Vulnerability Classification

Imagine a world where all vulnerabilities were treated equally – it would be utter chaos! That's why we need a systematic approach to classify vulnerabilities based on their severity, impact, and other critical factors. By organizing vulnerabilities into distinct categories, we can better understand their potential consequences and allocate our resources accordingly.

Classification of vulnerabilities are usually done under these three categories or frameworks.

- **Common Vulnerabilities and Exposures (CVE):** CVE provides a unique identifier for publicly known cybersecurity vulnerabilities. It helps standardize the naming and tracking of vulnerabilities across different databases and tools. CVE identifiers are widely used in the industry to refer to specific vulnerabilities.

In simpler terms, think of a CVE as a serial number or barcode for a specific vulnerability. Just like how products in a store have unique barcodes, each publicly known security vulnerability gets its own CVE identifier or "barcode" number.

The purpose of CVEs is to provide a centralized database where organizations, security researchers, and vendors can easily reference and share details about vulnerabilities they've discovered. This helps raise awareness and allows everyone to understand the nature of the vulnerability, which systems or products are affected, and what steps can be taken to fix or mitigate the issue.

For example, if a major software company like Microsoft discovers a security hole in one of their products, they would report it to the CVE program and get assigned a unique CVE number, like CVE-2022-12345. This CVE number, along with details about the vulnerability, would then be published in the CVE database for the world to see and take appropriate action.

Next we have is CWE.

- **Common Weakness Enumeration (CWE):** CWE is a taxonomy or dictionary of software and hardware weakness types that can lead to vulnerabilities. It provides a common language and structure for identifying, mitigating, and preventing weaknesses and vulnerabilities in software. CWE categorizes vulnerabilities into different types like design errors, input validation errors, etc.

In simpler terms, CWE is like a dictionary or encyclopedia that lists and defines various kinds of coding errors, design flaws, or configuration mistakes that can make a computer system or application vulnerable to cyber attacks.

Each weakness is assigned a unique CWE identifier number and a descriptive name. For example:

- **CWE-79 is "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')"**
- **CWE-89 is "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')"**
- **CWE-200 is "Exposure of Sensitive Information to an Unauthorized Actor"**

By having a standardized list of these common weaknesses, it becomes easier for developers, security professionals, and tool vendors to communicate about potential risks, prioritize which issues need to be addressed, and implement effective countermeasures or mitigations.

At last, we have CVSS

Common Vulnerability Scoring System (CVSS): CVSS is an open framework for calculating the severity of computer system vulnerabilities. It assigns a numerical score from 0 to 10 based on metrics like attack vector, complexity, privileges required, etc. This score helps organizations prioritize vulnerabilities based on their potential impact.

In simple terms, CVSS provides a numerical score from 0 to 10 that indicates how serious or severe a particular security vulnerability is. The higher the score, the more severe and critical the vulnerability.This scoring system takes into account various factors or metrics about the vulnerability, such as:

- How easy or difficult it is to exploit the vulnerability (attack complexity)
- What kind of access or privileges are required to exploit it
- What impact the vulnerability could have if exploited (e.g. allowing data theft, system crashes, etc.)
- How the vulnerability spreads or impacts other connected systems

By considering these different characteristics, CVSS assigns a standardized severity score to each vulnerability. This allows organizations and security professionals to quickly understand and compare the relative severity of different vulnerabilities they may be facing.
