Task 6 – Password Security and Strength Evaluation

1. Objective

To understand what makes a password strong, test different passwords using free online password strength checkers, and summarize best practices for creating secure passwords.

2. Tools Used

Password Strength Checker – https://passwordmeter.com
Password Analyzer – https://www.security.org/how-secure-is-my-password/

3. Steps Included

Step 1 – Create Multiple Passwords

A. Very Weak
suraj123
Suraj2025

B. Weak
Suraj@123
Suraj#india

C. Moderate
Sur@jP@ss
Ind!aSuraj2025

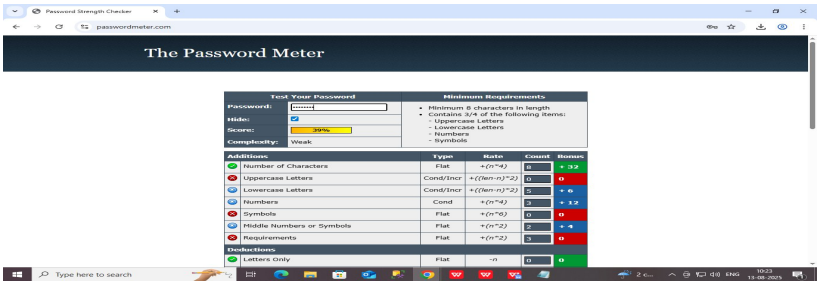
D. Strong
Sur@j_H0u$e2025
Tr@v3l_Suraj!Plan$

E. Very Strong
Cyb3r$3cur1ty!Suraj@Task6
M@x!mUM_Str3nGth_SurajP@ss2025

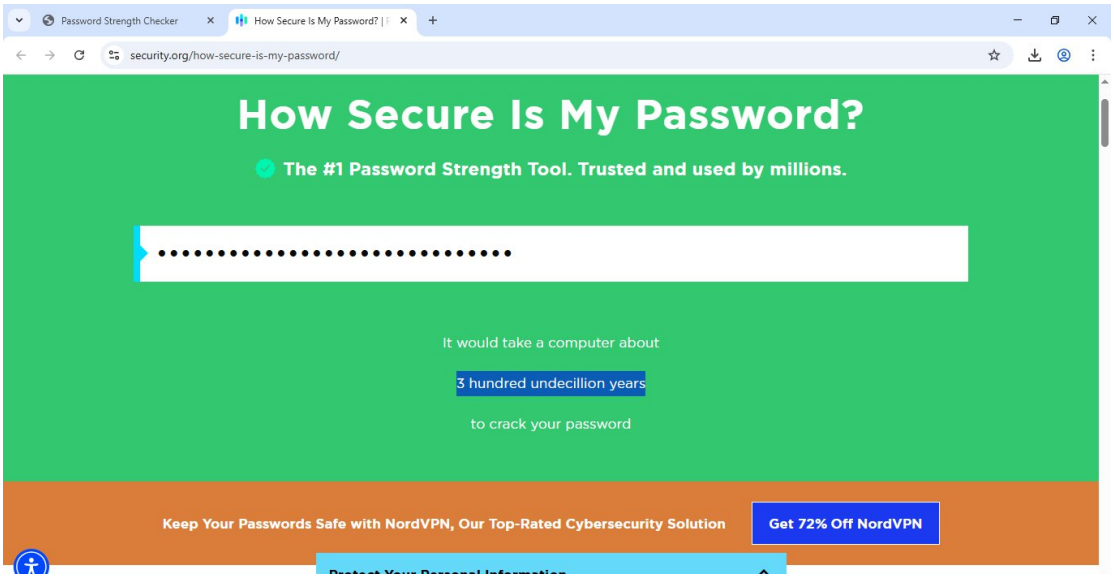
Step 2 – Testing all mentioned Password

Checked each password on passwordmeter.com. & https://www.security.org/how-secure-is-my-password/

Recorded strength score in Excel and feedback from the tool.


The Password Meter


Password Strength Checker
How Secure Is My Password?
passwordmeter.com
The Password Meter
Test Your Password
Minimum Requirements
Password:
M@xImUM_Str3nGth_Sura
Hide:
Score:
100%
Complexity:
Very Strong
Minimum 8 characters in length
Contains 3/4 of the following items:
- Uppercase Letters
- Lowercase Letters
- Numbers
- Symbols
Additions
Type
Rate
Count
Bonus
Number of Characters
Flat
+(n*4)
30
+ 120
Uppercase Letters
Cond/Incr
+((len-n)*2)
7
+ 46
Lowercase Letters
Cond/Incr
+((len-n)*2)
13
+ 34
Numbers
Cond
+(n*4)
5
+ 20
Symbols
Flat
+(n*6)
3
+ 18
Middle Numbers or Symbols
Flat
+(n*2)
7
+ 14
Requirements
Flat
+(n*2)
5
+ 10
Deductions
Letters Only
Flat
-n
0
0


Password Strength Checker
How Secure Is My Password?
security.org/how-secure-is-my-password/
How Secure Is My Password?
The #1 Password Strength Tool. Trusted and used by millions.
It would take a computer about
3 hundred undecillion years
to crack your password
Keep Your Passwords Safe with NordVPN, Our Top-Rated Cybersecurity Solution
Get 72% Off NordVPN

All Tested Password strength score and feedback:-

Password	Strength On Passwordmeter .com	Complexity	https://www.security.org/how-secure-is-my-password/ (Time Taken to crack the password)
suraj123	39	Weak	1 Minute
Suraj2025	79	Strong	3 Days
Suraj@123	83	Very Strong	3 Weeks
Suraj#india	69	Strong	96 Years
Sur@jP@ss	75	Strong	1 Week
Ind!aSuraj2025	100	Very Strong	2 hundred million years
Sur@j_H0u$e2025	100	Very Strong	15 billion years
Tr@v3l_Suraj!Plan$	100	Very Strong	7 quadrillion years
Cyb3r$3cur1ty!Suraj@Task6	100	Very Strong	1 hundred octillion years
M@x!mUM_Str3nGth_SurajP@ss2025	100	Very Strong	3 hundred undecillion years

Step 3 – Comparing Results

Identified patterns in what increased password strength:

Length ≥ 12 characters

Mix of uppercase, lowercase, numbers, symbols

No common dictionary words

Avoiding predictable sequences

4. Best Practices Learned

Use at least 12–16 characters.
Combine uppercase, lowercase, numbers, and symbols.
Avoid dictionary words and common patterns.
Use passphrases (random unrelated words with symbols).
Change passwords regularly.
Use multi-factor authentication (MFA) wherever possible.
Consider using a password manager to store strong passwords.

5. Common Password Attacks

Brute Force Attack – Systematically trying every possible combination.
Dictionary Attack – Using a list of common words and passwords.
Phishing – Trick users into revealing their password.
Keylogging – Capturing keystrokes to steal passwords.

6. How Password Complexity Affects Security

A password's length and randomness drastically increase the time required for a brute-force attack. For example:
8-character simple password → cracked in seconds
16-character complex password → potentially centuries to crack

7. Conclusion

Through this task, it was clear that password strength relies heavily on length, complexity, and unpredictability. Simple and short passwords are vulnerable to brute force and dictionary attacks, while longer complex ones provide better protection.