CVE API Documentation

This API provides access to data regarding Common Vulnerabilities and Exposures (CVE). It allows clients to retrieve CVE data based on different search criteria such as ID, year, base score, and last modification time. The responses are structured according to a MongoDB model.

Base URL

All URLs referenced in the documentation have the following base:

https://localhost:6969
where the server is hosted

The API starting point is /cves/list.

Endpoints

1. List All CVEs with Pagination

GET /cves/list?page=:pagenumber&limit=:limitnumber

Description: Retrieves a paginated list of all CVE entries.

Parameters:

- limit: Optional integer to specify the number of records to return per page

Response Codes:

- 200 OK: Successfully retrieved the list.

404 Not Found: No entries found.

2. Get CVE Data by ID

GET /cves/list/:cveId

Description: Retrieves specific CVE data by its ID.

Parameters:

cveId: The ID of the CVE to retrieve.

Response Codes:

200 OK: Successfully retrieved the CVE data.

404 Not Found: CVE not found.

3. Get CVE Data by Year

GET /cves/list/year/:year

Description: Retrieves all CVEs published in a specified year.

Parameters:

year: The year of CVEs to retrieve.

Response Codes:

200 OK: Successfully retrieved the list.

404 Not Found: No entries found for the given year.

4. Get CVE Data by Base Score

GET /cves/list/score/:basescore

Description: Retrieves CVEs based on a specific base score.

Parameters:

basescore: The base score to filter CVEs by.

Response Codes:

200 OK: Successfully retrieved the list.

404 Not Found: No entries found with the specified base score.

5. Get CVE Data by Last Modified Days

GET /cves/list/lastmodified/:days

Description: Retrieves CVEs that have been modified in the last specified number of days.

Parameters:

days: Number of days to check for modifications.

Response Codes:

200 OK: Successfully retrieved the list.

404 Not Found: No entries found modified within the specified days.

Data Model

The data for CVEs is structured as follows in MongoDB:

```
{
    "id": "String",
    "index": "String",
    "sourceIdentifier": "String",
    "published_date": "String",
    "last_modified_date": "String",
"status": "String",
"data": {
    "description": "String",
    "CVSS_Metrics": {
    "severity": "String",
    "baseScore": "String",
    "accessVector": "String",
    "vectorString": "String",
    "accessComplexity": "String",
    "authentication": "String",
    "confidentialityImpact": "String",
    "integrityImpact": "String",
    "availabilityImpact": "String"
    },
    "scores": {
    "exploitabilityScore": "String",
    "impactScore": "String"
    },
    "CPE": [
    {
        "criteria": "String",
        "match_criteria_id": "String",
        "vulnerable": "String"
    }
    ]
}
```

```
}
```

Security and Authentication

Please note that access to the CVE API requires authentication for TLS Certificate Verfication. The server uses a self-signed certificate for secure communication. Clients must have the server's public key to verify the certificate.

openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes is the command you can run in your local folder where the index.js main scriptnfile is placed to generate the public key and certificate.