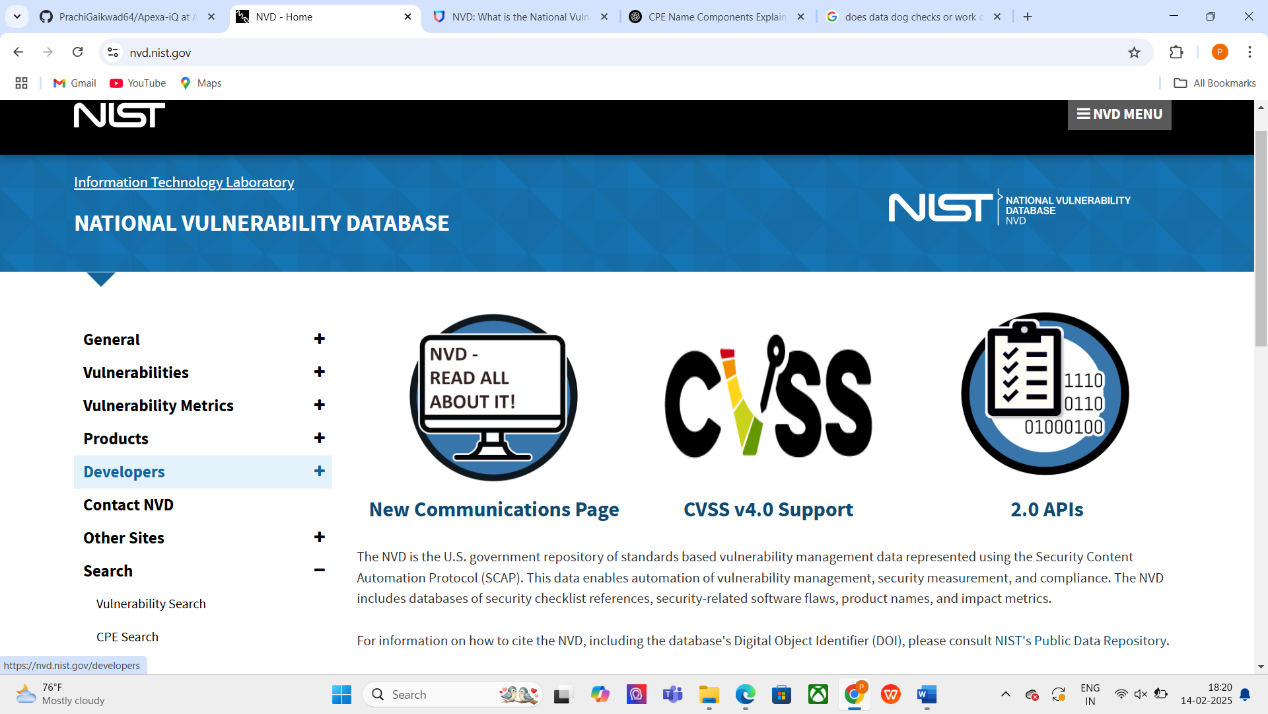
**Day 10 Assignment**

**What is NVD?**

* The National Vulnerability Database (NVD) is a foundational cybersecurity resource that provides detailed information on vulnerabilities across a wide range of software and hardware.
* Maintained by the National Institute of Standards and Technology (NIST), the NVD serves as the U.S. government repository of standards-based vulnerability management data.
* The NVD catalogues vulnerabilities based on the Common Vulnerabilities and Exposures (CVE) naming standard.
* A key benefit of the NVD is enabling near real-time vulnerability tracking. The NVD issues updates as new vulnerabilities are discovered and assigned CVE IDs.
* NVD is having option for searching we can search for
* Vulnerability Search
* CPE Search
* The NVD website provides a robust search engine to navigate its entire catalogue of vulnerability data efficiently.



**Common Platform Enumeration (CPE):**

* Common Platform Enumeration (CPE) is a structured [naming scheme](https://en.wikipedia.org/wiki/Naming_scheme) for information technology systems, software, and packages.
* One CPE can have numerous CVEs.

**CPE Name Components:**

1. **Part:** Tells about what type of product it is hardware, software or Operating System.
2. **Vendor:** Gives Information about the vendor ex. Microsoft
3. **Product:** Tells about the product.
4. **Version**
5. **Update**
6. **Software Edition**
7. **Target Hardware**

It consists of  **components**, separated by colons (:):

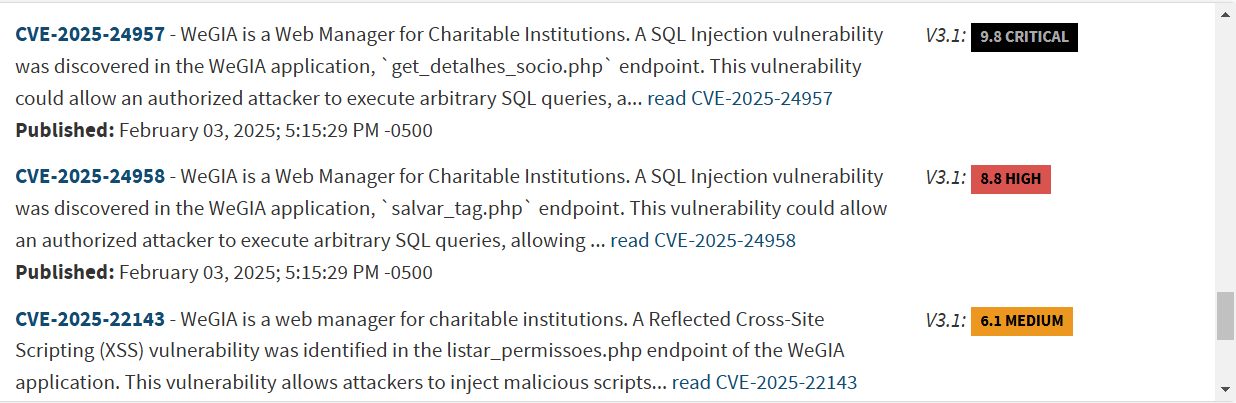
|  |  |  |
| --- | --- | --- |
| **Component** | **Description** | **Example** |
| **cpe** | Constant prefix | cpe |
| **Version (2.3)** | CPE format version | 2.3 |
| **Part** | Type of entity (a, o, h) | a (application) |
| **Vendor** | Software/hardware vendor | microsoft |
| **Product** | Product name | office |
| **Version** | Version number | 2016 |
| **Update** | Update/patch information | sp1 |
| **Edition** | Specific edition (enterprise, professional, etc.) | \* (any) |
| **Language** | Software language | \* (any) |
| **SW Edition** | Software edition (e.g., home, pro) | \* (any) |
| **Target SW** | Target software (if applicable) | \* (any) |
| **Target HW** | Target hardware (if applicable) | \* (any) |

**Common Vulnerabilities and Exposures (CVEs):**

* CVE identifiers form the foundation of NVD data. CVEs provide reference points that universally identify specific vulnerabilities and exposures.
* CVE entries contain basic identifying information like a descriptive name, the impacted software or hardware, version numbers, acknowledgments, and disclosure details.
* By using CVE IDs, the NVD links together vulnerability information from various sources into single records. This stitches together a complete narrative around each vulnerability.

**Common Vulnerabilities Scoring System (CVSS): Gauging vulnerability severity**

* The NVD leverages the Common Vulnerability Scoring System (CVSS) to assign severity scores to vulnerabilities.
* CVSS provides standardized and transparent ratings of vulnerability impact.
* These scores range from 0 to 10.
* NVD's CVSS data enables security teams to intelligently prioritize which vulnerabilities require immediate action.
* Flaws with higher CVSS ratings represent bigger risks.
* Severity can range from Low to Medium ,High and Also Critical.



**NVD and CVE: Understanding the connection**

* The NVD relies heavily on the Common Vulnerabilities and Exposures (CVE) standard in presenting vulnerability information.
* CVE serves as a dictionary of publicly known cybersecurity flaws.
* Each CVE entry provides a standardized name that identifies important attributes of a vulnerability.
* The CVE ID links the vulnerability to descriptive details and remediation guidance contained in the NVD entry.
* By leveraging CVE IDs, the NVD structures vulnerability data in a machine-readable format.
* This enables automation of vulnerability management powered by NVD's comprehensive CVE information.