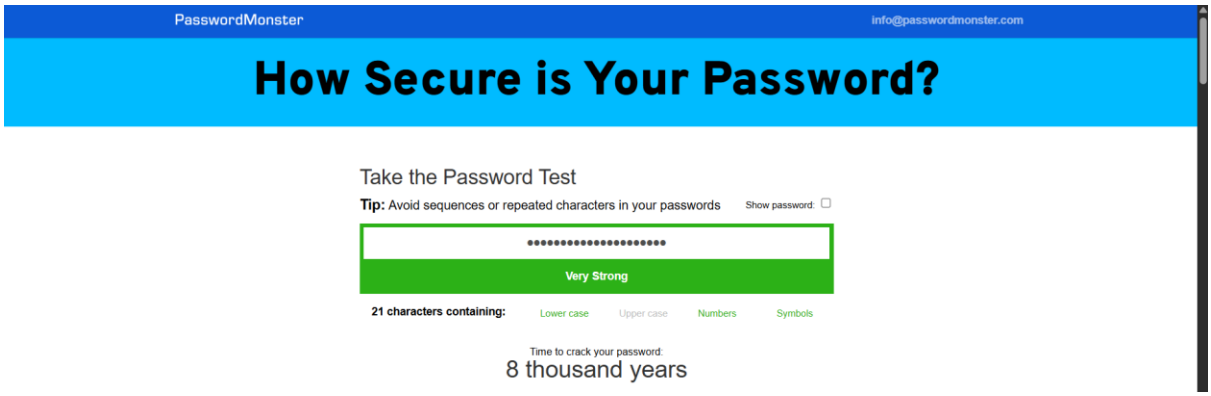
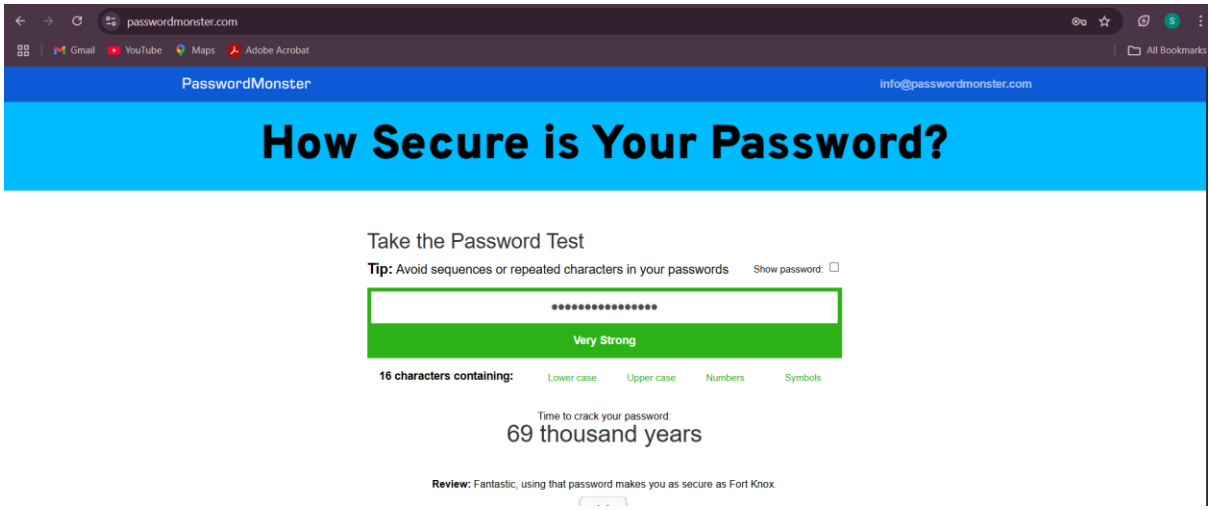
Task 5: Create multiple password and Evaluate its strength.

- Longer passwords are stronger — The example tested (16 characters) is rated Very Strong and estimated to take 69,000 years to crack.
- Mixed character types improve strength — Using uppercase, lowercase, numbers, and symbols greatly increases the difficulty of brute force and dictionary attacks.
- Avoid common patterns — No repeated sequences, dictionary words, or predictable substitutions (e.g., Password123!).
- Randomness is key — Randomly generated passwords are harder for attackers to guess compared to meaningful phrases.
- More length beats complexity alone — A 16-character password with mixed types is exponentially harder to crack than a short but complex one

Praticed Photos :





- Use at least 12–16 characters.
- Combine upper/lowercase letters, numbers, and symbols.
- Avoid personal info (name, birthday, phone number).
- Use a passphrase of random words for easier memorization (e.g., Grape$Tiger!Cloud42).
- Store passwords in a password manager (KeePassXC, Bitwarden, etc.).
- Enable two-factor authentication (2FA) for extra security

1. Brute Force Attack

Definition: A brute force attack tries every possible combination of characters until the correct password is found.

It can use uppercase, lowercase, numbers, and symbols.

Time taken grows exponentially with password length and complexity.

Example:

If your password is AB12, the attacker tries:

AA00 → AA01 → ... → ZZ99

until it matches.

Tools used: Hydra, John the Ripper, Hashcat

2. Dictionary Attack

Definition: A dictionary attack tries passwords from a predefined list of likely or common passwords instead of all combinations.

The “dictionary” may be made of real words, leaked passwords, or pattern-based lists.

Example: If your password is football2025, and it’s in the attacker’s wordlist, it gets cracked quickly without trying every possibility.

Tools used: John the Ripper (with wordlists), Hashcat, rockyou.txt (famous leaked password list).