🛠 Tools Used

- PasswordMeter.com – for password strength scoring and feedback

---

The report includes:

- Passwords tested (with scores and feedback)
- Analysis of weak vs strong passwords
- Common password attack types
- Best practices for secure password creation

Passwords Tested & Results

Password	Score	Complexity
1236	4%	Very Weak
anj326	56%	Good
Pass@123	77%	Strong
PAssword@123	93%	Very Strong
22@99126	99%	Very Strong

📷 Screenshots

Screenshots of password test results:-

1236

Test Your Password		Minimum Requirements
Password:	•••••••••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	18	+ 72
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	12	+ 12
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	4	+ 24
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	4	+ 8
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	12	- 4
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	11	- 22
Consecutive Numbers	Flat	-(n*2)	1	- 2
Sequential Letters (3+)	Flat	-(n*3)	0	0

A

Test Your Password		Minimum Requirements
Password:	•••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	✓	
Score:	56%	
Complexity:	Good	

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	7	+ 28
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 12
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 8
★	Numbers	Cond	+(n*4)	3	+ 12
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✗	Requirements	Flat	+(n*2)	3	0
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
!	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards nal bonuses are applied.

Pass@123

PAssword@123

Test Your Password		Minimum Requirements
Password:	•••••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	93%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	12	+ 48
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 20
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 12
✓	Numbers	Cond	+(n*4)	3	+ 12
✓	Symbols	Flat	+(n*6)	1	+ 6
✓	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✓	Requirements	Flat	+(n*2)	5	+ 10
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 2
!	Consecutive Uppercase Letters	Flat	-(n*2)	1	- 2
!	Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
!	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

✓ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.

✓ **Sufficient:** Meets minimum standards[illegible]nal bonuses are applied.

Cyy@99126

Test Your Password		Minimum Requirements
Password:	•••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	99%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	9	+ 36
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 14
✓	Numbers	Cond	+(n*4)	5	+ 20
✓	Symbols	Flat	+(n*6)	1	+ 6
✓	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
✓	Requirements	Flat	+(n*2)	5	+ 10
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	4	- 3
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
!	Consecutive Numbers	Flat	-(n*2)	4	- 8
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0
Legend					
✓	**Exceptional:** Exceeds minimum standards. Additional bonuses are applied.				

Tips Learned from the Evaluation

- Use at least 12–16 characters for strong security.
- Mix uppercase, lowercase, numbers, and symbols.

- Avoid common words and personal information.
- Use passphrases for memorability (e.g., Cyy@99126).
- Enable Multi-Factor Authentication (MFA) for extra protection.

Common Password Attacks

- Brute Force – Tries every possible combination until the password is found.
- Dictionary Attack – Uses lists of common words and passwords.
- Phishing – Tricks users into giving passwords via fake websites or emails.
- Credential Stuffing – Uses stolen passwords from other accounts.
- Keylogging – Records everything typed, including passwords.

🔑 **Key Learnings**

- Length, complexity, and unpredictability make passwords harder to crack.
- Weak passwords are vulnerable to brute force and dictionary attacks.
- Strong passwords can take years or centuries to break using brute force.
- Multi-Factor Authentication adds an extra layer of security.
- Password managers help store and manage complex passwords securely.
