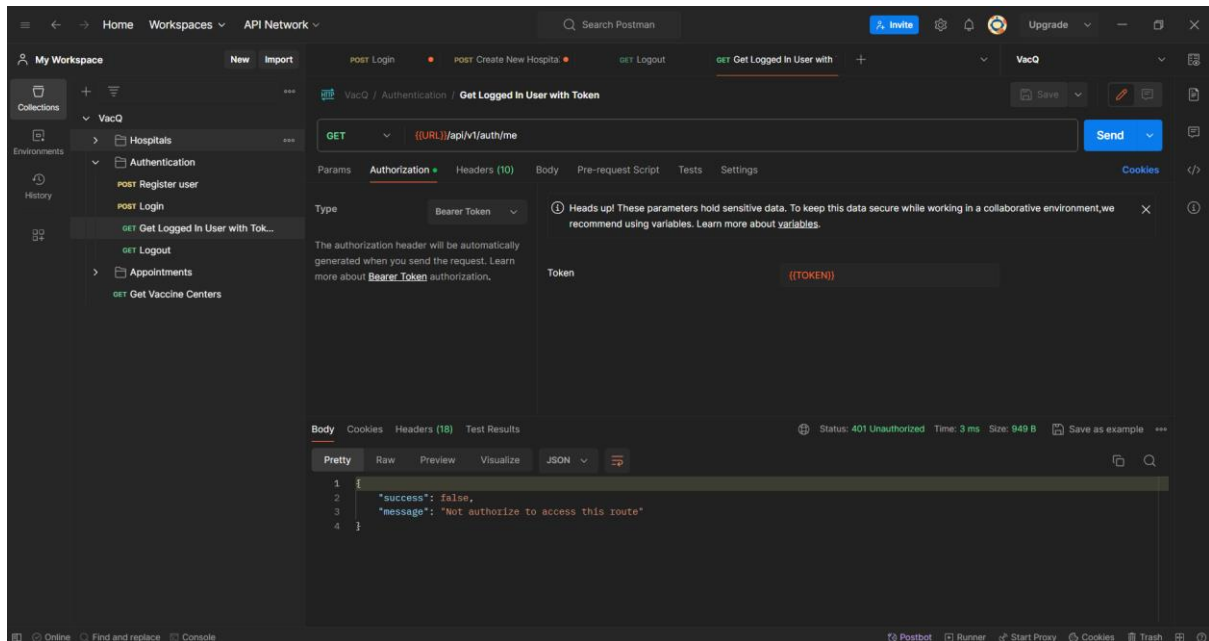
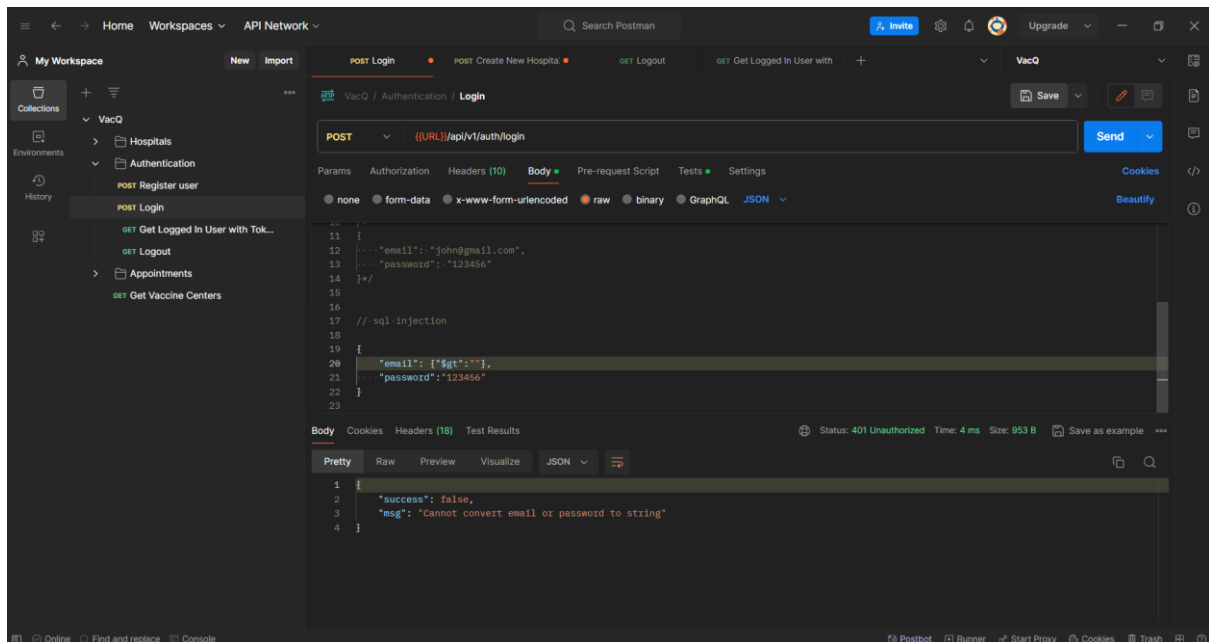


# API Security

## logout



## prevent SQL injection



## apply Helmet

The screenshot shows a Postman interface with a workspace named 'VacQ'. The active collection is 'VacQ' and the selected environment is 'Environments'. The request is a POST to '([URL])api/v1/auth/login'. The response status is 200 OK. The response headers are displayed in a table:

Key	Value
Content-Security-Policy	default-src 'self';base-uri 'self';font-src 'self' https://data.frame-ancesto...
Cross-Origin-Opener-Policy	same-origin
Cross-Origin-Resource-Policy	same-origin
Origin-Agent-Cluster	?1
Referrer-Policy	no-referrer
Strict-Transport-Security	max-age=15552000; includeSubDomains
X-Content-Type-Options	nosniff
X-DNS-Prefetch-Control	off
X-Download-Options	noopen
X-Frame-Options	SAMEORIGIN
X-Permitted-Cross-Domain-Policies	none
X-XSS-Protection	0
Set-Cookie	token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZiJpZGQwZGRZDE5NjYzYWE2M...
Content-Type	application/json, charset=utf-8
Content-Length	198

## prevent XSS

The screenshot shows a Postman interface with a workspace named 'VacQ'. The active collection is 'VacQ' and the selected environment is 'Environments'. The request is a POST to '([URL])api/v1/hospitals'. The request body is a JSON object with the following fields:

```
{  "name": "Hacker Hospital <script>alert(1)</script>",  "address": "Hospital",  "district": "Hacker",  "province": "Nonthaburi",  "postalcode": "10110",  "tel": "02-8369999",  "region": "Bangkok"}
```

The response status is 201 Created. The response body is a JSON object with the following fields:

```
{  "success": true,  "data": {    "name": "Hacker Hospital",    "address": "Hospital",    "district": "Hacker",    "province": "Nonthaburi",    "postalcode": "10110",    "tel": "02-8369999",    "region": "Bangkok",    "id": "65e8ec62faadebcd48394395",    "_v": 0,    "id": "65e8ec62faadebcd48394395"  }}
```

apply Express-rate-limit

The screenshot shows the Postman interface with a workspace named 'VacQ'. A collection 'Hospitals' is expanded, showing a 'GET Single Hospital' request. The request URL is `((URL))/api/v1/hospitals/65d7751cce1e1088f93e0de3`. The request is a GET method. The response status is 429 Too Many Requests, with a time of 4 ms and a size of 1021 B. The response body is 'Too many requests, please try again later.'

Query Params

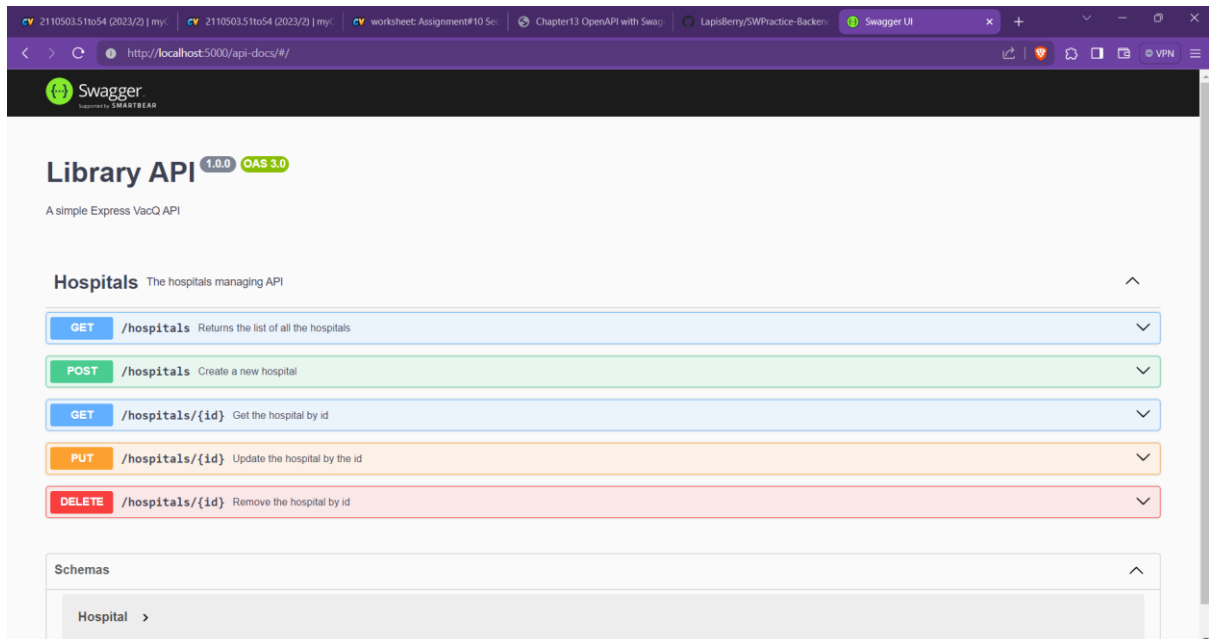
Key	Value	Description
Key	Value	Description

Body

```
1 Too many requests, please try again later.
```

# Open API

items



add the server URL to Open API document

