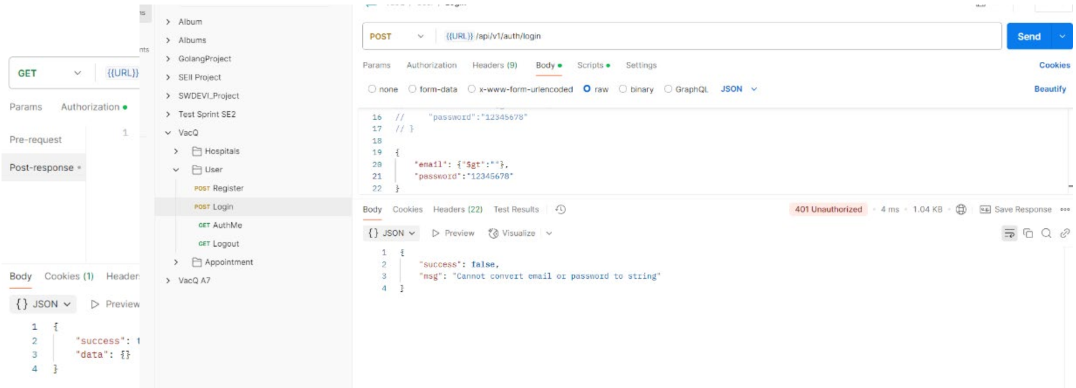
Security

1. Logout

หลัง Logout



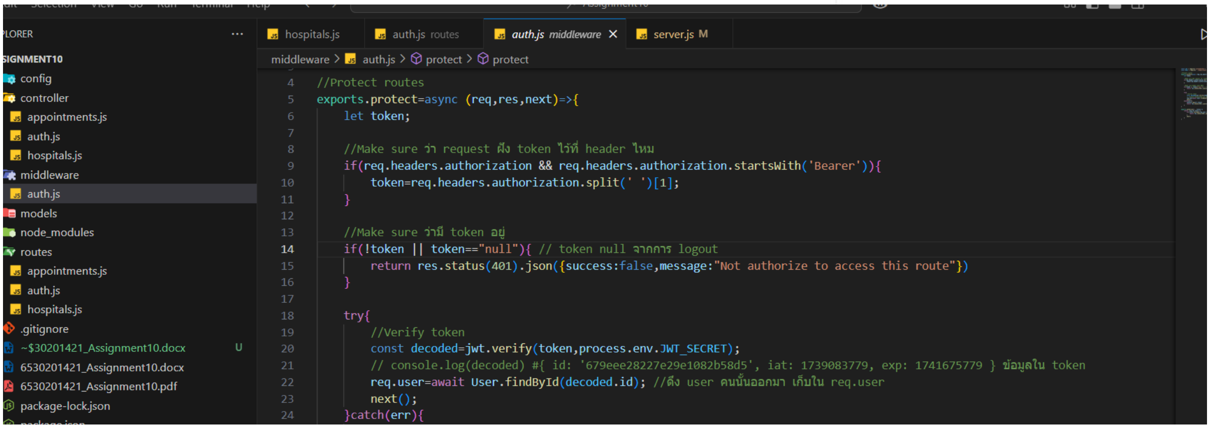
```
{
    "success": t
    "data": {}
}
```

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

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

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

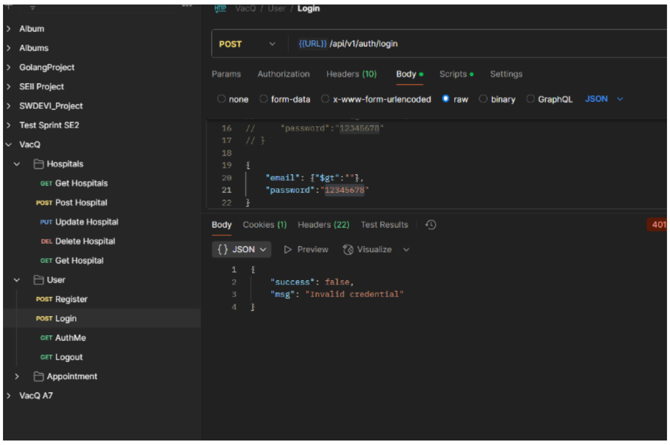
401 Unauthorized · 4 ms · 1.04 KB

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



```
//Protect routes
exports.protect=async (req,res,next)=>{
    let token;

    //Make sure ว่า request ฝัง token ไว้ที่ header ไหม
    if(req.headers.authorization && req.headers.authorization.startsWith('Bearer')){
        token=req.headers.authorization.split(' ')[1];
    }

    //Make sure ว่ามี token อยู่
    if(!token || token=="null"){ // token null จากการ logout
        return res.status(401).json({success:false,message:"Not authorize to access this route"})
    }

    try{
        //Verify token
        const decoded=jwt.verify(token,process.env.JWT_SECRET);
        // console.log(decoded) #{ id: '679eee28227e29e1082b58d5', iat: 1739083779, exp: 1741675779 } ข้อมูลใน token
        req.user=await User.findById(decoded.id); //ดึง user คนนั้นออกมา เก็บใน req.user
        next();
    }catch(err){
```

2. SQL injection (Before-After)

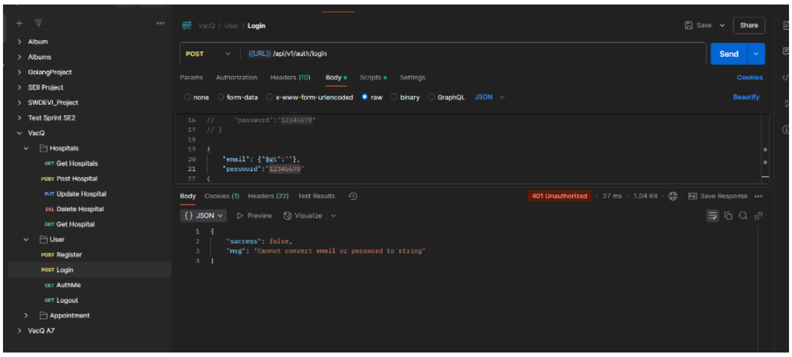


POST {{URL}} /api/v1/auth/login

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

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

401

```
{
    "success": false,
    "msg": "Invalid credential"
}
```



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

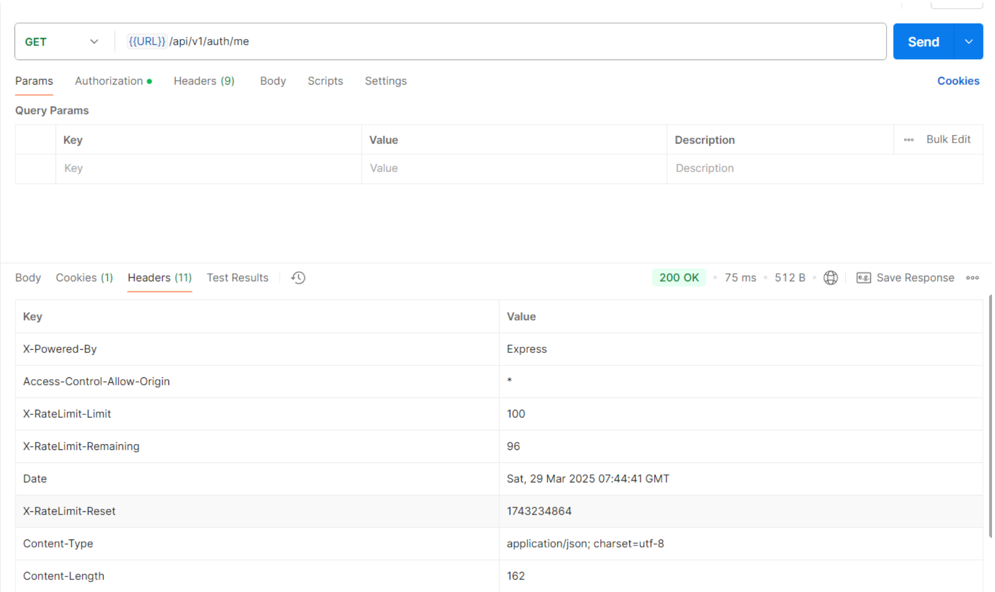
```
//      "password":"12345678"
// }

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

401 Unauthorized · 27 ms · 1.04 KB

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

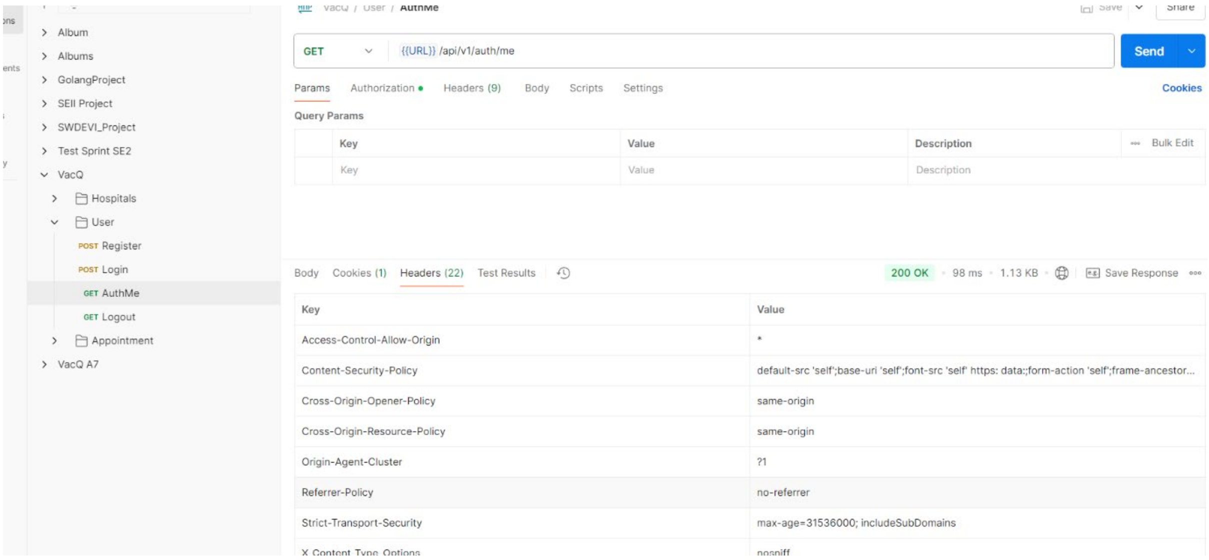
3. Helmet

Before



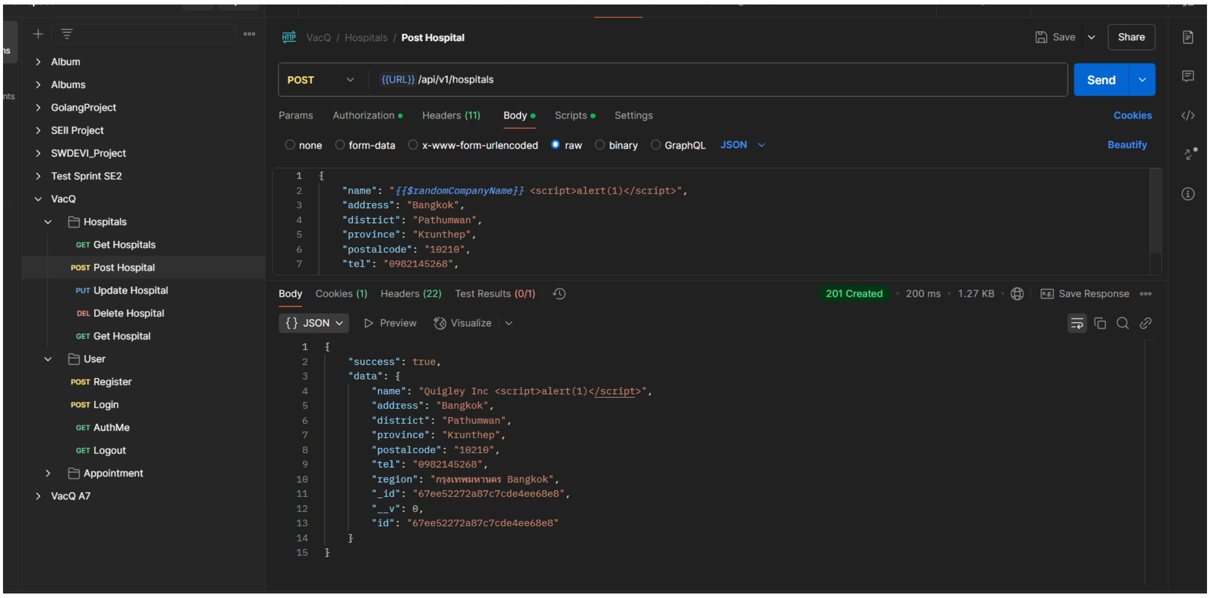
Key	Value
X-Powered-By	Express
Access-Control-Allow-Origin	*
X-RateLimit-Limit	100
X-RateLimit-Remaining	96
Date	Sat, 29 Mar 2025 07:44:41 GMT
X-RateLimit-Reset	1743234864
Content-Type	application/json; charset=utf-8
Content-Length	162

After: Insert Helmet at server.js



Key	Value
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 (ก่อน-หลัง)

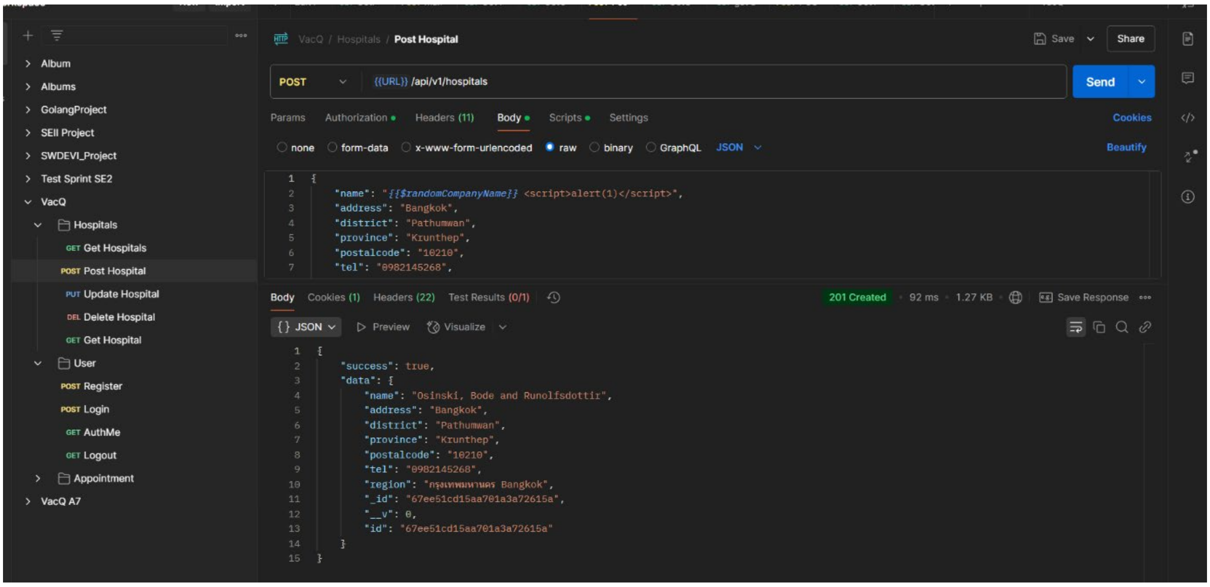


POST {{URL}} /api/v1/hospitals

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

201 Created · 200 ms · 1.27 KB

```
{
    "success": true,
    "data": {
        "name": "Quigley Inc <script>alert(1)</script>",
        "address": "Bangkok",
        "district": "Pathumwan",
        "province": "Krunthep",
        "postalcode": "10210",
        "tel": "0982145268",
        "region": "กรุงเทพมหานคร Bangkok",
        "_id": "67ee52272a87c7cde4ee68e8",
        "__v": 0,
        "id": "67ee52272a87c7cde4ee68e8"
    }
}
```



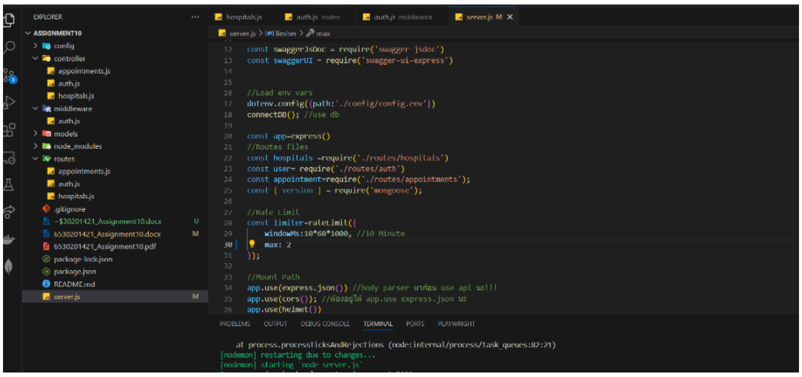
POST {{URL}} /api/v1/hospitals

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

201 Created · 92 ms · 1.27 KB

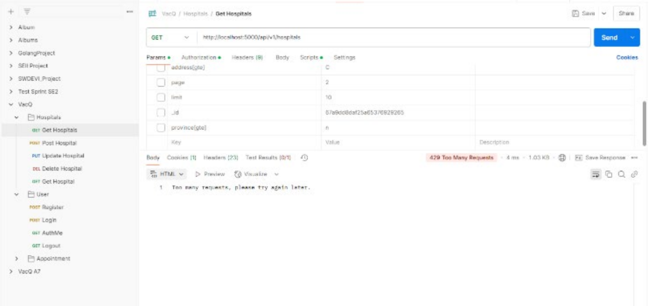
```
{
    "success": true,
    "data": {
        "name": "Osinski, Bode and Runolfsdottir",
        "address": "Bangkok",
        "district": "Pathumwan",
        "province": "Krunthep",
        "postalcode": "10210",
        "tel": "0982145268",
        "region": "กรุงเทพมหานคร Bangkok",
        "_id": "67ee51cd15aa701a3a72615a",
        "__v": 0,
        "id": "67ee51cd15aa701a3a72615a"
    }
}
```

5. Rate Limit



```
const swaggerJsDoc = require('swagger-jsdoc')
const swaggerUI = require('swagger-ui-express')


//Load env vars
dotenv.config({path:'./config/config.env'})
connectDB(); //use db

const app=express()
//Routes files
const hospitals =require('./routes/hospitals')
const user= require('./routes/auth')
const appointment=require('./routes/appointments');
const { version } = require('mongoose');

//Rate Limit
const limiter=rateLimit({
    windowMs:10*60*1000, //10 Minute
    max: 2
});

//Mount Path
app.use(express.json()) //body parser มาก่อน use api นะ!!!
app.use(cors()); //ต้องอยู่ใต้ app.use express.json นะ
app.use(helmet())
```

```
    at process.processTicksAndRejections (node:internal/process/task_queues:82:21)
[nodemon] restarting due to changes...
[nodemon] starting `node server.js`
```



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

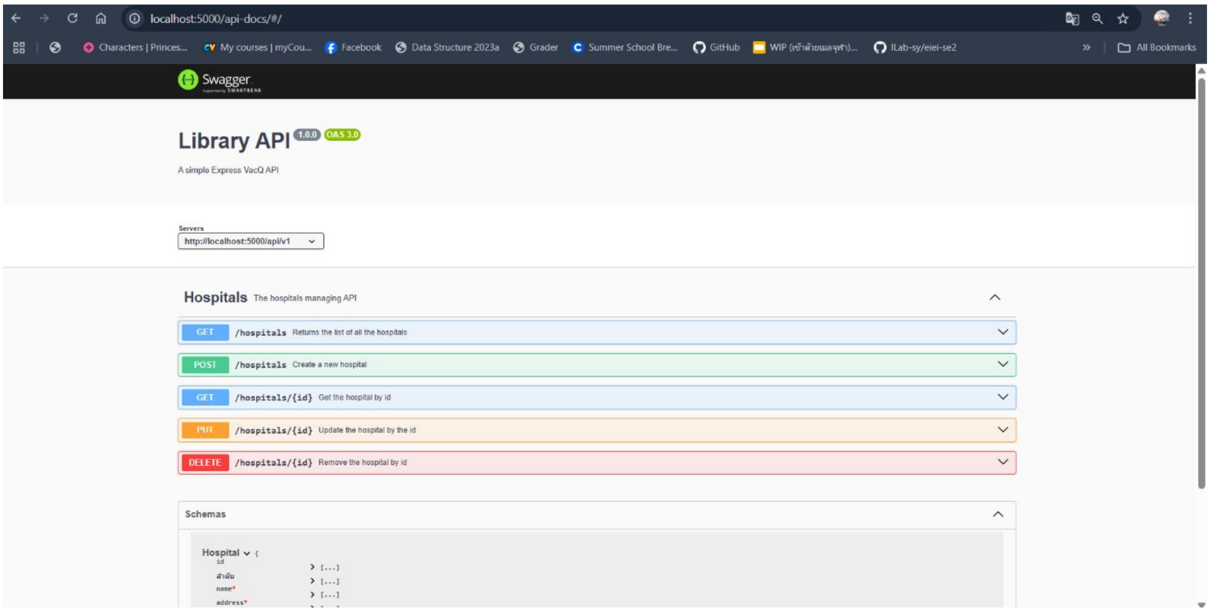
Key	Value	Description
address[gte]	C	
page	2	
limit	10	
_id	67a9dd8daf25a65376929265	
province[gte]	n	

429 Too Many Requests · 4 ms · 1.03 KB

```
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

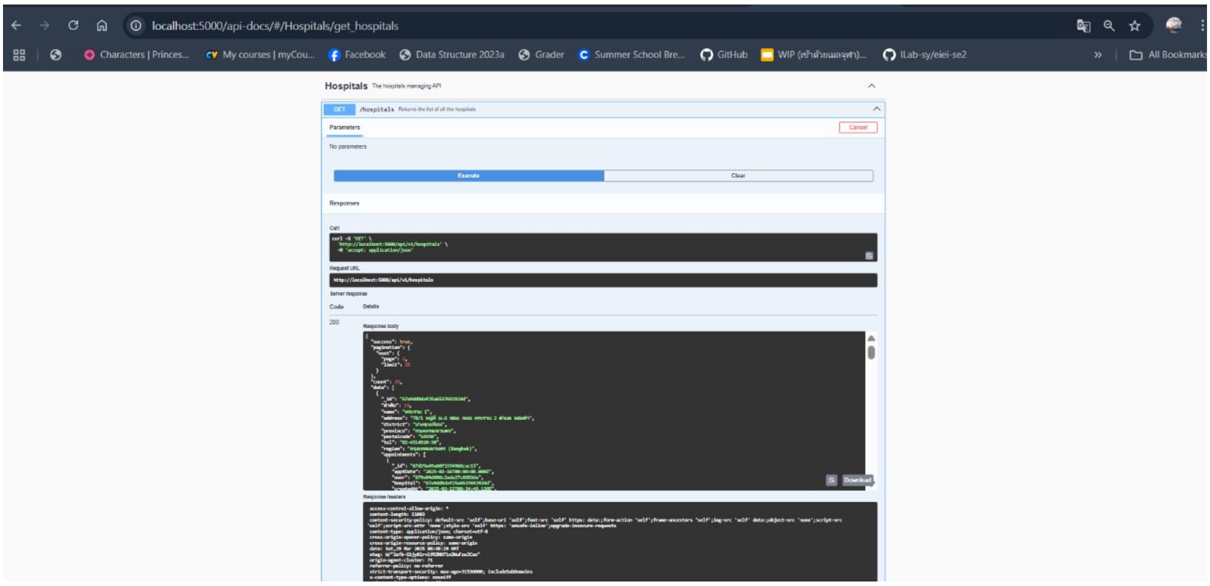
PUT `/hospitals/{id}` Update the hospital by the id

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": "67d25a45a6873374966cac13",
          "apptDate": "2025-02-16T00:00:00.000Z",
          "user": "679e04d606c2ada27c6082da",
          "hospital": "67a9dd8daf25a6537692924d",
          "createdAt": "2025-03-12T00:34:49.120Z",
```

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-GljyB1rvlfR2R071n3WuFzu2Cso"
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