

# Securein\_Assessment - CVE Data Explorer

## 1. Introduction:

This web application designed to fetch and display detailed information about Common Vulnerabilities and Exposures (CVEs). It provides users with an intuitive interface to explore crucial vulnerability details, including:

- CVE Descriptions (in multiple languages)
- CVSS Metrics (severity, score, vector string)
- CPE Matches (Common Platform Enumeration for affected systems)

The project leverages React.js for the frontend and Node.js (Express.js) for the backend, ensuring a smooth and scalable user experience.

---

## 2. Features:

- ✓ CVE List Display – View a structured table of CVEs with key details:
    - ✦ CVE ID | Identifier | Published Date | Last Modified Date | Status
  - ✓ Detailed CVE Information – Click on a CVE ID to access:
    - ✦ Multi-language descriptions
    - ✦ CVSS v2 metrics (Severity, Score, Vector String)
    - ✦ CPE Matches for affected platforms
  - ✓ Server-Side Pagination & Filtering – Efficiently browse large datasets using backend-optimized pagination and filters.
  - ✓ Periodic Synchronization – Ensures up-to-date CVE information by fetching new data at regular intervals.
  - ✓ Error Handling & Resilience – Displays informative messages for network failures, invalid responses, or missing data.
  - ✓ Minimal & Responsive UI – Clean and adaptable design across all devices.
- 

## 3. Technology Stack:

 Frontend:

- React.js – Component-based UI framework
- CSS – Custom styling for a seamless user experience

 Backend:

- Node.js – JavaScript runtime environment
- Express.js – Lightweight framework for API handling

## API:

The application interacts with a RESTful API for CVE data:

- Local API: <http://localhost:5000/cves/list?page=1&limit=10>
  - External API: <https://services.nvd.nist.gov/rest/json/cves/2.0>
- 

## 4. Installation & Setup:

### ◆ Prerequisites

Ensure you have the following installed:

- Node.js (v14 or higher)
- npm (or yarn) for dependency management

### ◆ Steps to Run Locally

1. Clone the Repository:
2. `git clone https://github.com/yourusername/Securein_Assesment.git`
3. `cd Securein_Assesment`
4. Install Dependencies:
5. `npm install`
6. Start the Application:
7. `npm start`

The app will run at <http://localhost:3000> by default.

8. Ensure API Availability:  
Run the backend API at <http://localhost:5000/cves/list?page=1&limit=10>.
- 

## 5. API Details:

The backend fetches data from NVD's CVE API and structures it for display.

### ◆ Endpoint Example

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

### ◆ Sample API Response:

```
{  
  "resultsPerPage": 1,  
  "startIndex": 0,  
  "totalResults": 1,
```

```
"format": "NVD_CVE",
"version": "2.0",
"timestamp": "2025-01-31T06:16:14.523",
"vulnerabilities": [
  {
    "cve": {
      "id": "CVE-2019-1010218",
      "sourceIdentifier": "josh@bress.net",
      "published": "2019-07-22T18:15:10.917",
      "lastModified": "2024-11-21T04:18:03.857",
      "vulnStatus": "Modified",
      "cveTags": [],
      "descriptions": [
        {
          "lang": "en",
          "value": "Cherokee Webserver Latest Cherokee Web server Upto Version 1.2.103 (Current stable) is affected by: Buffer Overflow - CWE-120. The impact is: Crash. The component is: Main cherokee command. The attack vector is: Overwrite argv[0] to an insane length with execl. The fixed version is: There's no fix yet."
        },
        {
          "lang": "es",
          "value": "El servidor web de Cherokee más reciente de Cherokee Webserver Hasta Versión 1.2.103 (estable actual) está afectado por: Desbordamiento de Búfer - CWE-120. El impacto es: Bloqueo. El componente es: Comando cherokee principal. El vector de ataque es: Sobrescribir argv[0] en una longitud no sana con execl. La versión corregida es: no hay ninguna solución aún."
        }
      ],
      "metrics": {
        "cvssMetricV31": [
          {
            "source": "nvd@nist.gov",
```

```
"type": "Primary",
"cvssData": {
  "version": "3.1",
  "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
  "baseScore": 7.5,
  "baseSeverity": "HIGH",
  "attackVector": "NETWORK",
  "attackComplexity": "LOW",
  "privilegesRequired": "NONE",
  "userInteraction": "NONE",
  "scope": "UNCHANGED",
  "confidentialityImpact": "NONE",
  "integrityImpact": "NONE",
  "availabilityImpact": "HIGH"
},
"exploitabilityScore": 3.9,
"impactScore": 3.6
}
],
"cvssMetricV2": [
  {
    "source": "nvd@nist.gov",
    "type": "Primary",
    "cvssData": {
      "version": "2.0",
      "vectorString": "AV:N/AC:L/Au:N/C:N/I:N/A:P",
      "baseScore": 5,
      "accessVector": "NETWORK",
      "accessComplexity": "LOW",
      "authentication": "NONE",
      "confidentialityImpact": "NONE",
```

```
        "integrityImpact": "NONE",
        "availabilityImpact": "PARTIAL"
    },
    "baseSeverity": "MEDIUM",
    "exploitabilityScore": 10,
    "impactScore": 2.9,
    "acInsufInfo": false,
    "obtainAllPrivilege": false,
    "obtainUserPrivilege": false,
    "obtainOtherPrivilege": false,
    "userInteractionRequired": false
}
]
},
"weaknesses": [
{
    "source": "josh@bress.net",
    "type": "Secondary",
    "description": [
        {
            "lang": "en",
            "value": "CWE-120"
        }
    ]
}
],
{
    "source": "nvd@nist.gov",
    "type": "Primary",
    "description": [
        {
            "lang": "en",
```

```
        "value": "CWE-787"
      }
    ]
  }
],
"configurations": [
  {
    "nodes": [
      {
        "operator": "OR",
        "negate": false,
        "cpeMatch": [
          {
            "vulnerable": true,
            "criteria": "cpe:2.3:a:cherokee-project:cherokee_web_server:*:*:*:*:*:*:*",
            "versionEndIncluding": "1.2.103",
            "matchCriteriaId": "DCE1E311-F9E5-4752-9F51-D5DA78B7BBFA"
          }
        ]
      }
    ]
  }
],
"references": [
  {
    "url": "https://i.imgur.com/PWCCyir.png",
    "source": "josh@bress.net",
    "tags": [
      "Exploit",
      "Third Party Advisory"
    ]
  }
]
```

```
    },
    {
      "url": "https://i.imgur.com/PWCCyir.png",
      "source": "af854a3a-2127-422b-91ae-364da2661108",
      "tags": [
        "Exploit",
        "Third Party Advisory"
      ]
    }
  ]
}
}
```

---

## 6. Application Flow:

- ◆ CVE List Page
    - Displays a table view of vulnerabilities with sorting & filtering.
    - Data is fetched with server-side pagination for performance efficiency.
  - ◆ CVE Details Page
    - Displays expanded details on a selected CVE.
    - Sections include:
      - Descriptions (multi-language support)
      - CVSS Metrics (severity, score, vector string)
      - CPE Matches (affected platforms)
- 

## 7. User Interface:

The app features a minimalist design with clear separation of data:

- ✓ CVE List Table – Paginated and searchable data view
- ✓ CVE Details Panel – Expandable sections for in-depth information
- ✓ Error & Loading States – Informative UI for failed fetches or missing data

---

## 8. Error Handling:

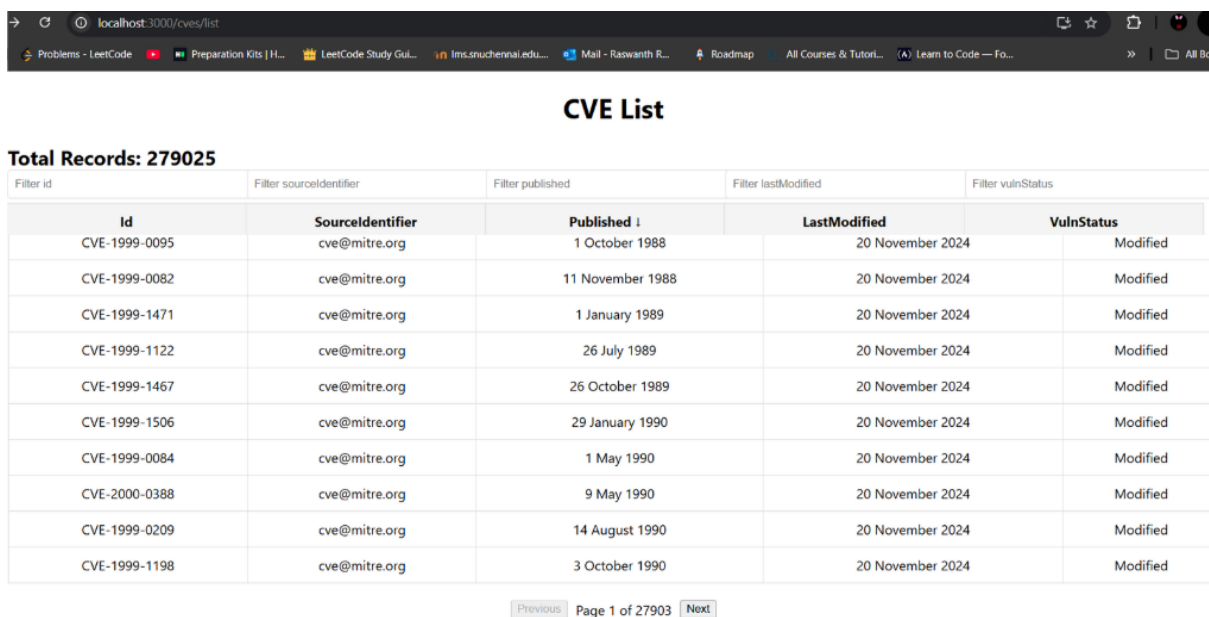
- API Failure → Displays "Failed to fetch data from server."
  - Invalid CVE ID → Shows "CVE not found"
  - Unexpected API Response → Displays "Invalid API response"
- 

## 9. Future Enhancements:

- ◆ Advanced Filtering: Search CVEs by date, severity, and vendor
  - ◆ Authentication & Authorization: Role-based access controls
  - ◆ Enhanced Visualization: Graphs and charts for impact analysis
  - ◆ Multi-source CVE Aggregation: Expand data sources for broader insights
- 

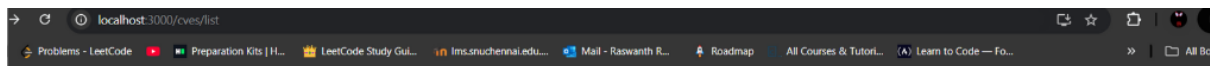
## 10. Output Screenshots:

### CVE List Page



CVE List				
Total Records: 279025				
Filter id	Filter sourceIdentifier	Filter published	Filter lastModified	Filter vulnStatus
Id	SourceIdentifier	Published	LastModified	VulnStatus
CVE-1999-0095	cve@mitre.org	1 October 1988	20 November 2024	Modified
CVE-1999-0082	cve@mitre.org	11 November 1988	20 November 2024	Modified
CVE-1999-1471	cve@mitre.org	1 January 1989	20 November 2024	Modified
CVE-1999-1122	cve@mitre.org	26 July 1989	20 November 2024	Modified
CVE-1999-1467	cve@mitre.org	26 October 1989	20 November 2024	Modified
CVE-1999-1506	cve@mitre.org	29 January 1990	20 November 2024	Modified
CVE-1999-0084	cve@mitre.org	1 May 1990	20 November 2024	Modified
CVE-2000-0388	cve@mitre.org	9 May 1990	20 November 2024	Modified
CVE-1999-0209	cve@mitre.org	14 August 1990	20 November 2024	Modified
CVE-1999-1198	cve@mitre.org	3 October 1990	20 November 2024	Modified
Previous Page 1 of 27903 Next				





## CVE List

Total Records: 279025

Filter id	Filter sourceIdentifier	Filter published	Filter lastModified	Filter vulnStatus
Id	SourceIdentifier	Published	LastModified	VulnStatus
CVE-1999-0095	cve@mitre.org	1 October 1988	20 November 2024	Modified
CVE-1999-0082	cve@mitre.org	11 November 1988	20 November 2024	Modified
CVE-1999-1471	cve@mitre.org	1 January 1989	20 November 2024	Modified
CVE-1999-1122	cve@mitre.org	26 July 1989	20 November 2024	Modified
CVE-1999-1467	cve@mitre.org	26 October 1989	20 November 2024	Modified
CVE-1999-1506	cve@mitre.org	29 January 1990	20 November 2024	Modified
CVE-1999-0084	cve@mitre.org	1 May 1990	20 November 2024	Modified
CVE-2000-0388	cve@mitre.org	9 May 1990	20 November 2024	Modified
CVE-1999-0209	cve@mitre.org	14 August 1990	20 November 2024	Modified
CVE-1999-1198	cve@mitre.org	3 October 1990	20 November 2024	Modified

Previous Page 1 of 27903 Next

## CVE Details Page



### CVE-1999-0095

#### Description:

- **en:** The debug command in Sendmail is enabled, allowing attackers to execute commands as root.
- **es:** El comando de depuración de Sendmail está activado, permitiendo a atacantes ejecutar comandos como root.

#### CVSS V2 Metrics:

Severity: HIGH Score: 10

Vector String: AV:N/ACL/Au:N/C/C/I/C/A/C

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
NETWORK	LOW	NONE	COMPLETE	COMPLETE	COMPLETE

#### Scores:

Exploitability Score: 10

Impact Score: 10

#### CPE:

Criteria	Match Criteria ID	Vulnerable
cpe:2.3:a:eric_allman:sendmail:5.58:*:*:*:*:*	1D07F493-9C8D-44A4-8652-F28B46CBA27C	Yes

## 11. Contributing

- ◆ Fork the repository to make changes.
- ◆ Create a new branch for features or fixes.
- ◆ Commit changes with meaningful messages.
- ◆ Push to your fork and submit a Pull Request.

