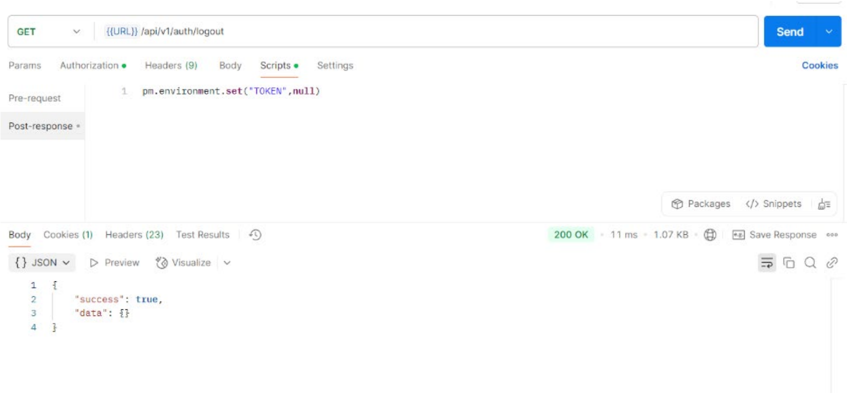
Security

1. Logout



GET {{URL}} /api/v1/auth/logout

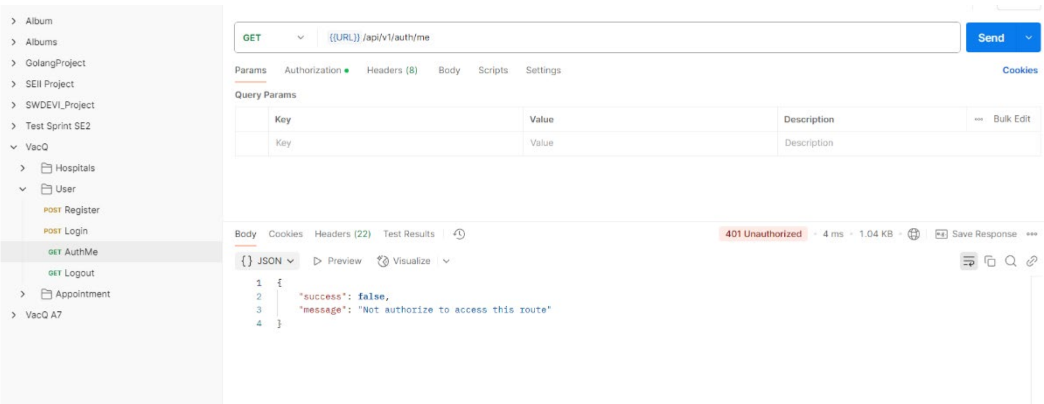
Scripts – Post-response

```
pm.environment.set("TOKEN",null)
```

200 OK · 11 ms · 1.07 KB

```
{
    "success": true,
    "data": {}
}
```

หลัง Logout

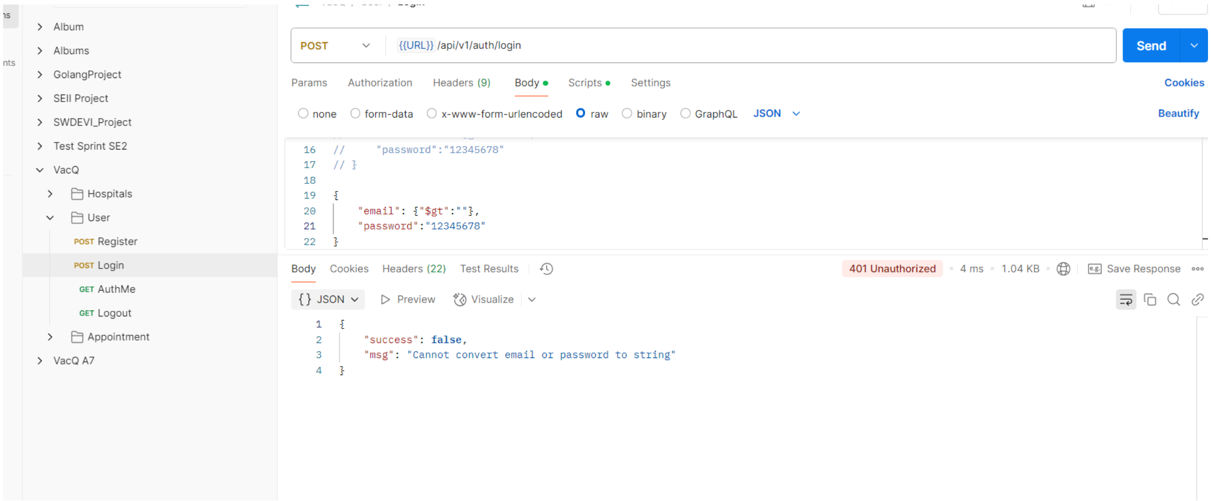


GET {{URL}} /api/v1/auth/me

401 Unauthorized · 4 ms · 1.04 KB

```
{
    "success": false,
    "message": "Not authorize to access this route"
}
```

2. SQL injection



POST {{URL}} /api/v1/auth/login

Body: ○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

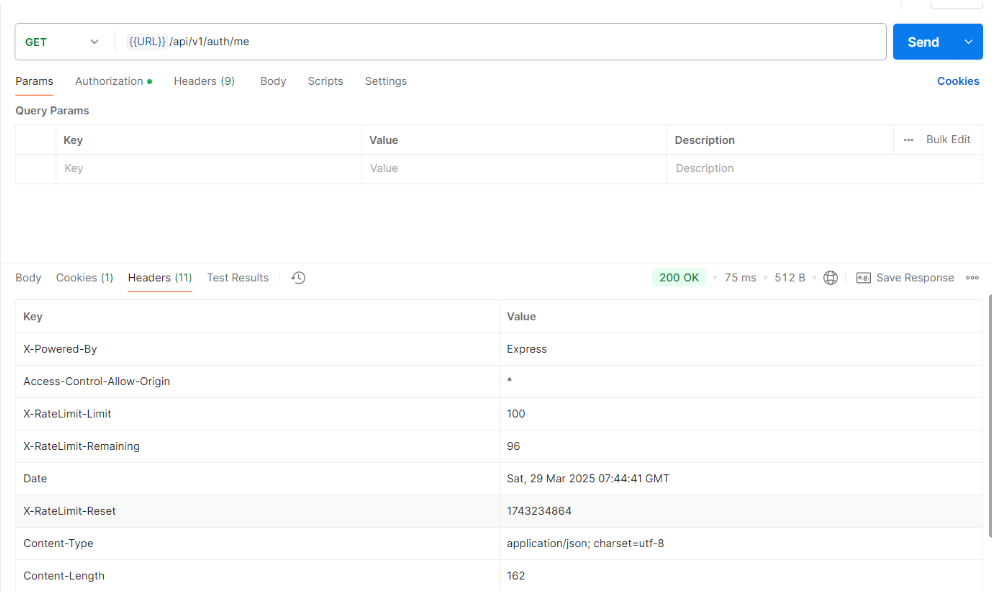
```
//     "password":"12345678"
// }

{
    "email": {"$gt":""},
    "password":"12345678"
}
```

401 Unauthorized · 4 ms · 1.04 KB

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

3. Helmet

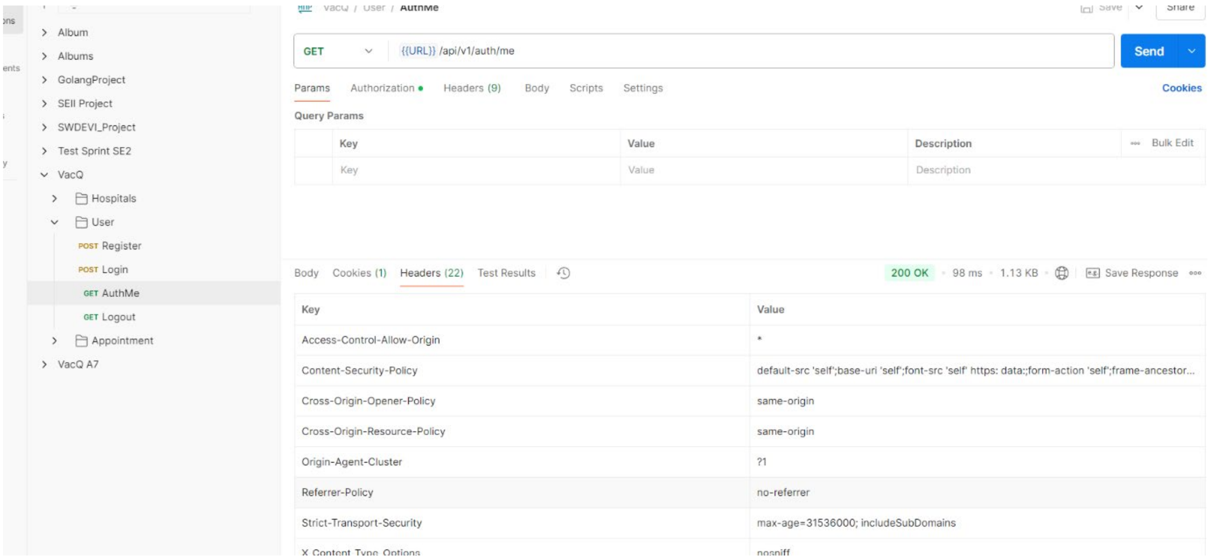
Before



Key	Value	Description
Key	Value	Description

Key	Value
X-Powered-By	Express
Access-Control-Allow-Origin	*
X-RateLimit-Limit	100
X-RateLimit-Remaining	96
Date	Sat, 29 Mar 2025 07:44:41 GMT
X-RateLimit-Reset	1743234864
Content-Type	application/json; charset=utf-8
Content-Length	162

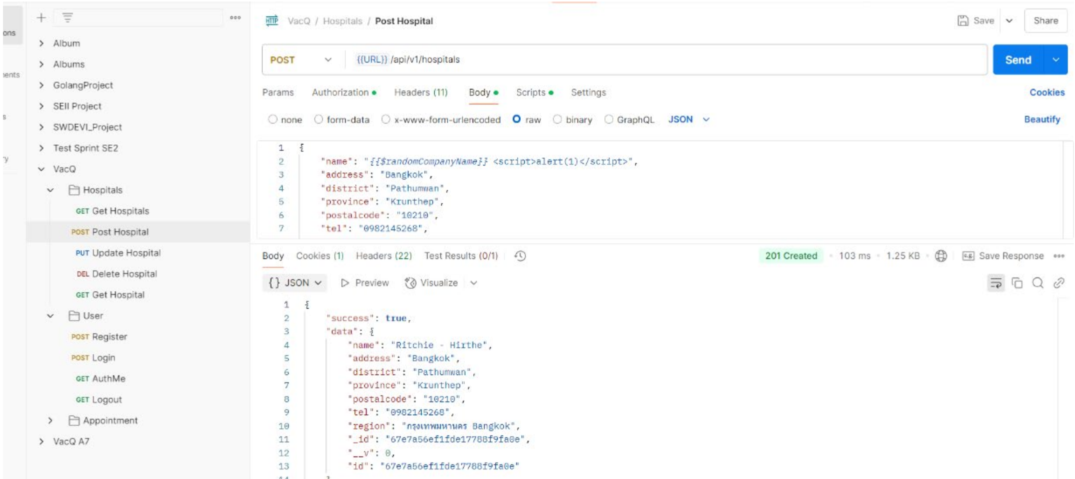
After: Insert Helmet at server.js



Key	Value	Description
Key	Value	Description

Key	Value
Access-Control-Allow-Origin	*
Content-Security-Policy	default-src 'self';base-uri 'self';font-src 'self' https: data:;form-action 'self';frame-ancestor...
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=31536000; includeSubDomains
X-Content-Type-Options	nosniff

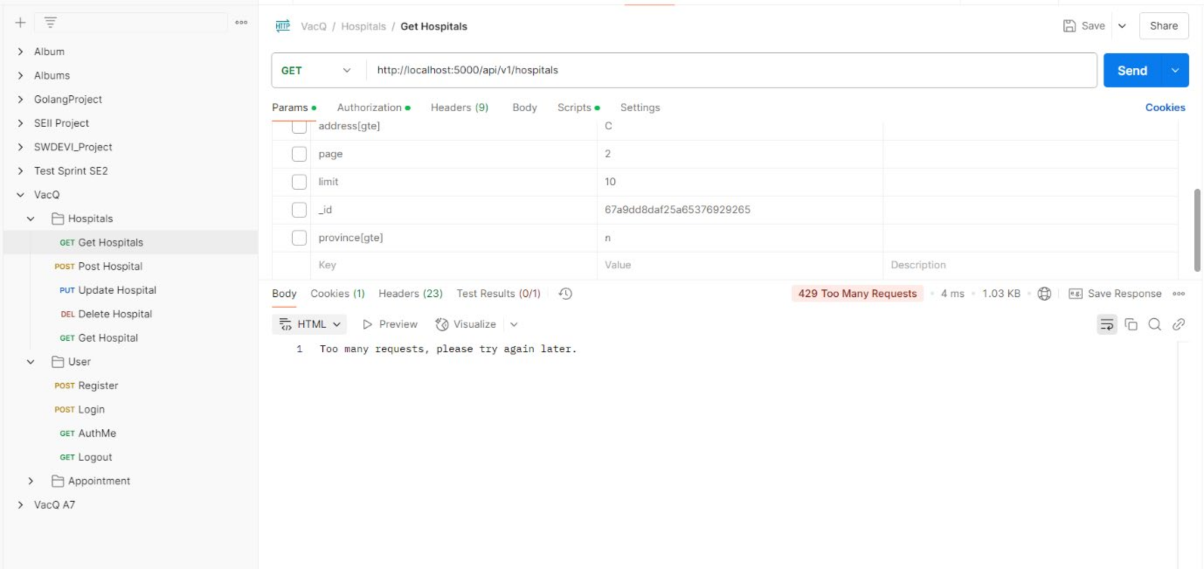
4. XSS



```
{
    "name": "{{$randomCompanyName}} <script>alert(1)</script>",
    "address": "Bangkok",
    "district": "Pathumwan",
    "province": "Krunthep",
    "postalcode": "10210",
    "tel": "0982145268",
```

```
{
    "success": true,
    "data": {
        "name": "Ritchie - Hirthe",
        "address": "Bangkok",
        "district": "Pathumwan",
        "province": "Krunthep",
        "postalcode": "10210",
        "tel": "0982145268",
        "region": "กรุงเทพมหานคร Bangkok",
        "_id": "67e7a56ef1fde17788f9fa0e",
        "__v": 0,
        "id": "67e7a56ef1fde17788f9fa0e"
```

5. Rate Limit



GET http://localhost:5000/api/v1/hospitals

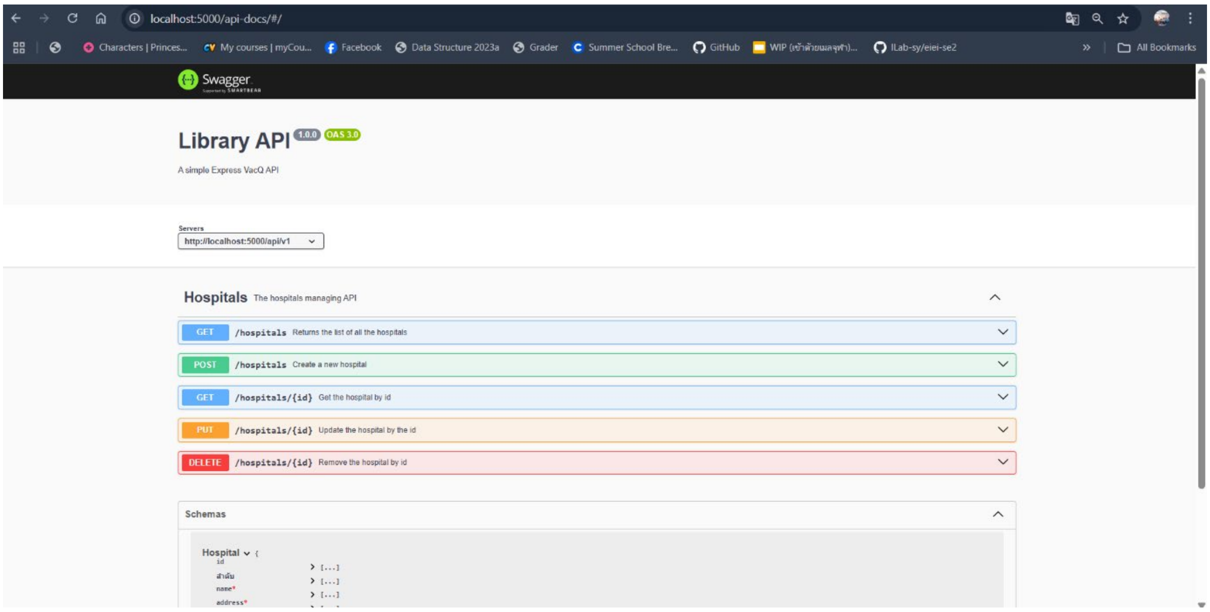
	Key	Value	Description
□	address[gte]	C	
□	page	2	
□	limit	10	
□	_id	67a9dd8daf25a65376929265	
□	province[gte]	n	

429 Too Many Requests

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

2. API Docs

Hospital API Docs



Library API 1.0.0 OAS 3.0

A simple Express VacQ API

Servers: http://localhost:5000/api/v1

Hospitals The hospitals managing API

GET /hospitals Returns the list of all the hospitals

POST /hospitals Create a new hospital

GET /hospitals/{id} Get the hospital by id

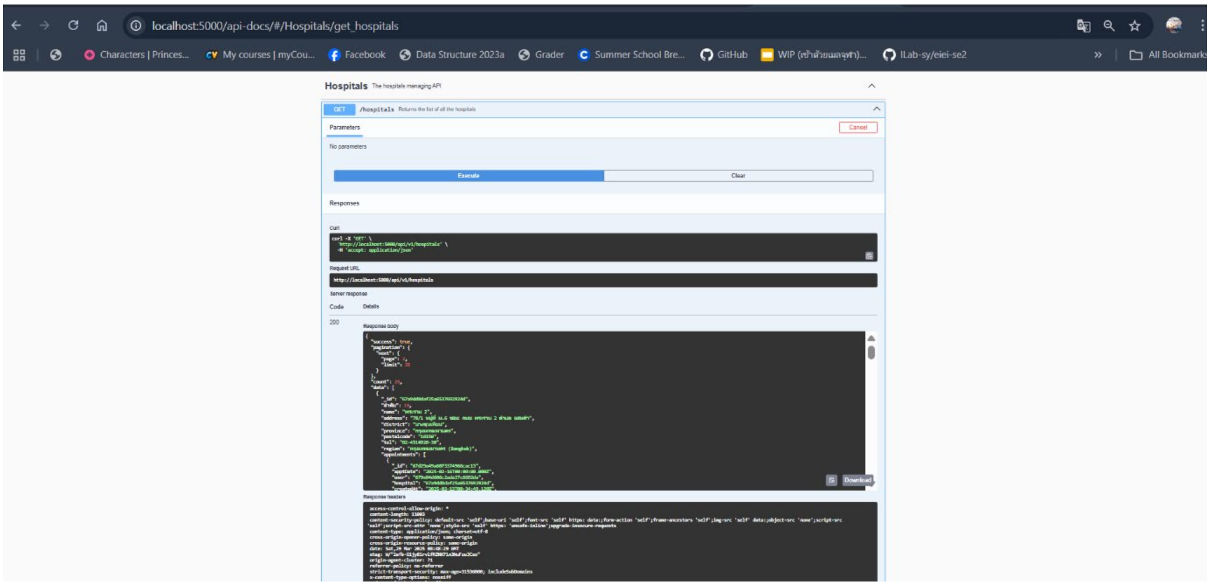
PUT /hospitals/{id} Update the hospital by the id

DELETE /hospitals/{id} Remove the hospital by id

Schemas

```
Hospital {
  id          > [...]
  ลำดับ        > [...]
  name*       > [...]
  address*
```

Get Hospitals Executions



Curl

```
curl -X 'GET' \
  'http://localhost:5000/api/v1/hospitals' \
  -H 'accept: application/json'
```

Request URL

```
http://localhost:5000/api/v1/hospitals
```

Server response

Code	Details
200	Response body

```
{
  "success": true,
  "pagination": {
    "next": {
      "page": 2,
      "limit": 25
    }
  },
  "count": 25,
  "data": [
    {
      "_id": "67a9dd8daf25a6537692924d",
      "ลำดับ": 19,
      "name": "พระราม 2",
      "address": "78/1 หมู่ที่ ม.6 ซอย ถนน พระราม 2 ตำบล แสมดำ",
      "district": "บางขุนเทียน",
      "province": "กรุงเทพมหานคร",
      "postalcode": "10150",
      "tel": "02-4514920-30",
      "region": "กรุงเทพมหานคร (Bangkok)",
      "appointments": [
        {
          "_id": "67d25a45a[illegible]66cac13",
          "apptDate": "2025-02-16T00:00:00.000Z",
          "user": "679e04d[illegible]",
          "hospital": "67a9dd8daf25a6537692924d",
          "createdAt": "2025-03-12T08:34:49.120Z",
```

Response headers

```
 access-control-allow-origin: *
 content-length: 11003
 content-security-policy: default-src 'self';base-uri 'self';font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src
'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
 content-type: application/json; charset=utf-8
 cross-origin-opener-policy: same-origin
 cross-origin-resource-policy: same-origin
 date: Sat,29 Mar 2025 08:48:29 GMT
 etag: W/"2afb-G1jy01rvlfR20071n3WufzuJCao"
 origin-agent-cluster: ?1
 referrer-policy: no-referrer
 strict-transport-security: max-age=31536000; includeSubDomains
 x-content-type-options: nosniff
```

GITHUB URL: https://github.com/pok1220/SW-DEV-I-Assignment10