※ Password Vulnerabilities:

Password vulnerabilities are weaknesses or flaws in the way passwords are created, managed or used, which can be exploited by attackers to gain unauthorized access to accounts, systems or data. These vulnerabilities can be broadly categorized as follows:

1) Weak Passwords:

- Short and simple Passwords:
Short passwords or those that consist of common words or phrases are easier for attackers to guess or crack using brute force methods.

- Lack of Complexity:
Passwords that dont include a mix of uppercase letters, lowercase letters, numbers, and special characters are more susceptible to attacks.

- Dictionary Words:
Passwords that use easily guessable dictionary words, even with substitutions like "P@ssw0rd", can be cracked.

- Common Passwords:
Using commonly used passwords like "123456", "password", or "admin" is a major vulnerability.

2. Password Storage:

- Storing passwords in an insecure manner, like plain text or weakly hashed, leaves them vulnerable to data breaches.

3. Password Reuse:

- Reusing the same password across multiple accounts or services can lead to widespread security issues. If one account is compromised, all accounts using the same password are at risk.

4. No Multifactor Authentication (MFA):

- Not enabling MFA is a significant ~~vul~~ vulnerability. Even if an attacker guesses or steals your passwords, MFA adds an extra layer of security.

5. Social Engineering:

- Attackers may use psychological manipulation to trick individuals into revealing their passwords, often through tactics like phishing emails or phone calls.

6. No Account Lockout Policies:

- Failing to implement account lockout policies that temporarily disable an account after ~~mai~~ multiple failed login attempts can expose the account to brute force attacks.

7. Inadequate Password Recovery:

- Weak password recovery mechanisms can enable attackers to bypass passwords by answering simple security questions or using easily obtainable information.

8. Outdated Passwords:

- Not changing passwords regularly or after a security breach can pose risks if old passwords are compromised.

9. Unencrypted Transmission:

- Transmitting passwords over unsecured channels without encryption makes them vulnerable to interception during data transfer.

10. Default Passwords:

- Many devices and systems come with default passwords and failing to change these poses a serious security risk.

11. Password sharing:

- Sharing Passwords, even among trusted individuals, can* lead to breaches if those individuals inadvertently expose the password.