Pentesting (parte 3)

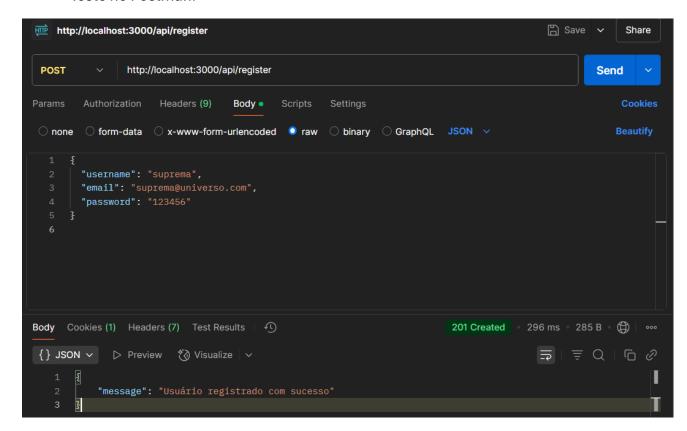
Pâmela Baron, Dereck Conink, Maria A. Giuliari e Mariele Vieira

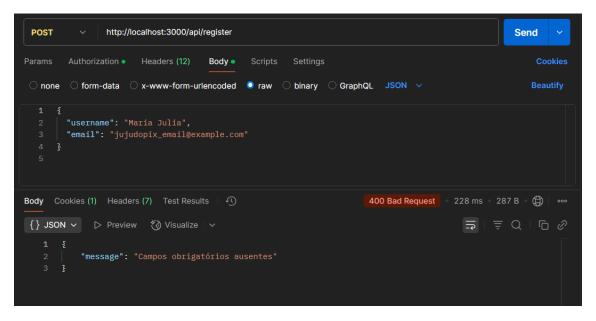
ROTA DE REGISTRO

Método: POST

URL: http://localhost:3000/api/register

Teste no Postman:





ROTA DE LOGIN

Método: POST

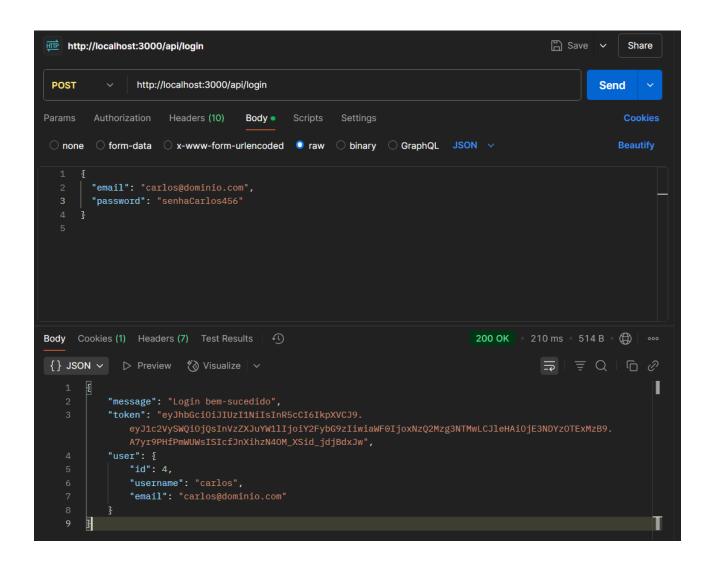
URL: http://localhost:3000/api/login

• Teste no Postman:

ROTAS CRUD PARA USUÁRIOS

Pré requisitos:

- Estar cadastrado e logado no sistema com um usuário válido.
- Fazer uma requisição POST para /api/login com email e senha válidos.
- Copiar o token JWT retornado.
- Utilizar o token em requisições protegidas.



Para testas as rotas protegidas (CRUD de usuários) no Postman:

Pré requisitos:

- Fazer login em /api/login.
- Copiar o token JWT retornado na reposta.

1. GET /api/users - Listar usuários

Configuração no Postman:

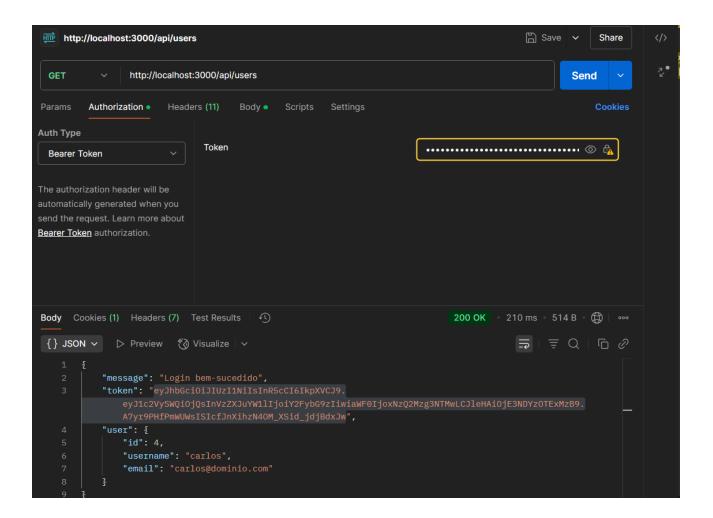
• Método: GET.

URL: http://localhost:3000/api/users

Headers:

o Content-Type: application/json

o Authorization: Bearer < O TONKEN DO CARLOS>



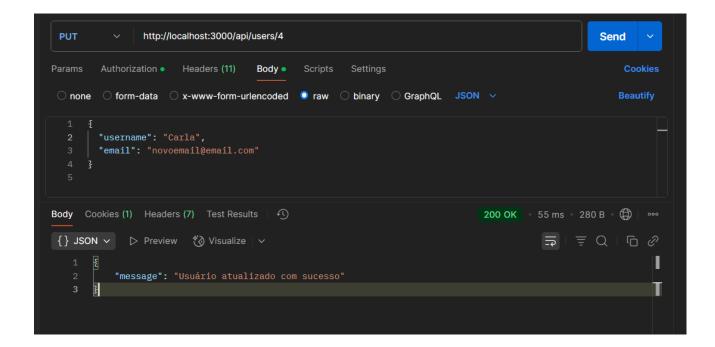
```
GET
                http://localhost:3000/api/users
                                                                                                     Send
                                     Body •
○ none ○ form-data ○ x-www-form-urlencoded ○ raw ○ binary ○ GraphQL JSON ∨
                                                                                                         Beautify
                                                                                                         (
Body Cookies (1) Headers (7) Test Results
                                                                               200 OK 220 ms 480 B
 {} JSON ✓ ▷ Preview 🍪 Visualize ✓
                                                                                           = Q 1 G 0
           "users": [
                   "username": "suprema",
                   "email": "suprema@universo.com"
                   "username": "joana",
                   "email": "joana@dominio.com"
                   "username": "carlos",
                   "username": "marina",
"email": "marina@dominio.com"
```

2. PUT /users: Atualiza os dados de um usuário com base em seu id (apenas usuários autenticados).

Configuração no Postman:

Método: PUT.

URL: http://localhost:3000/api/users/



3. DELETE /users: Exclui um usuário com base em seu id (apenas usuários autenticados).

Pré requisitos:

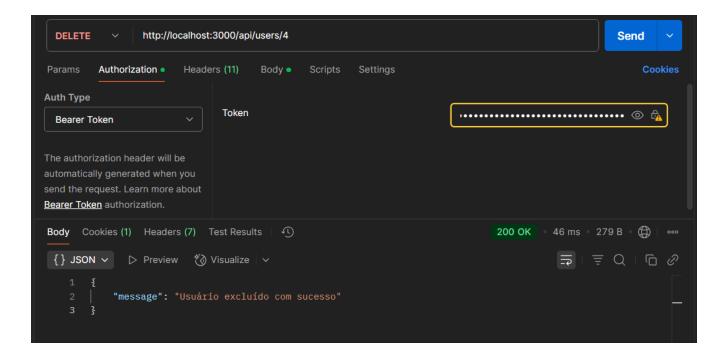
- Já estar autenticado (ou seja, já ter feito login e ter um token JWT)
- O ID que será usado no DELETE deve ser o seu próprio ID de usuário (o mesmo contido no token).

Configuração no Postman:

• Método: DELETE.

• URL: http://localhost:3000/api/login

```
POST
                 http://localhost:3000/api/login
                                                                                                      Send
Params
                                      Body •
                                               Scripts
                                                       Settings
○ none
        ○ form-data ○ x-www-form-urlencoded ○ raw ○ binary ○ GraphQL JSON ∨
        "email": "novoemail@email.com",
        "password": "senhaCarlos456"
Body Cookies (1) Headers (7) Test Results
                                                                                         621 ms 513 B 🕀
                                                                               200 OK
{} JSON ~ Preview 🖔 Visualize ~
                                                                                                  <u>=</u> Q ∣
                                                                                                                ı
           "message": "Login bem-sucedido",
           "token": "eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.
               {\tt eyJ1c2VySWQi0jQsInVzZXJuYW1lIjoiQ2FybGEiLCJpYXQi0jE3NDYzOTEzNzksImV4cCI6MTc0NjM5NDk30X0.}
               mH8Zkr_agcp004JeWLFRRFyRfan73QKTFPUF_DD-yy4",
           "user": {
               "username": "Carla",
               "email": "novoemail@email.com"
       3
```



PROTEÇÃO DE ROTAS PUT e DELETE

Passo a Passo (Rota PUT):

- 1. Realizar Login e obter o Token JWT.
- 2. Abrir o Postman.

3. Criar uma nova requisição do tipo POST.

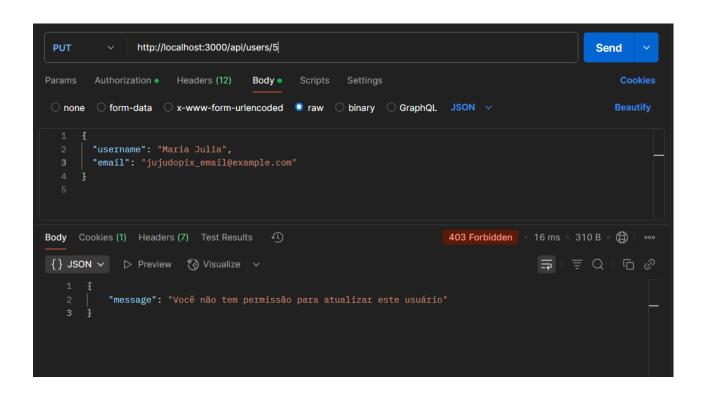
Configuração no Postman:

Método: POST.

URL: http://localhost:3000/api/login

```
🖺 Save 🗸
http://localhost:3000/api/login
                                                                                                             Share
                 http://localhost:3000/api/login
 POST
                                                                                                        Send
                                     Body •
                                                       Settings
 onne of form-data ox-www-form-urlencoded oraw obinary of GraphQL JSON ∨
         "email": "joana@dominio.com",
Body Cookies (1) Headers (7) Test Results
                                                                                 200 OK 441 ms 511 B
{} JSON ✓ ▷ Preview 🖔 Visualize ✓
            "message": "Login bem-sucedido",
                eyJ1c2VySWQi0jMsInVzZXJuYW11Ijoiam9hbmEiLCJpYXQi0jE3NDYzOTIzMTIsImV4cCI6MTc0NjM5NTkxMn0.
               0dlDBJnthGRpCbiSWS3T-ebXkHxZkYn7tqaHHnt0qCg",
                "username": "joana",
"email": "joana@dominio.com"
```

```
http://localhost:3000/api/users/3
                                                                                          □ Save ∨
                                                                                                        Share
                http://localhost:3000/api/users/3
 PUT
                                                                                                   Send
        Authorization • Headers (12)
                                     Body •
                                                                                                       Cookies
Params
○ none
        ○ form-data ○ x-www-form-urlencoded ◎ raw ○ binary ○ GraphQL JSON ∨
        "username": "Maria Julia",
Body Cookies (1) Headers (7) Test Results
                                                                              200 OK
                                                                                       40 ms 🏻 280 B 🐧 🗎
{} JSON ✓ ▷ Preview 🍪 Visualize ✓
                                                                                                             I
           "message": "Usuário atualizado com sucesso"
```



Passo a Passo (Rota DELETE):

- 1. Realizar Login e obter o Token JWT.
- 2. Abrir o Postman.
- 3. Criar uma nova requisição do tipo DELETE.

Configuração no Postman:

- Método: DELETE.
- URL: http://localhost:3000/api/users/

