**Task 6**

**Create a Strong Password and Evaluate Its Strength**

Objective:

Understand what makes a password strong and test it against password strength tools.

The goal is to create strong passwords, evaluate their strength using online tools, and understand the principles behind password security.

Create Passwords with Varying Complexity:

Generate multiple passwords with different combinations of:

* Uppercase Letter (A-Z)
* Lowercase Letter (a-z)
* Number (0-9)
* Symbols (!, @, #, etc.)
* Varying Length (8,12,16 characters)

Example Passwords:

* Password123
* P@ssw0rd@
* Br0ught$34
* hX!2p8#qR&
* Goeshandinhand

Test Password on Online Strength Checkers:

I am using “https://password.kaspersky.com/” website to check password strength.

Test Result:

Password123:

* Feedback: “This password appeared 612400 times in a database of leaked passwords. It is not strong because it lacks special symbols, length.”

P@ssw0rd@:

* Feedback: “This password appeared 9862 times in a database of leaked passwords. It is not strong because it lacks length.”

Br0ught$34:

* Feedback: “Your password does not appear in any databases of leaked passwords. It is not strong because it lacks length.”

hX!2p8#qR&:

* Feedback: “Your password does not appear in any databases of leaked passwords. It is not strong because it lacks length.”

Goeshandinhand:

* Feedback: “Your password does not appear in any databases of leaked passwords. It is not strong because it lacks digits, special symbols, length.”

Analyse Feedback and Best Practices:

* Length matters: Longer passwords are harder to crack.
* Complexity: Mix character types to increase entropy.
* Avoid common words: Dictionary attacks exploit predictable patterns.
* Unpredictability: Randomness is key; avoid personal info.

Common Password Attacks:

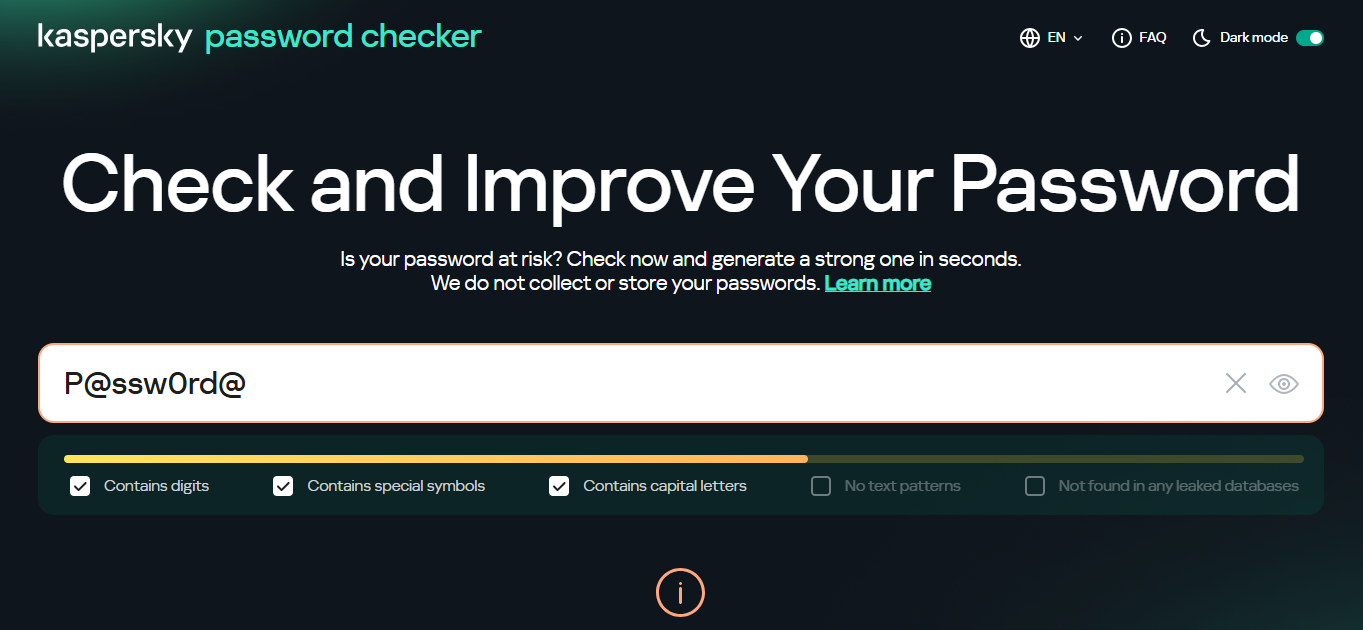
* Brute Force: Trying all possible combinations.
* Dictionary Attack: Using common words/phrases.
* Rainbow Tables: Precomputed hash tables for quick cracking.

Summarize Key Learnings:

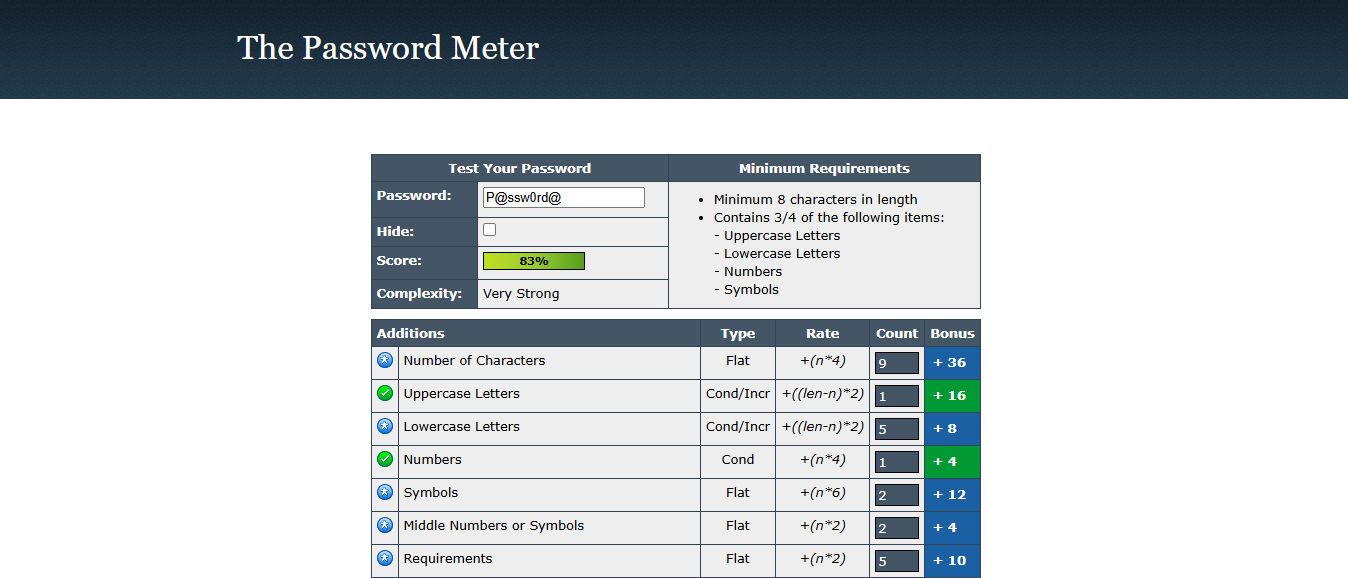
* Strong passwords require length, complexity, and unpredictability.
* Passphrases (long, memorable sentences) can balance security and usability.
* Multi-factor authentication (MFA) adds an extra layer of security.
* Password managers help generate and store strong passwords securely.

Screenshot:

Screenshot of online password checker



Kaspersky Password Checker



Password Meter Checker