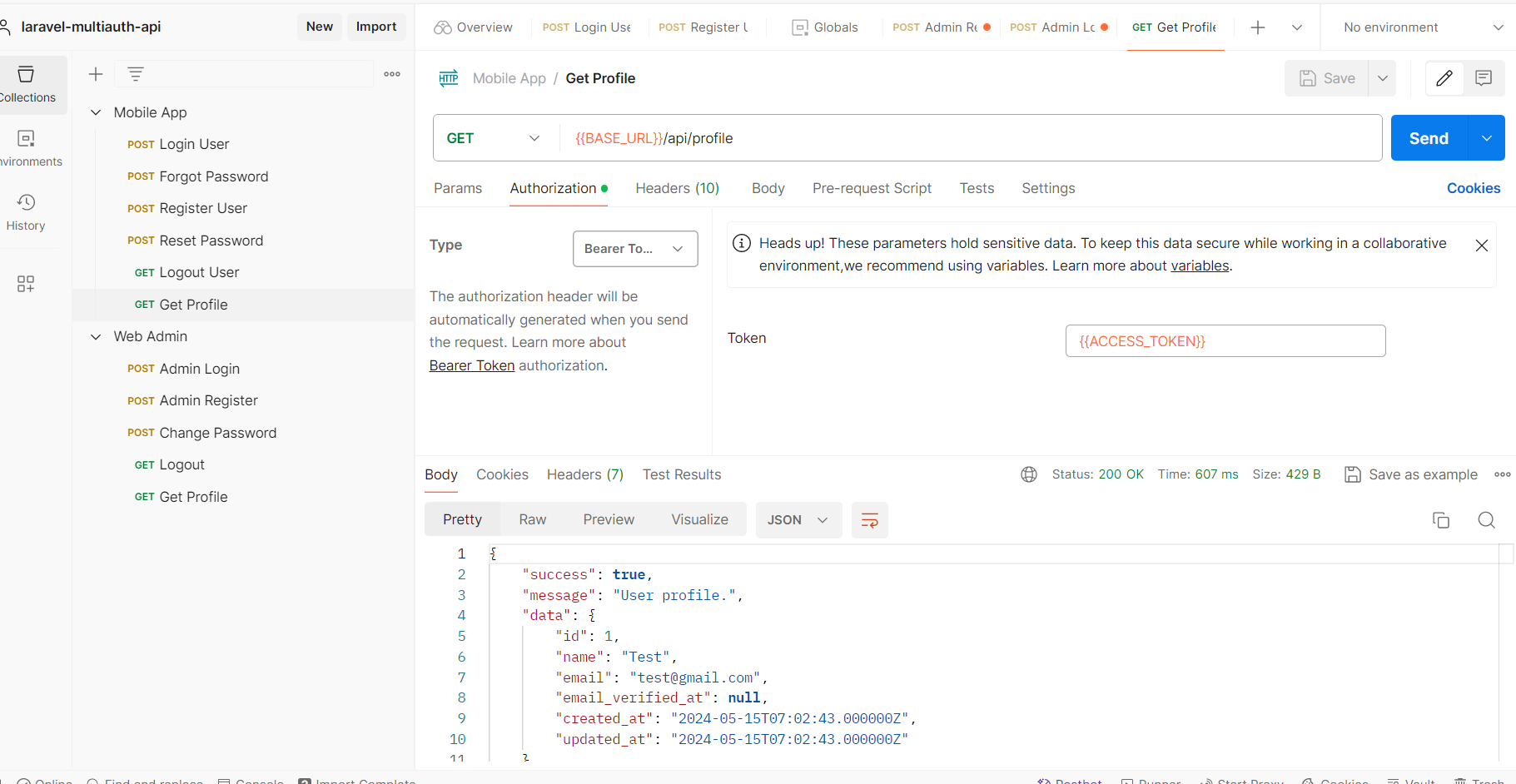
**Note: If we are testing using postman, then we can set {{ACCESS\_TOKEN}} and {{BASE\_URL}} in global environment variables.**



We need to set Auth as “Bearer token” in postman, and provide the value of token that we received from login API.

Note: We can manually put the access token for every API in Auth section, or we can create the environment variable named ‘ACCESS\_TOKEN’ for this token and can use that variable into API auth section.

**API - Get Profile:**



**API Endpoint**: <http://localhost:8000/api/>profile

**Method**: GET

**Headers**:

Accept: application/vnd.api+json

Content-Type: application/vnd.api+json

Authorization: Bearer {{ACCESS\_TOKEN}}

**Response**:

{

"success": true,

"message": "User profile.",

"data": {

"id": 1,

"name": "Test",

"email": "test@gmail.com",

"email\_verified\_at": null,

"created\_at": "2024-05-15T07:02:43.000000Z",

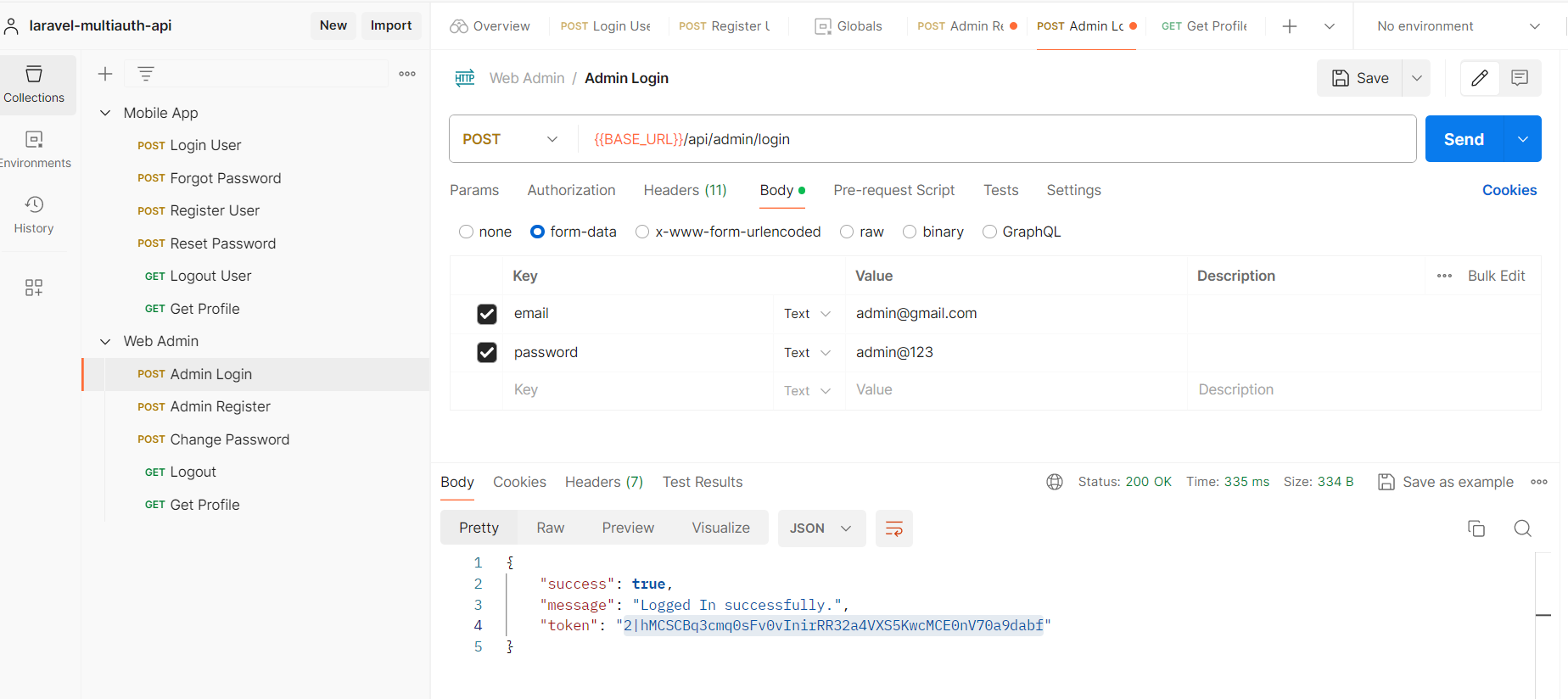
"updated\_at": "2024-05-15T07:02:43.000000Z"

}

}

…………

**API – Admin Login:**



**API Endpoint**: <http://localhost:8000/api/admin/login>

**Method**: POST

**Headers**:

Accept: application/vnd.api+json

Content-Type: application/vnd.api+json

**Body Form Data:**

email: "admin@gmail.com"

password: "admin@123"

**Response**:

{

    "success": **true**,

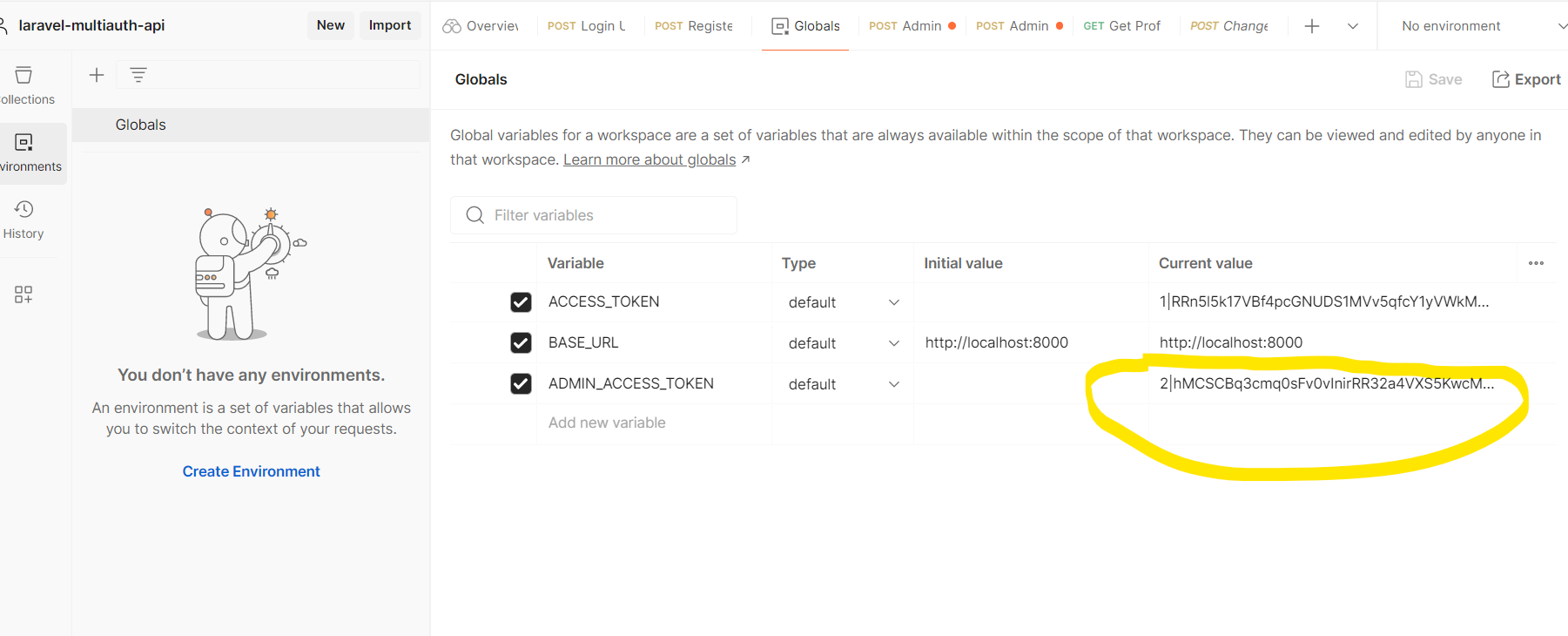
    "message": "Logged In successfully.",

    "token": " 2|hMCSCBq3cmq0sFv0vInirRR32a4VXS5KwcMCE0nV70a9dabf"

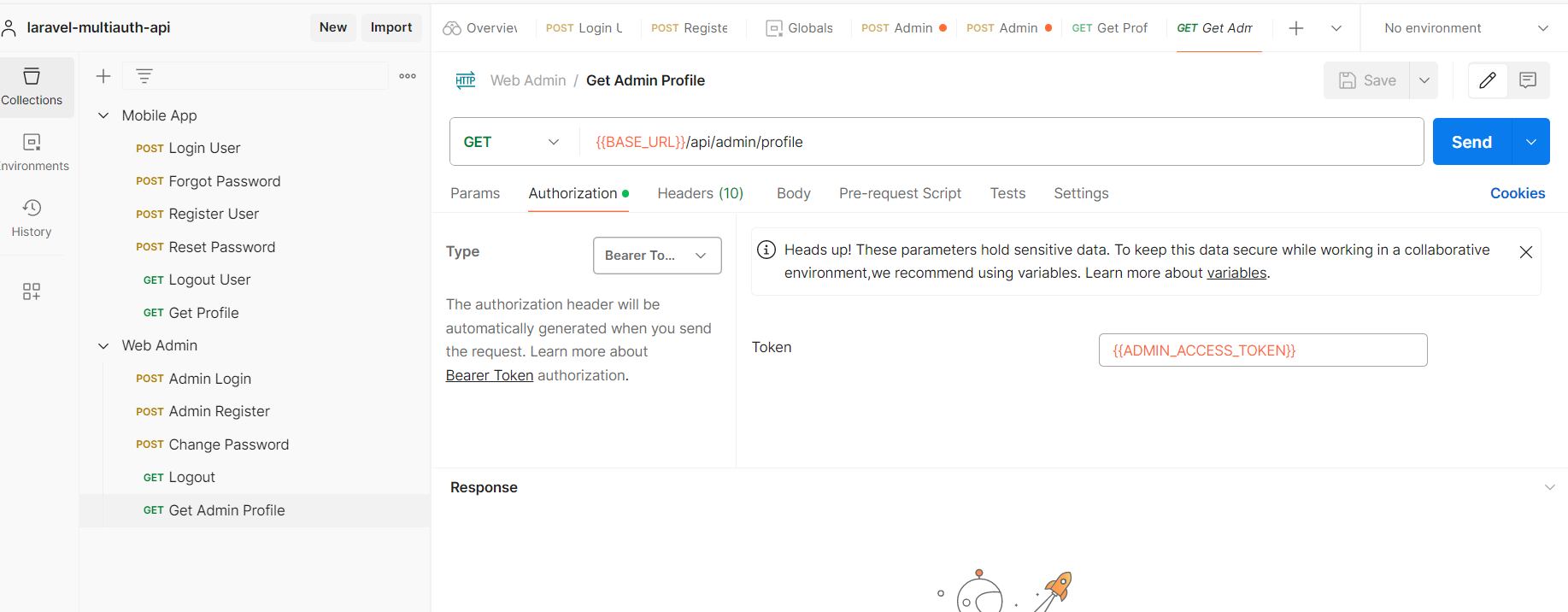
}

We need to use this yellow highlighted token to access other Admin API endpoints.

**Note: Now we need to set {{ADMIN\_ACCESS\_TOKEN}} in global environment variables for accessing admin routes.**



**API – Get Admin Profile:**



**API Endpoint**: <http://localhost:8000/api/admin/profile>

**Method**: GET

**Headers**:

Accept: application/vnd.api+json

Content-Type: application/vnd.api+json

Authorization: Bearer {{ADMIN\_ACCESS\_TOKEN}}

**Response**:

{

"success": true,

"message": "Admin profile.",

"data": {

"id": 2,

"name": "Admin",

"email": "admin@gmail.com",

"email\_verified\_at": null,

"created\_at": "2024-05-15T07:12:27.000000Z",

"updated\_at": "2024-05-15T07:12:27.000000Z"

}

}

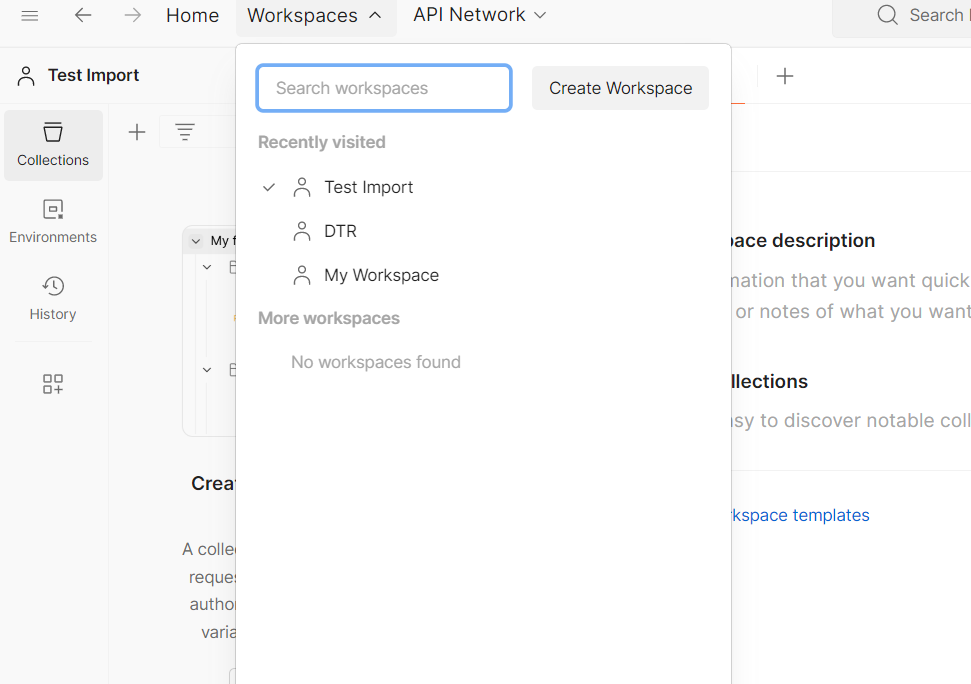
**Guideline**:

For testing the APIs, we have shared the API collections here:

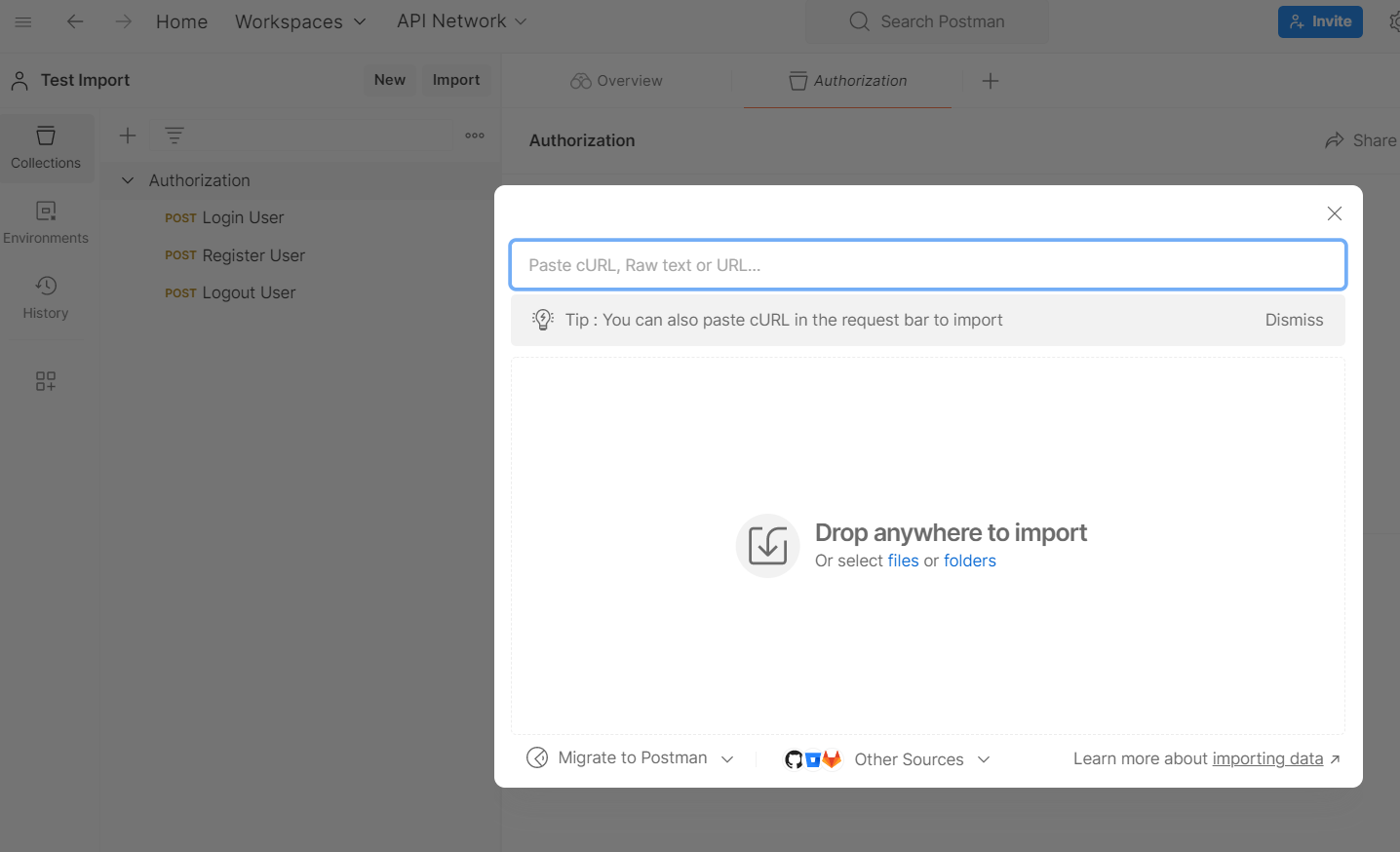
<https://github.com/harshitjaindev/laravel-multiauth-api/tree/main/Postman-Collections>

We need to import the collections and globals files in postman.

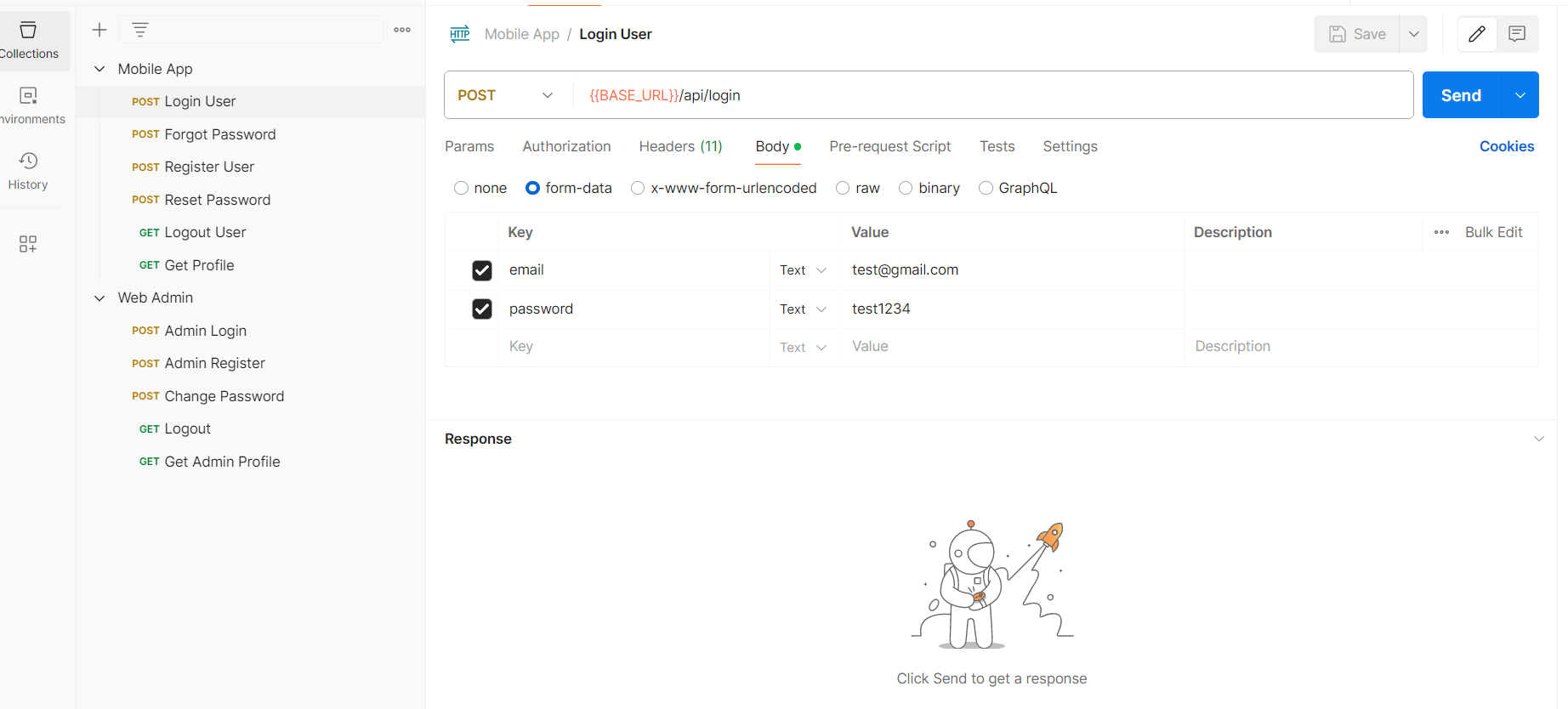
Step 1. Create a New workspace in postman using “**Create Workspace**”.



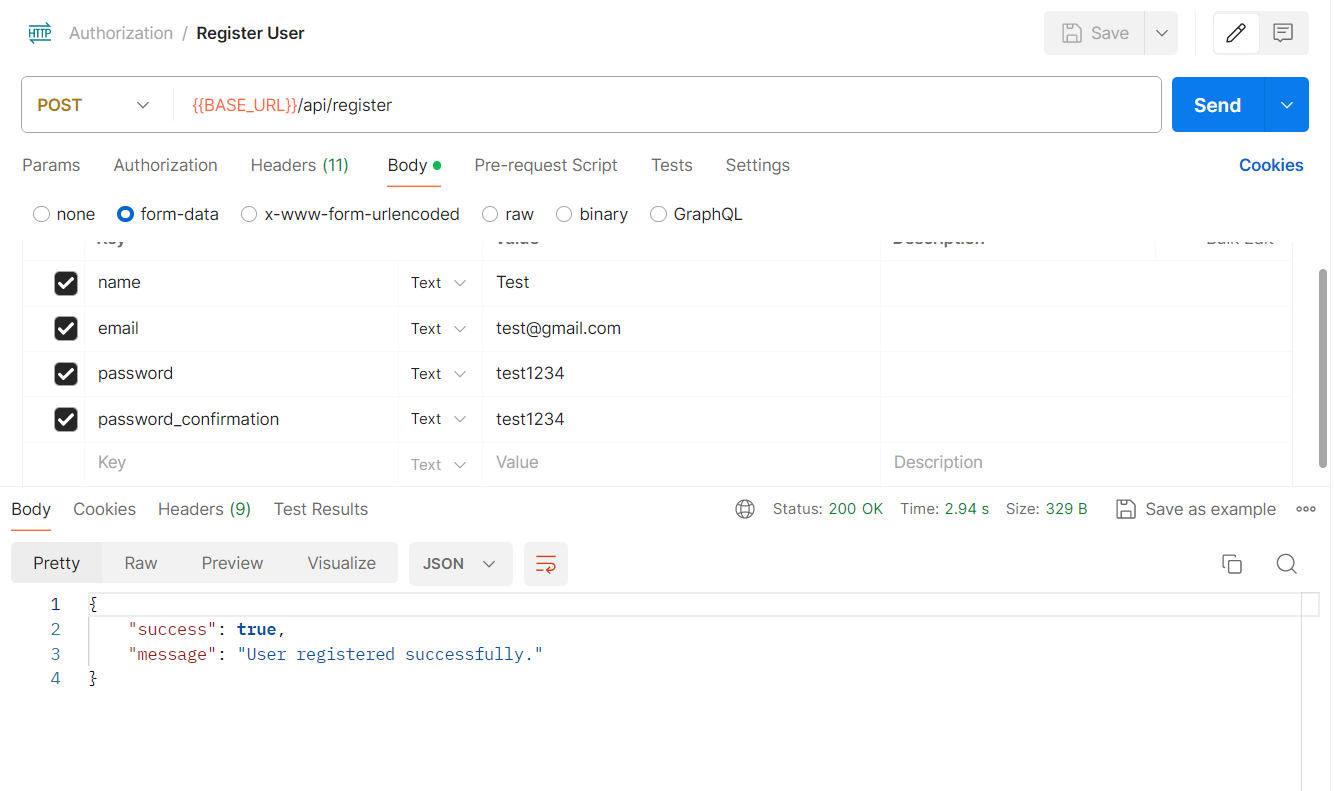
2. Once workspace is being created, kindly click on “Import button”. It will ask to select the file for import, we need to provide all the 3 files one by one.



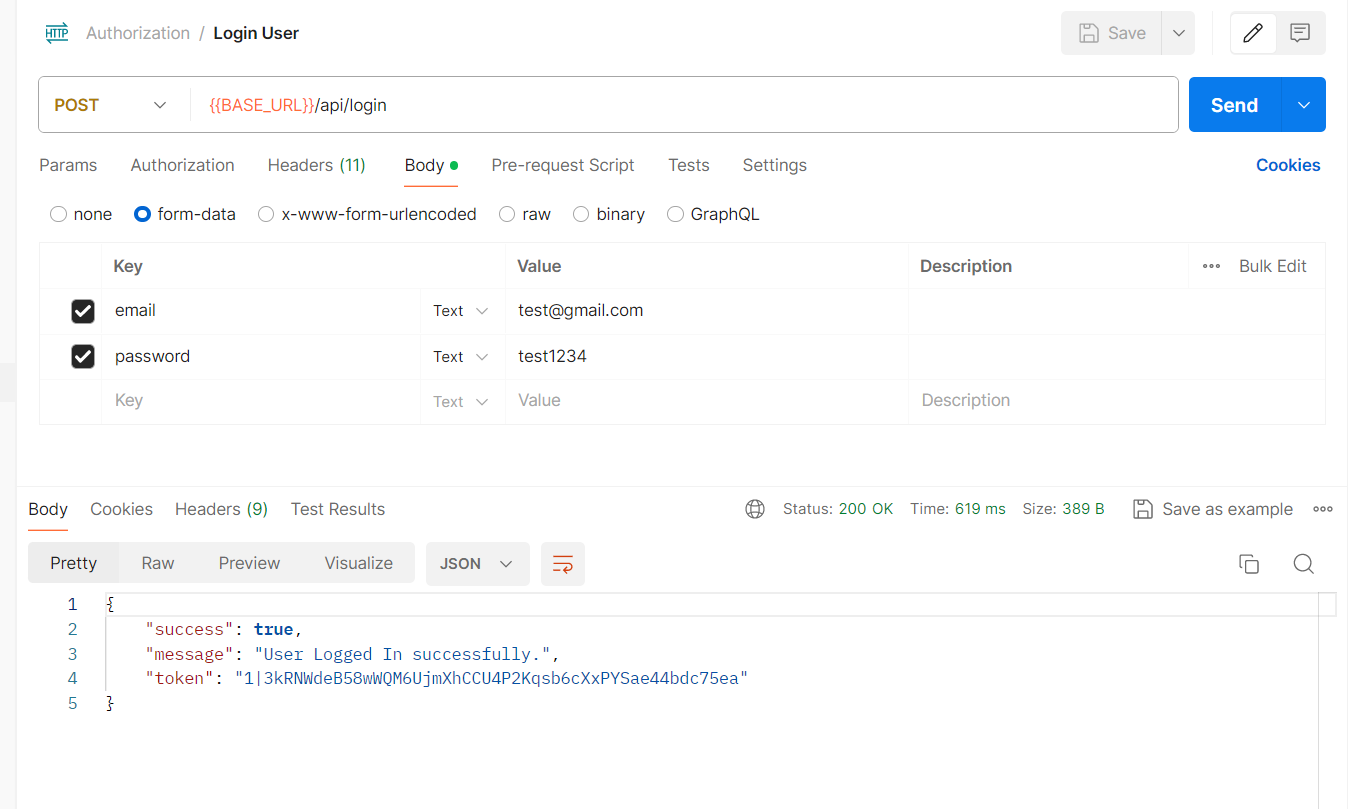
Step 3. After successful import, we can see all the APIs inside workspace.



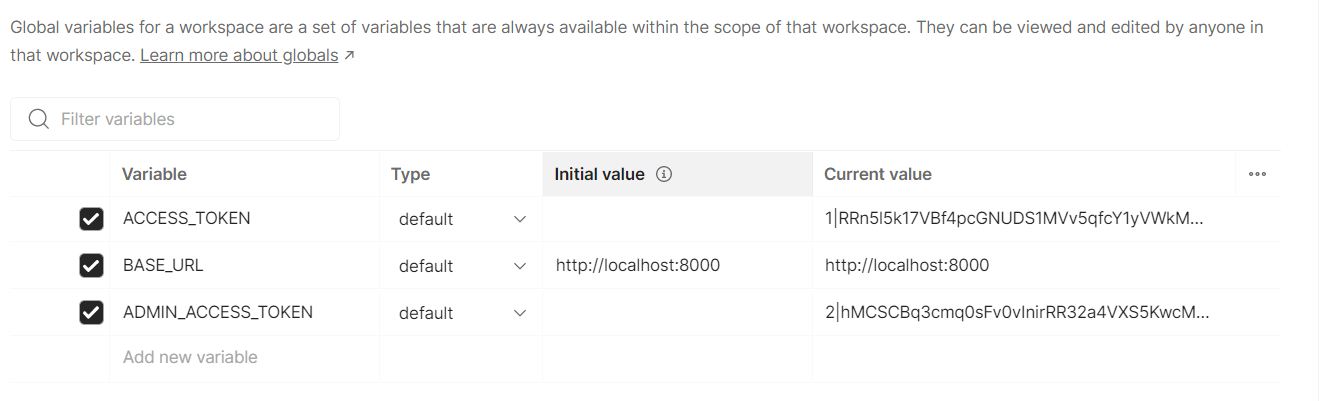
4. We need to go to “Register User” API to register a user.



5. Once user got registered, we need to go to “Login User” API and we need to trigger the API to get the access token:



6. Last step is to go to Environment > Global and update the variables (ACCESS\_TOKEN, BASE\_URL, ADMIN\_ACCESS\_TOKEN) accordingly.



**ACCESS\_TOKEN** : We need to place the generated token here.

**BASE\_URL**: We need to update our base URL here. (Ex: <http://localhost:8000>)

**ADMIN\_ACCESS\_TOKEN**: We need to place the generated admin token here.

Now we can test all the APIs.

API Endpoints:

**Mobile App Users:**

{{BASE\_URL}}/api/login

{{BASE\_URL}}/api/forgot-password

{{BASE\_URL}}/api/register

{{BASE\_URL}}/api/reset-password

{{BASE\_URL}}/api/logout

{{BASE\_URL}}/api/profile

**Web Admin:**

{{BASE\_URL}}/api/admin/login

{{BASE\_URL}}/api/admin/register

{{BASE\_URL}}/api/admin/change-password

{{BASE\_URL}}/api/admin/logout

{{BASE\_URL}}/api/admin/profile