Module 5: Vulnerability Analysis

Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. By default, **Windows 11** machine is selected, click Ctrl+Alt+Delete to activate the machine and login with **Admin**/**Pa$$w0rd**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

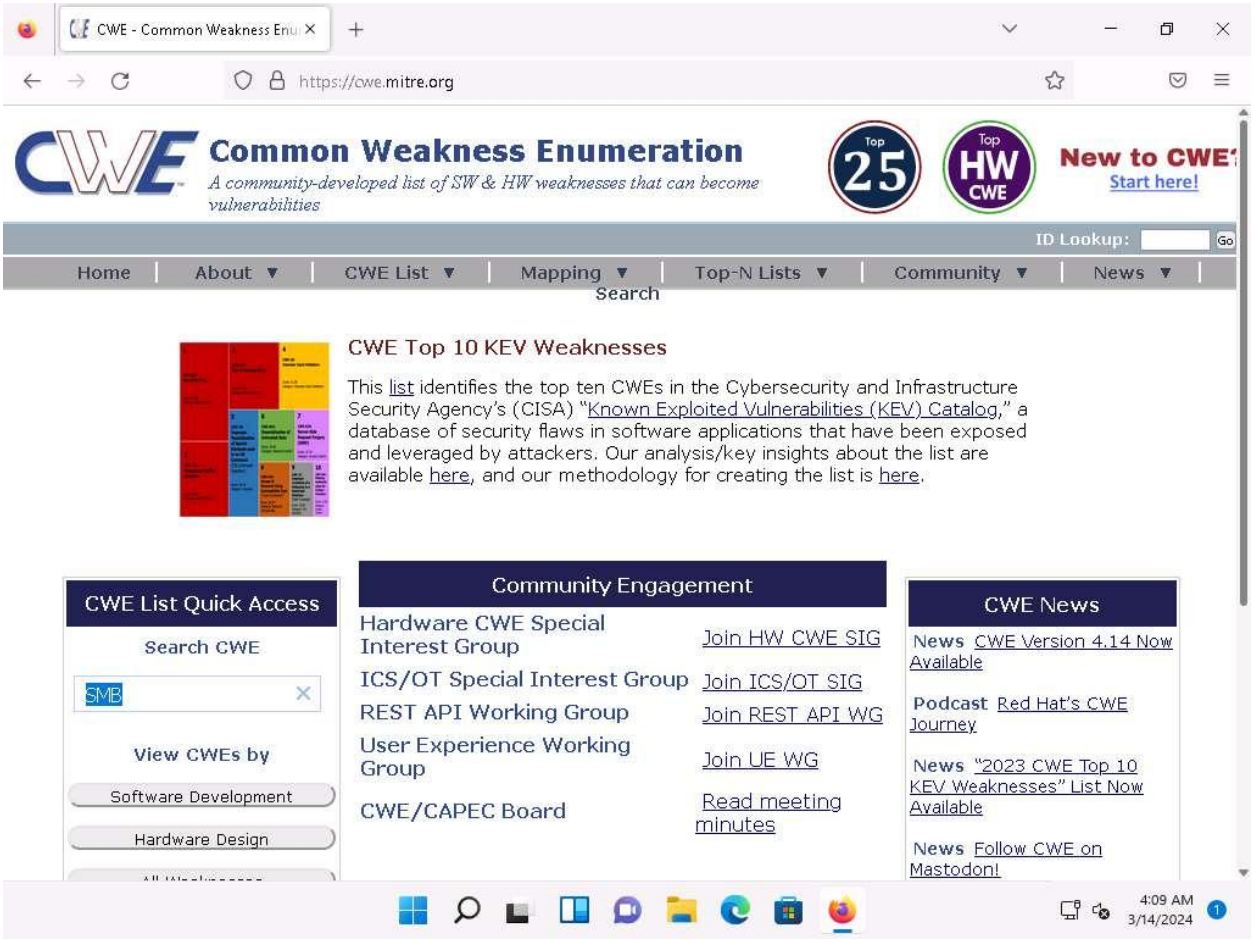
2. Launch any web browser, and go to **https://cwe.mitre.org/** website (here, we are using **Mozilla Firefox**).

If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click start browsing to finish viewing the information.

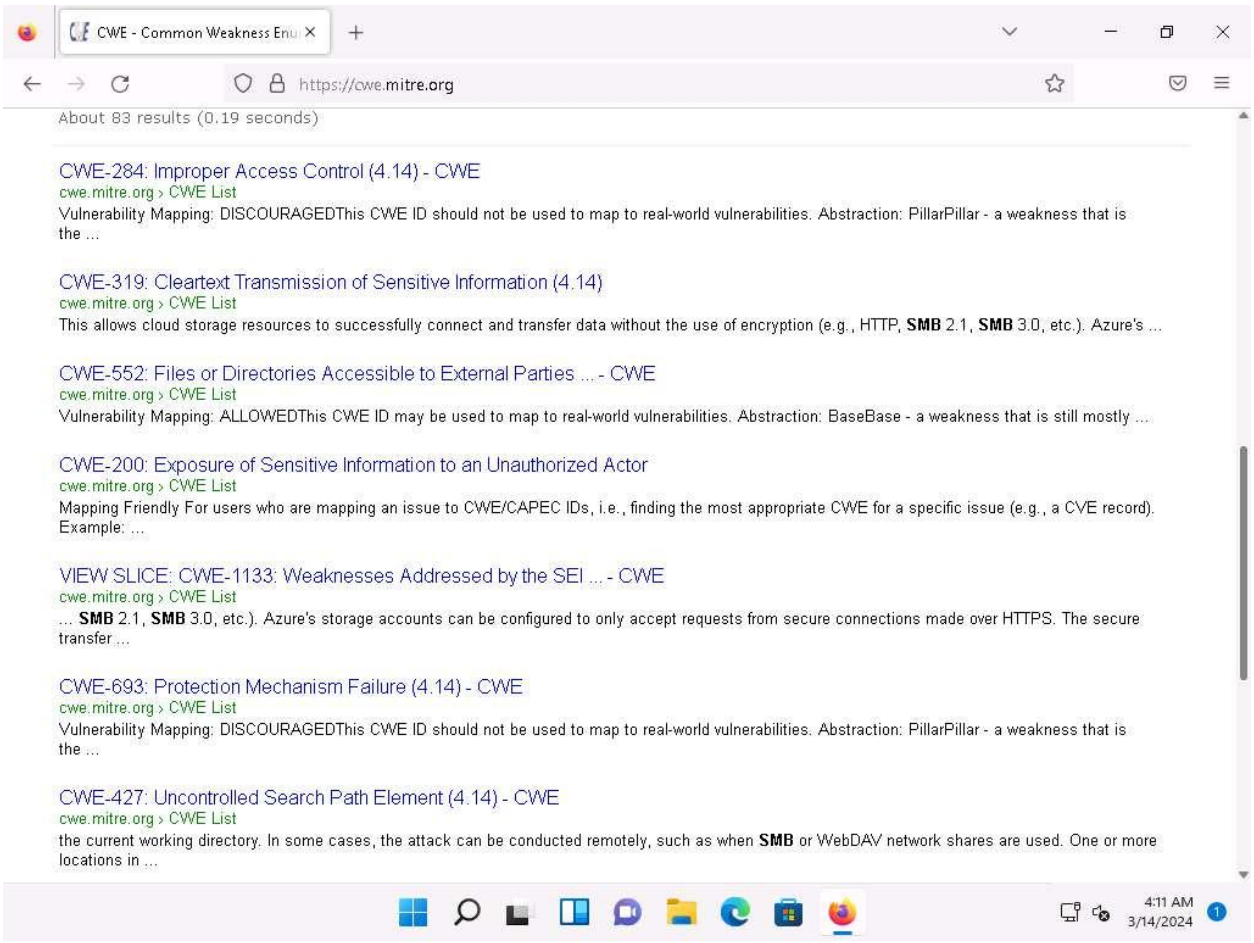
3. **CWE** website appears. Navigate to **Search** tab, in the **Google Custom Search** under **CWE List Quick Access** section and search for **SMB** in the search field.

Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

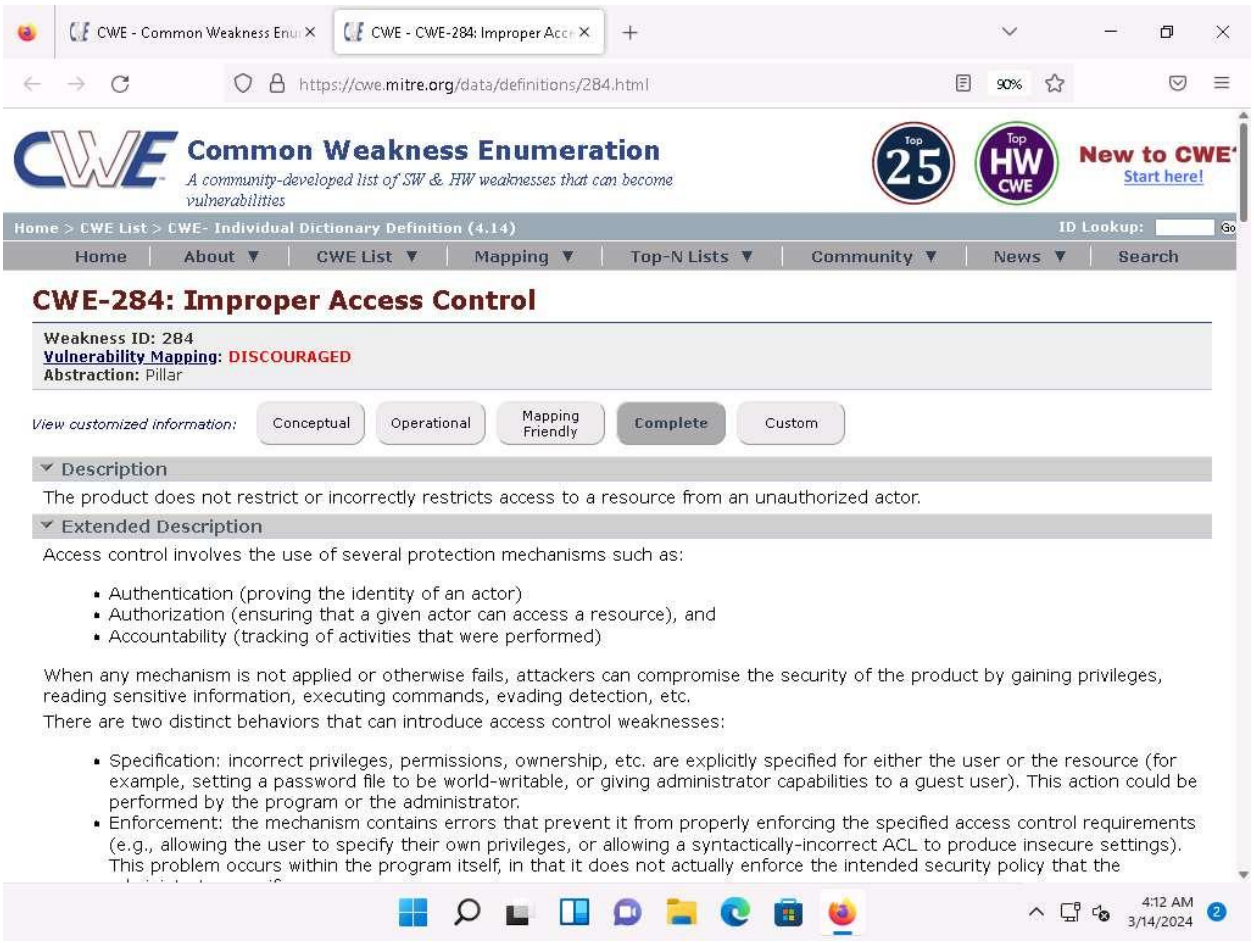


4. The search results appear, scroll-down to view the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

The search results might differ when you perform this task

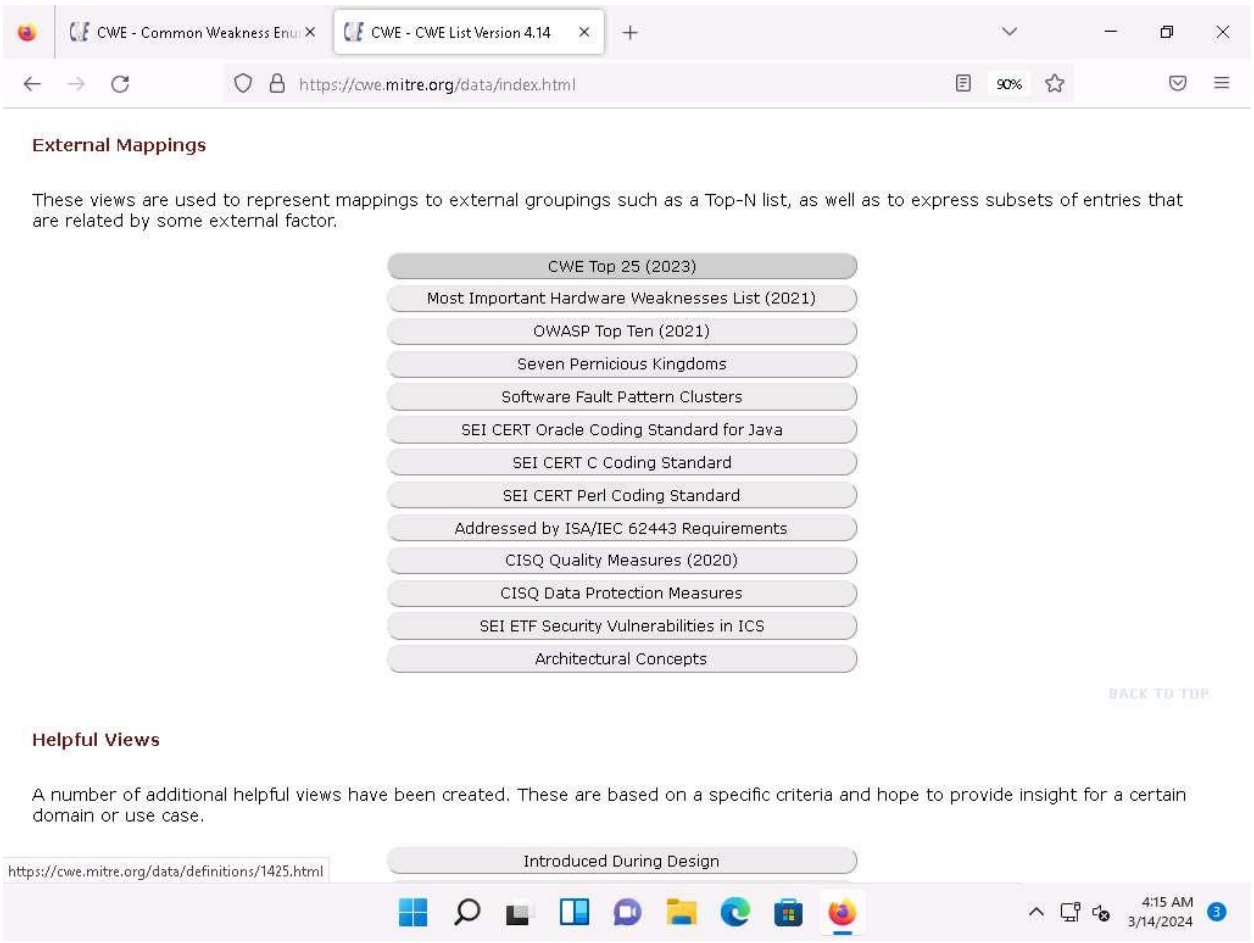


5. Now, click any link (here, **CWE-284**) to view detailed information about the vulnerability.



6. Similarly, you can click on other vulnerabilities and view detailed information.
7. Now, navigate to the **CWE List** tab. **CWE List Version** will be displayed. Scroll down, and under the **External Mappings** section, select **CWE Top 25 (2023)**.

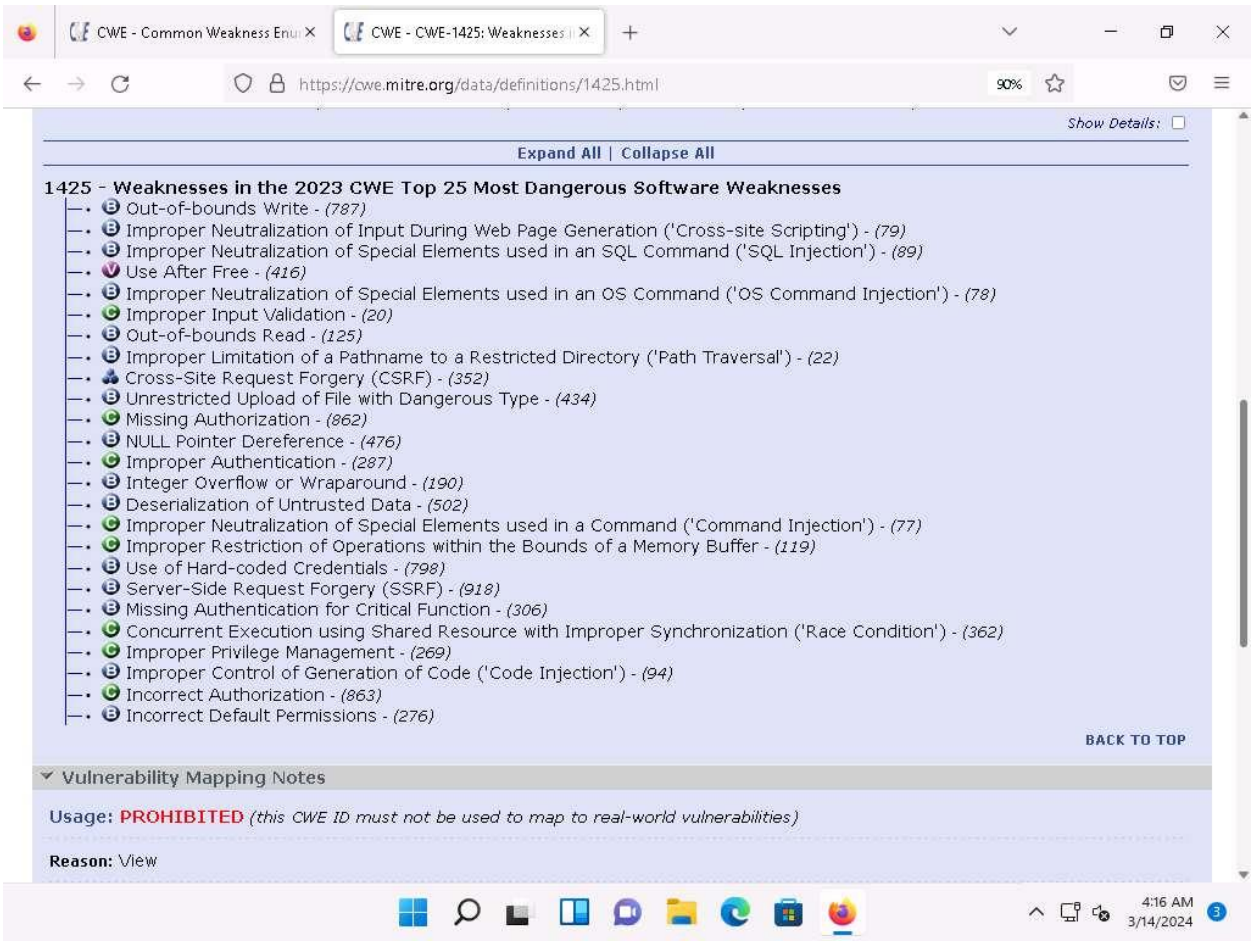
The result might differ when you perform this task.



8. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can check each weakness to view detailed information on it.

This information can be used to exploit the vulnerabilities in the software and further launch attacks.

The result showing publishing year might differ when you perform this task.



9. Similarly, you can go back to the CWE website and explore other options, as well.
10. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.
11. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
12. Close all open windows and document all the acquired information.

Question 5.1.1.1

Search the Common Weakness Enumeration (CWE) list and find the name of the vulnerability with the CWE ID 591.

Question 5.1.1.2

Search the Common Weakness Enumeration (CWE) list and find the top weakness in the list "Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weakness."