Lab 6 - CVE and CVSS

1. *Consider two vulnerabilities with the following vectors:*
    a. *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H*
    b. *CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N*

   Discuss which one is riskier and why. Provide sound arguments supporting your choice.

   If we compare both vectors field by field, we can get the following ideas:
   - Vector A has a network attack vector, instead of an adjacent one as vector B does, which makes the vulnerability riskier by giving the attacker the possibility of performing the attack from any point of the Internet.
   - Vector B attack's complexity is low. Compared to the high attack complexity of vector A, it should make the attack easier to perform.
   - Vector A' vulnerability is highly affecting the availability of the component compared to vector B, as it does not affect availability at all, thus, making the vulnerability riskier.
   - All of the other fields of the vectors are the same between both of them.

   Taking into consideration these observations, I would say **vector A poses a higher threat**, as the attack can be performed from any point of the internet, meaning that a higher number of people have access to the vulnerable component, as they do not need to be in the same local network as the component, even though the attack complexity is lower in vector B, I think that it is riskier by being available from any point in the Internet. We also need to take into account that vector A affects the availability of the component highly, meaning that there is a total loss of availability of the component or service, meanwhile an attack on vector B's vulnerability would not affect the availability of the component.

2. *Use cvedetails.com to browse through SQL injection vulnerabilities (select "Vulnerabilities by type") for different years.*
    a. *What is the most common CVSS score for this type of vulnerability? What is the reason?*

       The most common score is by far 7.5 (it comprehends 137 out of the 196 pages listed). The reason is that these attacks are able to be performed from anywhere on the Internet normally and have a low complexity, as well as not requiring elevated privileges and having partial consequences in the confidentiality, integrity and availability of the system.

    b. *Find two SQL injection vulnerabilities with a CVSS score different from the most common (one higher and one lower) and explain why the score is different in these cases.*

- CVE-2022-24260. This vulnerability has a CVSS score of 10.0. The reason the score is higher is that, compared to the vulnerabilities with a CVSS score of 7.5, they compromise the availability, confidentiality and integrity of the component totally.
- CVE-2015-7448. With a score of 6.5, this vulnerability has a lower score compared to the most common score ones because the authentication required seems to be higher, or is not known. Other vulnerabilities with this or a lower score have a higher attack complexity to the most common case.