

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).

The screenshot shows the homepage of the CWE website. At the top, there's a navigation bar with links for Home, About, CWE List, Mapping, Top-N Lists, Community, and News. Below the navigation is a banner for the 'Top 25 HW CWE' with a link to 'Start here!'. A search bar labeled 'ID Lookup:' is present. The main content area features a large graphic titled 'CWE Top 10 KEV Weaknesses' with a list of ten items. To the left, a sidebar titled 'CWE List Quick Access' includes a search bar with 'SMB' typed in, and buttons for 'View CWEs by Software Development' and 'Hardware Design'. On the right, there's a 'Community Engagement' section with links to various working groups and a 'CWE News' section with news items about version 4.14 and the 2023 Top 10 KEV Weaknesses.

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

The screenshot shows a Microsoft Edge browser window with the following details:

- Title Bar:** CWE - Common Weakness Enumeration
- Address Bar:** https://cwe.mitre.org
- Search Query:** About 83 results (0.19 seconds)
- First Result:** CWE-284: Improper Access Control (4.14) - CWE
cwe.mitre.org > CWE List
Vulnerability Mapping: DISCOURAGED This CWE ID should not be used to map to real-world vulnerabilities. Abstraction: PillarPillar - a weakness that is the ...
- Second Result:** CWE-319: Cleartext Transmission of Sensitive Information (4.14)
cwe.mitre.org > CWE List
This allows cloud storage resources to successfully connect and transfer data without the use of encryption (e.g., HTTP, **SMB** 2.1, **SMB** 3.0, etc.). Azure's ...
- Third Result:** CWE-552: Files or Directories Accessible to External Parties ... - CWE
cwe.mitre.org > CWE List
Vulnerability Mapping: ALLOWED This CWE ID may be used to map to real-world vulnerabilities. Abstraction: BaseBase - a weakness that is still mostly ...
- Fourth Result:** CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
cwe.mitre.org > CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...
- Fifth Result:** VIEW SLICE: CWE-1133: Weaknesses Addressed by the SEI ... - CWE
cwe.mitre.org > CWE List
... **SMB** 2.1, **SMB** 3.0, etc.). Azure's storage accounts can be configured to only accept requests from secure connections made over HTTPS. The secure transfer ...
- Sixth Result:** CWE-693: Protection Mechanism Failure (4.14) - CWE
cwe.mitre.org > CWE List
Vulnerability Mapping: DISCOURAGED This CWE ID should not be used to map to real-world vulnerabilities. Abstraction: PillarPillar - a weakness that is the ...
- Seventh Result:** CWE-427: Uncontrolled Search Path Element (4.14) - CWE
cwe.mitre.org > CWE List
the current working directory. In some cases, the attack can be conducted remotely, such as when **SMB** or WebDAV network shares are used. One or more locations in ...

The browser interface includes standard controls like back, forward, and search, along with a taskbar at the bottom featuring icons for File Explorer, Task View, Start, Taskbar settings, and a clock showing 4:11 AM on 3/14/2024.

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

The screenshot shows a web browser window displaying the CWE-284: Improper Access Control page on the Common Weakness Enumeration (CWE) website. The URL in the address bar is <https://cwe.mitre.org/data/definitions/284.html>. The page title is "CWE-284: Improper Access Control". Key sections include:

- Weakness ID:** 284
- Vulnerability Mapping:** DISCOURAGED
- Abstraction:** Pillar
- Description:** The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.
- Extended Description:** Access control involves the use of several protection mechanisms such as:
 - Authentication (proving the identity of an actor)
 - Authorization (ensuring that a given actor can access a resource), and
 - Accountability (tracking of activities that were performed)When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.
- Behaviors:** There are two distinct behaviors that can introduce access control weaknesses:
 - Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.
 - Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the

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.

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor.

CWE Top 25 (2023)

Most Important Hardware Weaknesses List (2021)

OWASP Top Ten (2021)

Seven Pernicious Kingdoms

Software Fault Pattern Clusters

SEI CERT Oracle Coding Standard for Java

SEI CERT C Coding Standard

SEI CERT Perl Coding Standard

Addressed by ISA/IEC 62443 Requirements

CISQ Quality Measures (2020)

CISQ Data Protection Measures

SEI ETF Security Vulnerabilities in ICS

Architectural Concepts

BACK TO TOP

Helpful Views

A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight for a certain domain or use case.

Introduced During Design

https://cwe.mitre.org/data/definitions/1425.html

4:15 AM 3/14/2024

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.

1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

- ⚡ Out-of-bounds Write - (787)
- ⚡ Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - (79)
- ⚡ Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - (89)
- 🛡 Use After Free - (416)
- ⚡ Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - (78)
- ⚡ Improper Input Validation - (20)
- ⚡ Out-of-bounds Read - (125)
- ⚡ Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - (22)
- ⚡ Cross-Site Request Forgery (CSRF) - (352)
- ⚡ Unrestricted Upload of File with Dangerous Type - (434)
- ⚡ Missing Authorization - (862)
- ⚡ NULL Pointer Dereference - (476)
- ⚡ Improper Authentication - (287)
- ⚡ Integer Overflow or Wraparound - (190)
- ⚡ Deserialization of Untrusted Data - (502)
- ⚡ Improper Neutralization of Special Elements used in a Command ('Command Injection') - (77)
- ⚡ Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)
- ⚡ Use of Hard-coded Credentials - (798)
- ⚡ Server-Side Request Forgery (SSRF) - (918)
- ⚡ Missing Authentication for Critical Function - (306)
- ⚡ Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - (362)
- ⚡ Improper Privilege Management - (269)
- ⚡ Improper Control of Generation of Code ('Code Injection') - (94)
- ⚡ Incorrect Authorization - (863)
- ⚡ Incorrect Default Permissions - (276)

BACK TO TOP

▼ Vulnerability Mapping Notes

Usage: **PROHIBITED** (this CWE ID must not be used to map to real-world vulnerabilities)

Reason: View

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."