Laud Mills

Part A: This task will give you better understanding of impact of the website vulnerabilities in real world using CVE – MITRE.

Follow the steps:

1. Click on the URL : <https://cve.mitre.org/cve/search_cve_list.html>
2. Write down the name of the vulnerability that you want to explore in the search box. (Use the following list of vulnerabilities)
3. After that answer the following questions.

List of Vulnerabilities:

* SQL Injection
* Buffer Overflow
* Broken Authentication
* Cross-site scripting
* Cross-Site Request Forgery
* Phishing
* Path traversal attack
* Distributed Denial-of-Service (DDoS)
* Man In the Middle Attack
* Brute Force Attack

Questions:

1. What is the full meaning of CVE and NVD?

Common Vulnerabilities and Exposures

National Vulnerability Database

1. Why CVE is important?

It is a standard for tagging and tracking vulnerabilities. It provides industry professionals and businesses with a universal method of identifying security vulnerabilities and tracking them over time.

1. Find out the total number of CVE records for each of the 10 vulnerabilities/attacks mentioned above.

SQL Injection 15588 records

Buffer Overflow 16380 records

Broken Authentication 75 records

Cross-site scripting 29669 records

Cross-Site Request Forgery 5234 records

Phishing 7659 records

Path traversal attack 2575 records

Distributed Denial-of-Service (DDoS) 166 records

Man In the Middle Attack 3203 records

Brute Force Attack 876 records

1. Find out the base score and severity of first CVE record of all the vulnerabilities listed above according to version 3.x and version 2.0 and fill the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of the**  **Vulnerability** | **Number of CVE record** | **Base Score &**  **Severity 2.0** | **Base Score &**  **Severity Version 3.X** |
|  |
| SQL Injection | 15608 | 7.5 high severity | 9.8 critical severity |  |
| Buffer Overflow | 16391 | 9.3 critical severity | 9.5 critical severity |  |
| Broken Authentication | 75 | 8.5 high severity | 9.8 critical severity |  |
| Cross-site scripting | 29749 | 6.1 medium severity | 6.1 medium severity |  |
| Cross-Site Request Forgery | 5246 | 6.8 medium severity | 7.3 high severity |  |
| Phishing | 765 | 6.4 medium severity | 7.5 high severity |  |
| Path traversal attack | 2577 | 7.5 high severity | 7.5 high severity |  |
| Distributed Denial-of-Service (DDoS) | 166 | 7.8 high severity | 7.8 high severity |  |
| Man In the Middle Attack | 3203 | 7.5 high severity | 7.8 high severity |  |
| Brute Force Attack | 876 | 7.0 high severity | 7.5 high severity |  |

1. Find out the total number of CVE recorded for year 2000, 2001, 2002 and 2003 for one of the vulnerabilities of your choice from the given list.

Year: 2000 2001 2002 2003

SQL Injection Records 1236 1482 2391 1599

Part B: Privacy and personal data

1. Choose any one of the social/professional websites (such as Facebook, Twitter, LinkedIn) and check what personal information you are able to access? How can identity thieves take advantage of social networking users to steal personal information?

On LinkedIn, a user's public profile often contains the following personal information:

Full Name, Professional Title/Current Job, Work Experience, Education such as schools attended, degrees obtained, and years of attendance, skills & Endorsements, Recommendations, Connections, Contact Information like email address or other contact details, often shared for networking, Profile Picture etc.

Fraudsters might create fake job offers or opportunities using information copied from profiles. They might ask for a fee upfront to secure a job or for other personal details under the guise of employment verification. They can also gather enough information from a LinkedIn profile to trick a user into revealing more sensitive details. For instance, if they know your workplace, job responsibilities, and colleagues, they can convincingly impersonate someone from HR or IT support, asking for login credentials or other sensitive data.

1. What type of personal information could an attacker obtain from a user profile on LinkedIn.com that he or she could use for identity theft?

Full Name, Professional Title and Current Job, Work Experience, Education, Contact Information, Connections, Profile Picture just to mention a few.

1. What security feature you should always look for in any website that will ask for personal information to share with others?

First of all look ensure that the website is secured with SSL/TLS encryption (HTTPS), allows two factor authentication for the collection of personal information, has privacy and terms of service policy and strong password requirements.