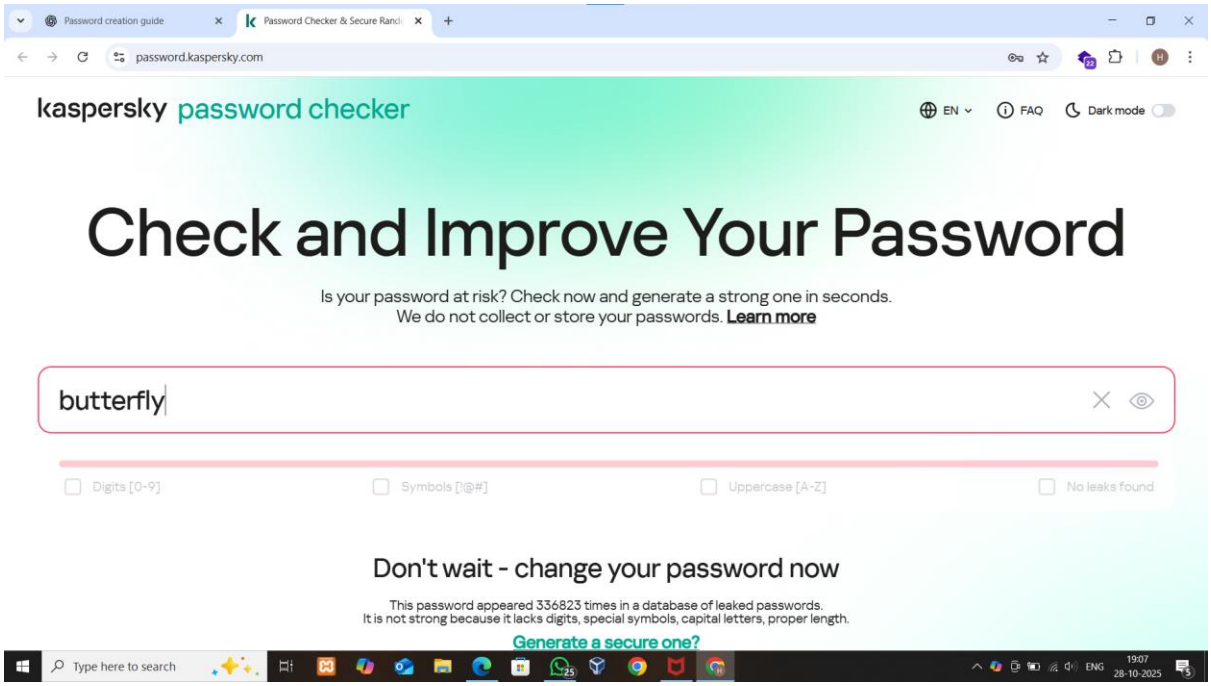
Step 1: Create 5 Different Passwords:

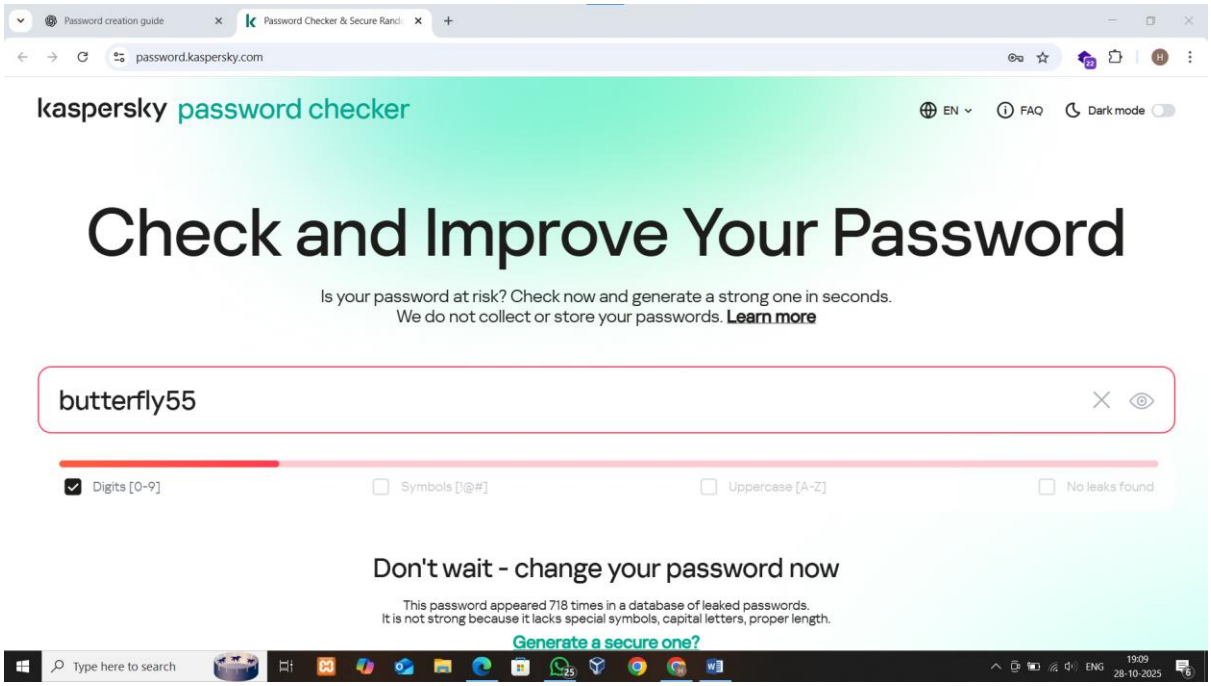
1. butterfly
2. butterfly55
3. bu!!er4ly@55
4. ASD@fgh$jkl789^
5. Mydream@556

Step 2: Test Them on a Password Strength Checker:
https://howsecureismypassword.net/

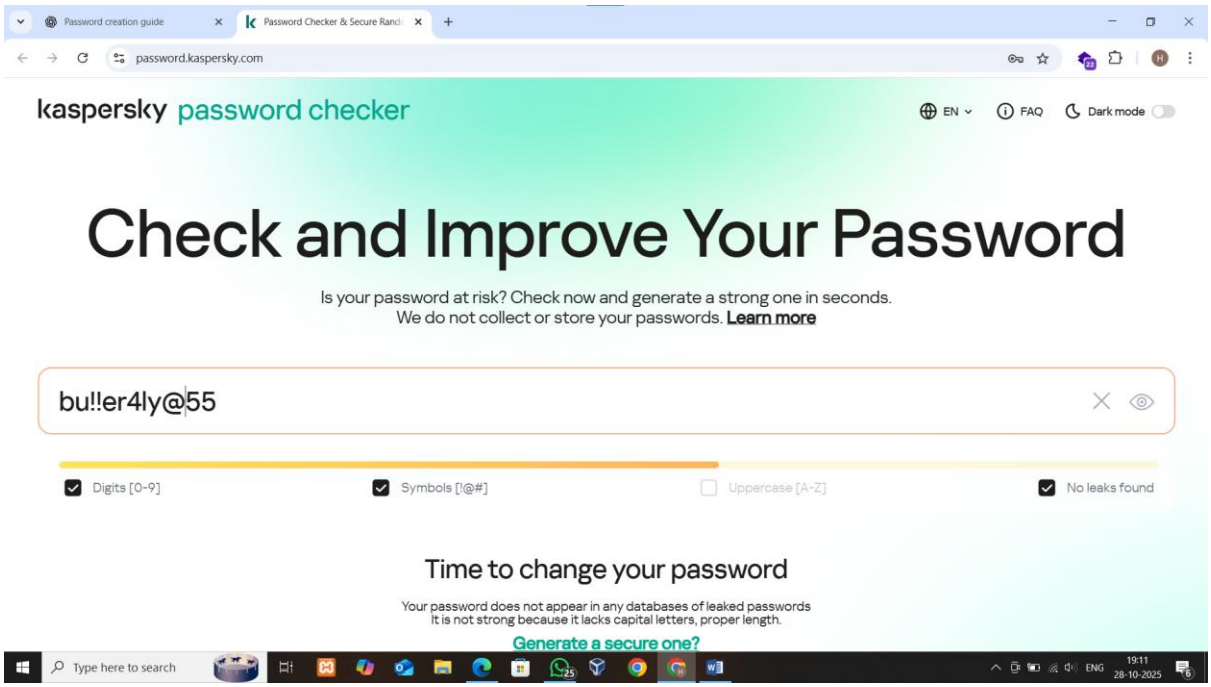
1. **butterfly :**



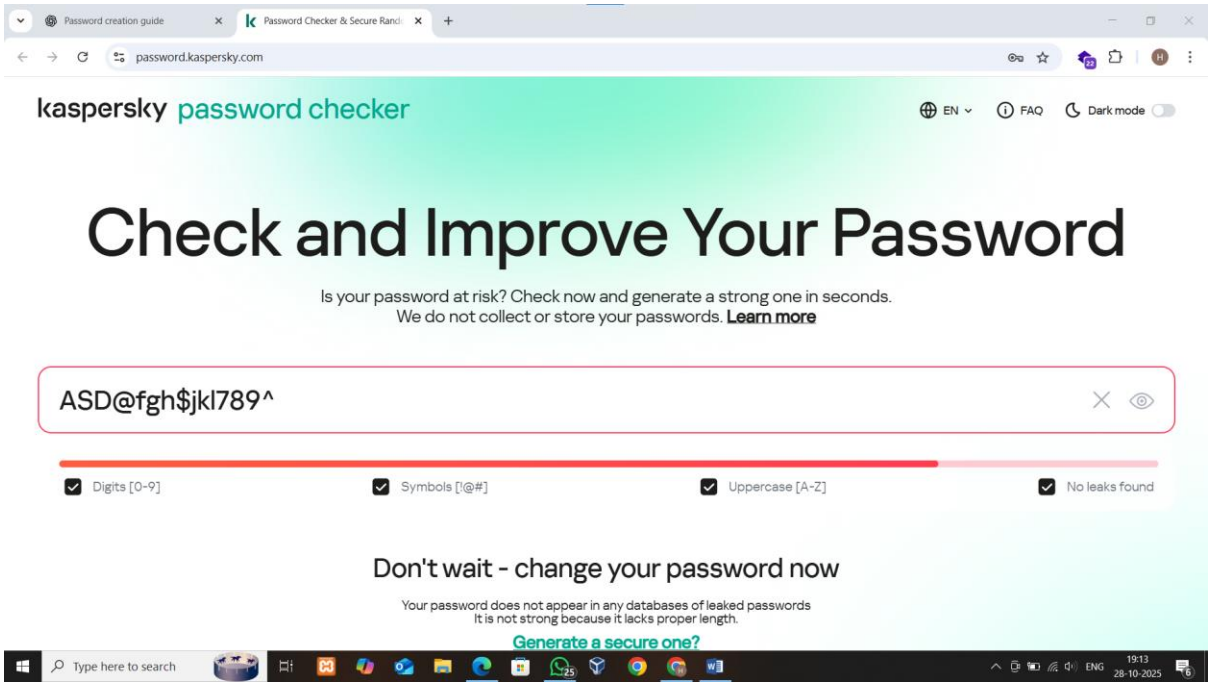
2. **butterfly55:**



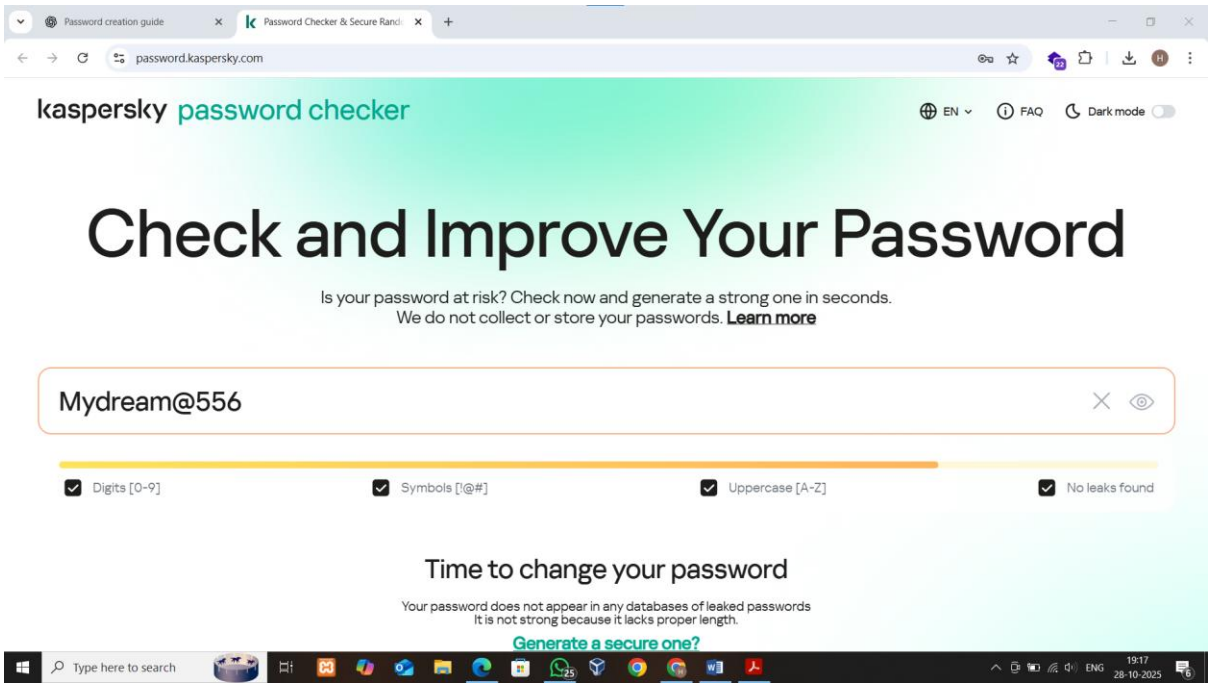
3. **bu!!er4ly@55:**



4. **ASD@fgh$jkl789^ :**



5. **Mydream@556 :**



Step 3: Record the Results :

#	Password	Strength Rating	Estimated Time to Crack (rough)	Feedback / Notes
1	butterfly	Very Weak	**< 1 second — seconds** (dictionary attack)	Common dictionary word, only lowercase, short. Will be found almost instantly by dictionary attacks.
2	butterfly55	Weak	**Seconds → minutes** (dictionary + common digit suffix)	Same base word plus a common two-digit suffix — slightly better but still highly predictable and vulnerable to targeted/dictionary lists.
3	bu!!er4ly@55	Medium → Strong	**Hours → years** (depends on attacker resources & rules)	Uses symbol substitutions and numbers which raises entropy. However it's clearly derived from a single dictionary word (butterfly) so advanced rule-based cracking (substitutions) reduces effective strength. Better than 1–2, but not ideal.
4	ASD@fgh$jkl789^	Strong → Very Strong	**Decades → centuries** (large search space)	Long and includes upper/lower, symbols, and digits. But it appears to follow keyboard-row patterns (ASD fgh jkl) which are somewhat predictable — still quite strong due to length and mixed characters. Randomize more to maximize strength.
5	Mydream@556	Medium	**Years → decades**	Passphrase-like (word + symbol + digits). Better than short single words, but mydream is a phrase that could appear in targeted guesses; repeated digits (556) reduce entropy relative to fully random digits.

Step 4: Observe & Identify Patterns

You'll notice:

- Longer and more random = stronger passwords.
- Words found in the dictionary or with numbers like "123" = weak.
- Mixed symbols, letters, and case = much stronger.

Step 5: Write Down Best Practices

- Minimum 12–16 characters.
- Use uppercase, lowercase, numbers, and symbols.
- Avoid personal info (birthday, name, etc.)
- Use a password manager.
- Enable 2FA for extra protection.

Step 6: Research & Note Attacks:

Common Attacks:

- **Brute Force**: Tries every possible combination.
- **Dictionary Attack**: Uses a list of common passwords.
- **Phishing**: Tricks you to reveal password.

Example:
If your password is sunflower, a dictionary attack will guess it instantly.
If your password is Tg$9eR!2m@x#8, brute force might take **millions of years**.