

API Documentation

1. Requirements

- Retrieve a list of CVEs from the CVE API.
- Paginate the data and allow users to choose how many results are displayed per page (e.g., 10, 50, or 100).
- Allow users to click on a CVE ID to view detailed information about that specific vulnerability.
- Display detailed information such as CVE ID, description, CVSS score, vector strings, and CPE information.

2. Steps to Solve the Problem

Set Up Pagination for CVE List

- Initial API Call: Set up a call to fetch the first page of results, specifying `startIndex` and `resultsPerPage`.
- Results Per Page Selection: Provide options for the user to select how many records to display per page (e.g., 10, 50, 100).
- Next/Previous Page Navigation: Implement buttons to allow users to move between pages. The current page should track state.

Implement Clickable CVE IDs

- Add an event listener to the CVE ID column in the table.
- When the user clicks the CVE ID, navigate to a new page (or section) passing the CVE ID in the URL (e.g., `/cves/CVE-2023-1234`).
- Use the CVE ID from the URL to fetch the detailed data for that specific CVE.

Fetch and Display CVE Details

- On the CVE details page (or section), retrieve the CVE ID from the URL.
- Make an API call to get the details for the specified CVE.
- Display the CVE information, including any metrics like CVSS score, access vector, and impact.

Set Up Filtering

- Add filters to the main CVE list, allowing users to filter by year, CVSS score range, etc.
- Use the filter criteria to modify the API call (e.g., by adding `year` or `cvssScoreMin` parameters).
- Re-render the table based on the filtered results.

3. Developing the API Documentation

Base URL : <https://services.nvd.nist.gov/rest/json/cves/2.0>

All API calls will be made to the base URL: <https://services.nvd.nist.gov/rest/json/cves/2.0>

3.1 Retrieve CVE List : HTTP Method: GET

Parameters:

startIndex: Specifies the starting index for pagination (defaults to 0).

resultsPerPage: Defines the number of CVEs to fetch in one request (defaults to 10).

Example API Call:

GET <https://services.nvd.nist.gov/rest/json/cves/2.0?startIndex=0&resultsPerPage=10>

Returns a paginated list of CVEs.

Includes the CVE ID, Source Identifier, Publish Date, Last Modified Date, Vulnerability Status, and Description

Example :

```
{
  "resultsPerPage": 10,
  "startIndex": 0,
  "totalResults": 1500,
  "vulnerabilities": [
    {
      "cve": {
        "id": "CVE-2023-1234",
        "sourceIdentifier": "Vendor X",
        "published": "2023-01-01T12:00:00.000",
        "lastModified": "2023-02-01T12:00:00.000",
        "vulnStatus": "Active",
        "descriptions": [
          { "value": "Sample description of the vulnerability." }
        ]
      }
    }
  ]
}
```

.Operation :

1. Fetch the first 10 CVEs from the API.
2. Display the results in a table with columns for CVE ID, source, dates, and status.
3. Allow the user to move to the next page using buttons.

3.2. Fetch Details of a Specific CVE

Endpoint: /cves/{cveId}

HTTP Method: GET

Parameters:

cveId: The unique identifier for the specific CVE.

GET <https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2023-1234>

Response:

Returns detailed information about the specified CVE, including:

CVE ID

Description

CVSS Scores

Impact Information

CPE (Common Platform Enumeration) data (software configurations related to the vulnerability)

```
{
  "cve": {
    "id": "CVE-2023-1234",
    "sourceIdentifier": "Vendor X",
    "published": "2023-01-01T12:00:00.000",
    "lastModified": "2023-02-01T12:00:00.000",
    "vulnStatus": "Active",
    "descriptions": [
      { "value": "Detailed vulnerability description." }
    ],
    "metrics": {
      "cvssMetricV2": [
        {
          "cvssData": {
            "baseScore": 7.5,
```

```
        "vectorString": "AV:N/AC:L/Au:N/C:P/I:P/A:P"
      },
      "baseSeverity": "Medium",
      "exploitabilityScore": 8.6,
      "impactScore": 6.4
    }
  ]
}
}
```

Operation :

When a CVE ID is clicked, redirect the user to a detailed view page (e.g., /cves/CVE-2023-1234).

Fetch detailed information from the API and display the CVSS score, description, and additional metrics

Filter CVEs by Criteria

HTTP Method: GET

year: Filter CVEs by the year of publication (e.g., 2023).

cvssScoreMin: Filter by minimum CVSS score.

cvssScoreMax: Filter by maximum CVSS score.

Response :

- Returns a filtered list of CVEs matching the specified criteria.

By implementing the operations for listing, paginating, and fetching detailed CVE information