

## Logout:

The screenshot shows the Postman interface with a workspace named 'My Workspace'. The left sidebar displays a collection of API endpoints under 'SW\_backend'. The selected endpoint is 'GET get me' under the 'auth' folder. The main panel shows the request details for 'GET /api/v1/auth/me'. The response is a 401 Unauthorized status with a message: 'Not authorize to access this route'.

```
1 {
2   "success": false,
3   "message": "Not authorize to access this route"
4 }
```

## NoSQL injection:

The screenshot shows the Postman interface with a workspace named 'My Workspace'. The left sidebar displays a collection of API endpoints under 'SW\_backend'. The selected endpoint is 'POST login' under the 'auth' folder. The main panel shows the request details for 'POST /api/v1/auth/login'. The request body is a JSON object with a NoSQL injection payload: `{ "email": {"$gt": ""}, "password": "user123" }`. The response is a 401 Unauthorized status with a message: 'Cannot convert email or password to string'.

```
1 {
2   "email": {"$gt": ""},
3   "password": "user123"
4 }
```

```
1 {
2   "success": false,
3   "msg": "Cannot convert email or password to string"
4 }
```

# Helmet

The screenshot shows the API Network client interface. The left sidebar displays a collection of endpoints under 'My Workspace'. The main panel shows a GET request to `SW_backend / assignment-10 / auth / get me` with the URL `{{URL}}/api/v1/auth/me`. The response is a 401 Unauthorized status with the following headers:

Key	Value
Content-Security-Policy	default-src 'self';base-uri 'self';font-src 'self' https; dat...
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

# XSS

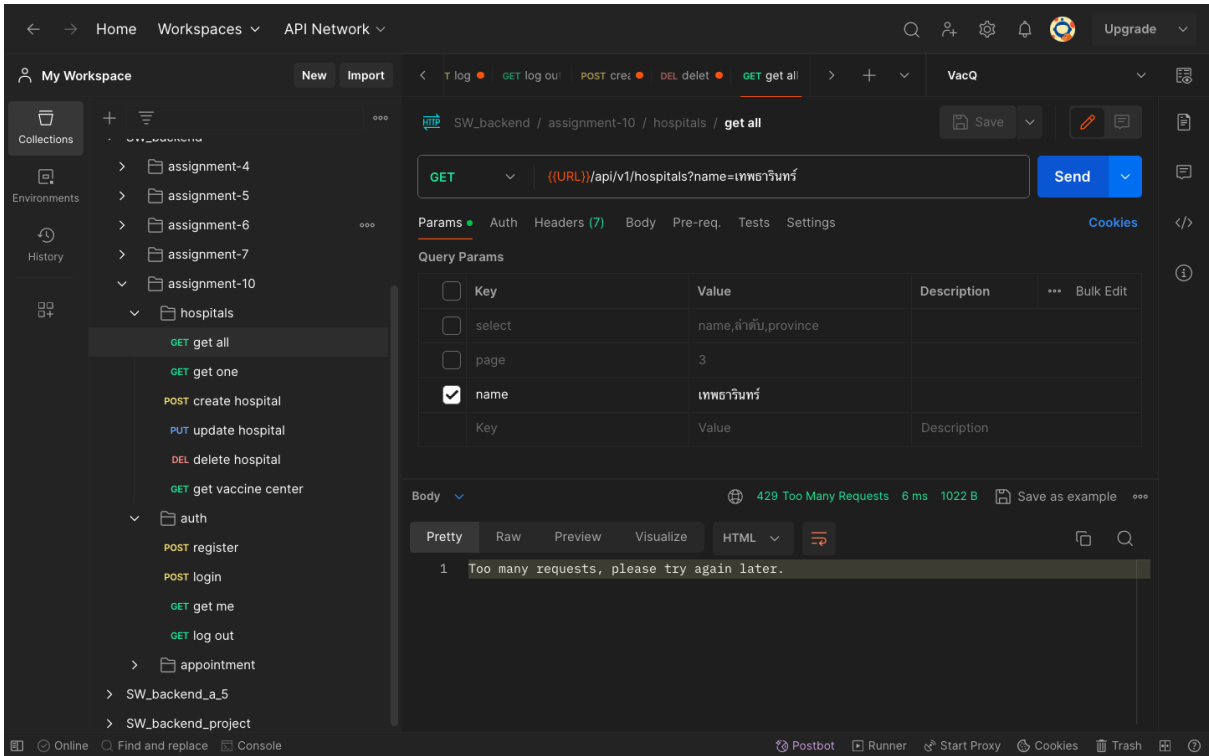
The screenshot shows the API Network client interface. The left sidebar displays a collection of endpoints under 'My Workspace'. The main panel shows a POST request to `SW_backend / assignment-10 / hospitals / create hospital` with the URL `{{URL}}/api/v1/hospitals/`. The request body is in JSON format:

```
{
  "name": "dummy <script>alert(1)</script> naja",
  "address": "2012/5-7 ถนนพหลโยธิน แขวงจตุจักร",
  "district": "จตุจักร",
  "province": "กรุงเทพมหานคร",
  "postalcode": "10900",
  "tel": "02-5791770-4",
  "region": "กรุงเทพมหานคร (Bangkok)"
}
```

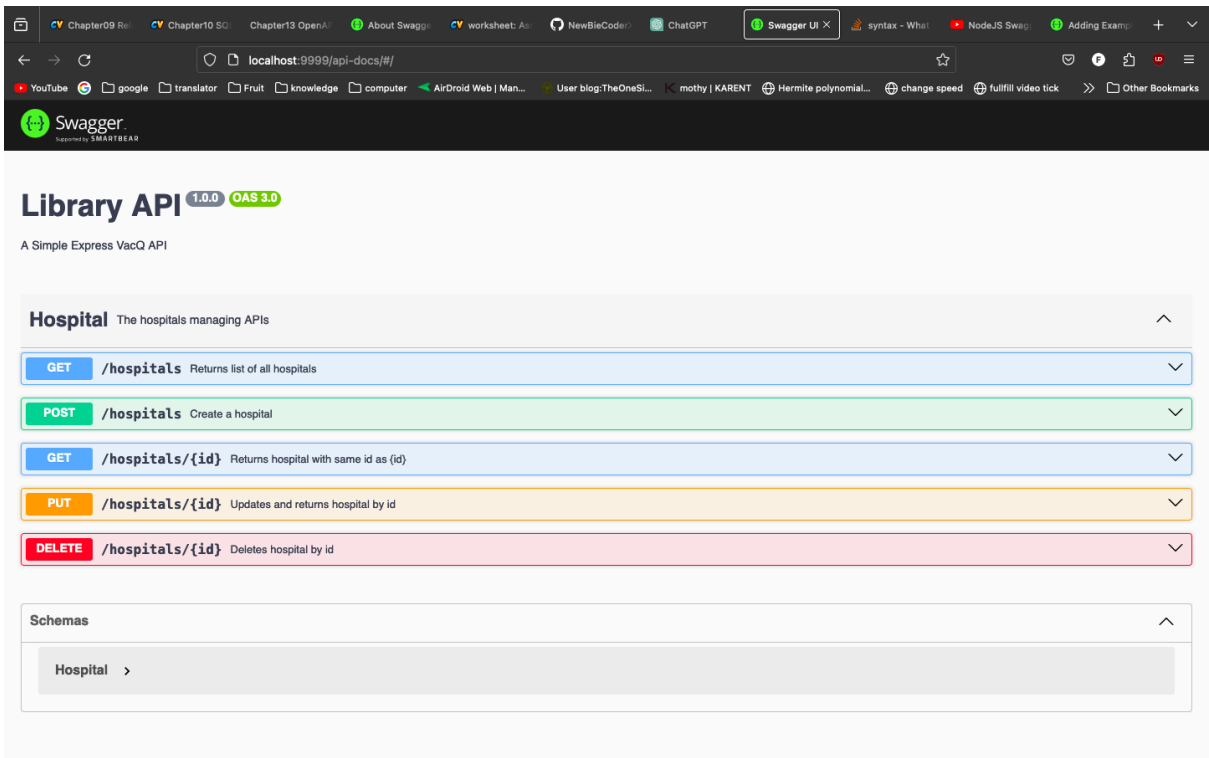
The response is a 201 Created status with the following body:

```
{
  "success": true,
  "data": {
    "name": "dummy naja",
    "address": "2012/5-7 ถนนพหลโยธิน แขวงจตุจักร",
    "district": "จตุจักร",
    "province": "กรุงเทพมหานคร",
    "postalcode": "10900",
    "tel": "02-5791770-4",
    "region": "กรุงเทพมหานคร (Bangkok)"
  }
}
```

rate limit:



openAPI all hospital routes:



## openAPI add server url

The image shows the Swagger UI interface for the 'Library API' (version 1.0.0, OAS 3.0). The server URL is set to 'http://localhost:9999/api/v1'. The API is described as 'A Simple Express VacQ API'. The 'Hospital' section lists the following endpoints:

- GET** /hospitals: Returns list of all hospitals
- POST** /hospitals: Create a hospital
- GET** /hospitals/{id}: Returns hospital with same id as {id}
- PUT** /hospitals/{id}: Updates and returns hospital by id
- DELETE** /hospitals/{id}: Deletes hospital by id

The 'Schemas' section is also visible but empty.

## openAPI get all hospitals execute

The image shows the Swagger UI interface for the 'Library API' with the 'GET /hospitals' endpoint selected. The 'Parameters' section is empty. The 'Execute' button is highlighted. The 'Responses' section shows the server response for the 200 status code:

```
curl -X 'GET' \
  'http://localhost:9999/api/v1/hospitals' \
  -H 'accept: application/type'
```

Request URL: http://localhost:9999/api/v1/hospitals

Server response:

```
200
Response body
{
  "success": true,
  "count": 25,
  "pagination": {
    "next": {
      "page": 2,
      "limit": 25
    }
  },
  "data": [
    {
      "_id": "65d87dcl1ca757d26ee2bdf5",
      "status": 27,
      "name": "โรงพยาบาลสุราษฎร์ธานี"
    }
  ]
}
```