Elevate Labs Task 6

1) Creating password with varying complexity

- sunflower
- Sunflower123
- S!unfL0w3r#2025
- Pa$$w0rd
- 59_zr6r4t6Rz9A@

2) Use of Character Variations

- **Included**: Uppercase letters, lowercase letters, numbers, special characters, and varying lengths.

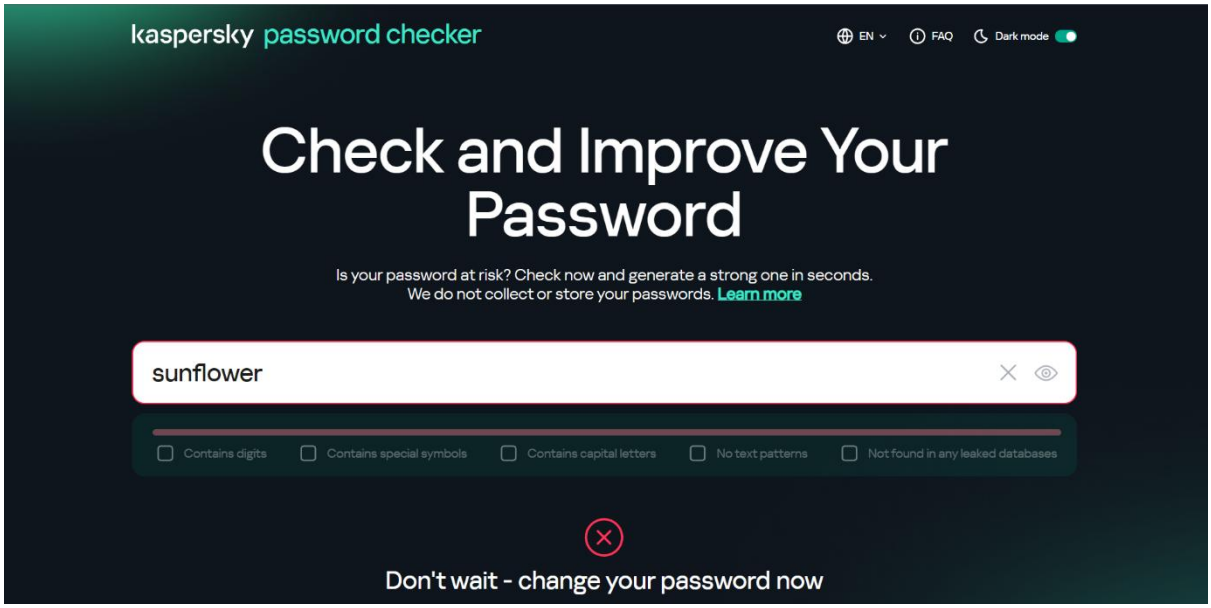
- Goal was to test how combinations of these factors affect password strength.

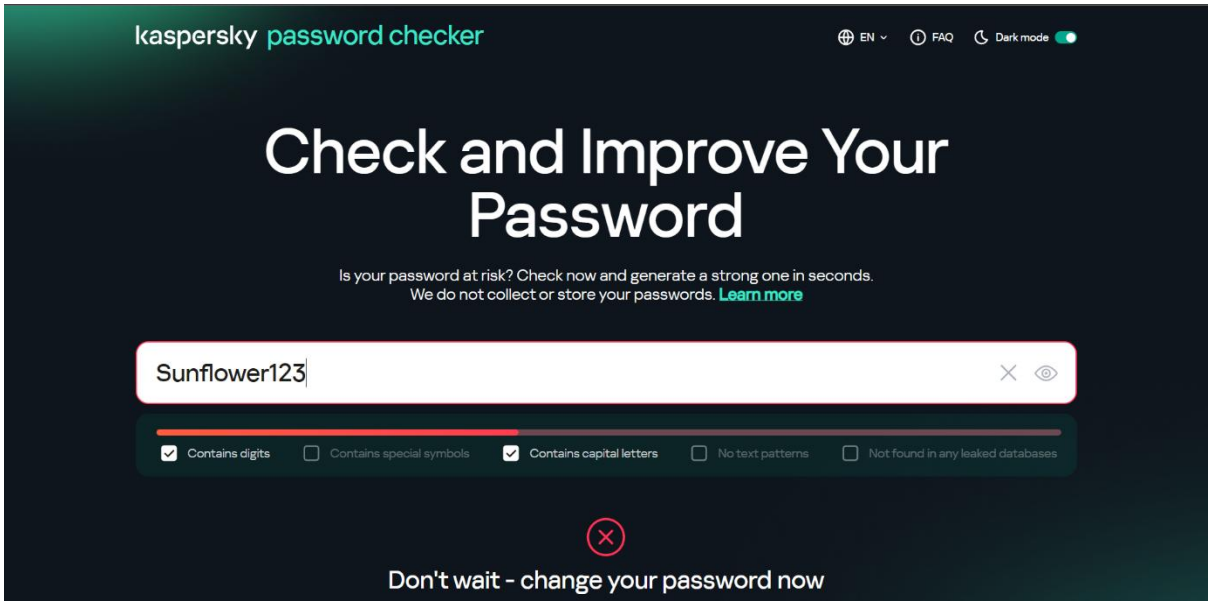
3) Testing with Password Strength Checker

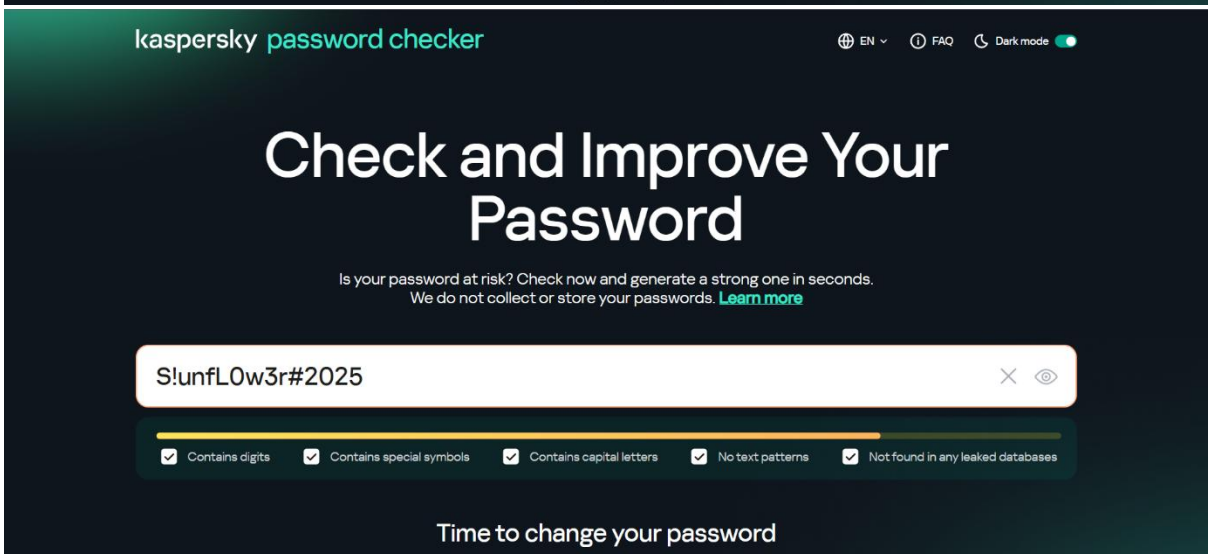
- For checking password strength, I have used ***Kaspersky Password Checker***

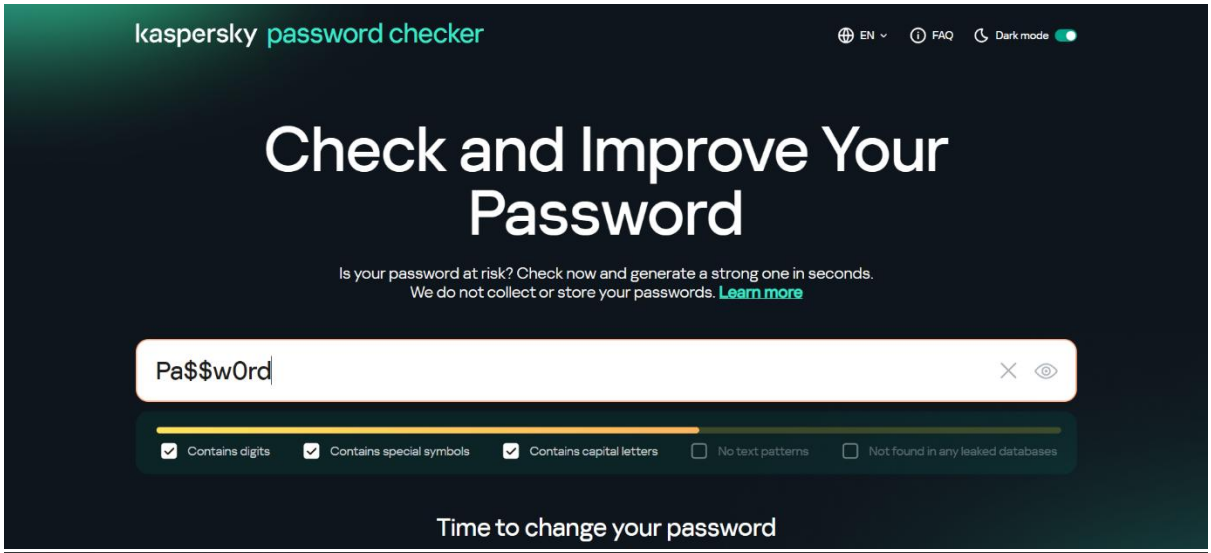
4) Scores and Feedback Summary

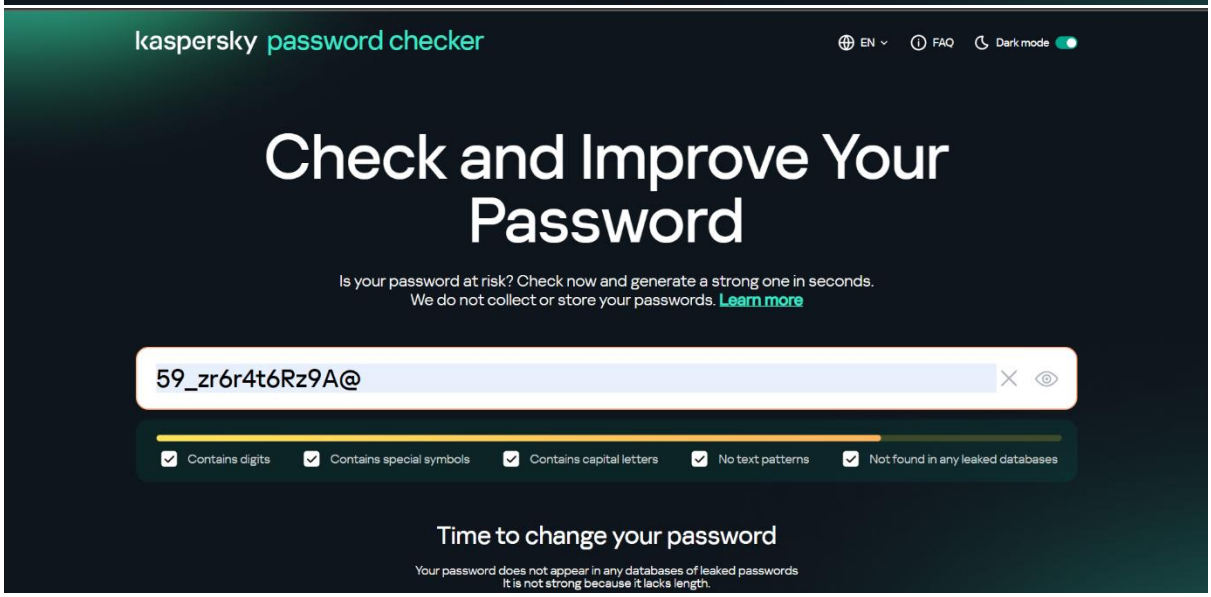
Password	Tool Rating	Estimated Time to Crack	Feedback
sunflower	Weak	<1 second (dictionary attack)	Too common, lacks variation
Sunflower123	Medium	Minutes to hours	Predictable, lacks special characters
S!unfL0w3r#2025	Strong	Centuries	Good length, randomness, and variation
Pa$$w0rd	Weak	<1 second (very common)	Very predictable, commonly used variant
59_zr6r4t6Rz9A@	Very Strong	Centuries	Excellent entropy and randomness


kaspersky password checker
EN
FAQ
Dark mode
Check and Improve Your Password
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more
sunflower
Contains digits
Contains special symbols
Contains capital letters
No text patterns
Not found in any leaked databases
Don't wait - change your password now


kaspersky password checker
EN
FAQ
Dark mode
Check and Improve Your Password
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more
Sunflower123
Contains digits
Contains special symbols
Contains capital letters
No text patterns
Not found in any leaked databases
Don't wait - change your password now


kaspersky password checker
EN
FAQ
Dark mode
Check and Improve Your Password
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more
S!unfL0w3r#2025
Contains digits
Contains special symbols
Contains capital letters
No text patterns
Not found in any leaked databases
Time to change your password


kaspersky password checker
EN
FAQ
Dark mode
Check and Improve Your Password
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more
Pa$$w0rd
Contains digits
Contains special symbols
Contains capital letters
No text patterns
Not found in any leaked databases
Time to change your password


kaspersky password checker
EN
FAQ
Dark mode
Check and Improve Your Password
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more
59_zr6r4t6Rz9A@
Contains digits
Contains special symbols
Contains capital letters
No text patterns
Not found in any leaked databases
Time to change your password
Your password does not appear in any databases of leaked passwords
It is not strong because it lacks length.

5) Best Practices Identified

- Avoid dictionary words and common phrases
- Use longer passwords (12+ characters recommended)
- Mix character types (upper/lower, numbers,symbols)
- Avoid predictable patterns (like ‘123’ or ‘password)

6) Tips Learned

- Randomness is key: avoid using real word or predictable substitution
- Password manager help generate and store strong password
- Reuse of password across sites is a major risk

7) Common Password Attack Methods

- **Brute-force attack**: Tries every possible combination.
- **Dictionary attack**: Uses lists of common passwords.
- **Credential stuffing**: Reuses stolen credentials from data breaches.

8. Summary: Password Complexity & Security

Password complexity directly affects how resistant a password is to various attacks. Simple passwords can be cracked in seconds, while strong, complex, and random passwords may take centuries with current computing power. Using a password manager, generating long and unique passwords, and avoiding reuse are critical steps for digital security.