Password Strengths:

Weak:

123456 **Very Weak** **Time to crack your password:0 seconds**

Password **Very Weak** **Time to crack your password:0 seconds**

Qwerty **Very Weak** **Time to crack your password:0 seconds**

abcd1234 **Very Weak** **Time to crack your password:0 seconds**

letmein **Very Weak** **Time to crack your password:0 seconds**

Medium:

R3d$h1ft_P@55 **Medium** **Time to crack your password:8 hours**

Strong:

Un1qu3!K3y#987 **Strong** **Time to crack your password:1 years**

Very Strong:

$g7@L1^vPx*Qm9#E2dZ Very Strong Time to crack your password:8 billion trillion years

Common Password Attacks

1. Brute Force Attack

Definition:

Attempts every possible combination of characters until the correct password is found.

How it works:

Tries a, then aa, then ab, etc.

Can crack short or simple passwords quickly.

Tools Used:

Hydra

John the Ripper

Hashcat

Prevention:

Use long passwords (12+ characters).

Implement rate limiting and account lockout mechanisms.

Use 2FA (Two-Factor Authentication).

2. Dictionary Attack

Definition:

Tries passwords from a predefined list (dictionary of common passwords or leaked credentials).

How it works:

Loads a file like rockyou.txt.

Tries passwords like 123456, qwerty, iloveyou, etc.

Tools Used:

John the Ripper (with wordlists)

THC Hydra

Medusa

Prevention:

Avoid using common or predictable passwords.

Enforce password complexity rules.

Salting and hashing passwords securely on the server.

Difference Between Brute Force and Dictionary:

Feature	Brute Force	Dictionary
Tries all combos	Yes	No
Speed (on short pwds)	Slower	Faster (on common passwords)
Requires wordlist?	No	Yes
Efficient for	Short/weak passwords	Common/guessable passwords

Summary: How Password Complexity Affects Security

Password complexity greatly enhances security by making passwords **harder to guess or crack** through automated attacks like brute force and dictionary attacks.

High Complexity Passwords:

- Use **uppercase + lowercase letters**
- Include **numbers** and **symbols**
- Are **longer (12+ characters)**

Benefits:

- Exponentially increases the number of possible combinations.
- Makes brute-force attacks **impractical**.
- Avoids common passwords found in dictionary lists.

Low Complexity Passwords:

- Use simple words or number patterns (e.g., 123456, password)
- Are short or based on personal info

Risks:

- Easily cracked by dictionary attacks.
- Require **very little time** with brute-force methods.