Elevate_Labs_Task_6

Rudra Srilakshmi

Task 6 : Create a Strong Password and Evaluate Its Strength.

Tools used: The Password Meter

1.Create multiple passwords with varying complexity.

2.Use uppercase, lowercase, numbers, symbols, and length variations.

I created a set of passwords differently with different structures and combinations. Here, the aim was to test how factors like length, characters and randomness affect password strength.

- **hello123**
  used lowercase letters and numbers only - weak
- **Hello@123**
  mix of letters, number, and a symbol - moderate
- **qwerty**
  common weak password
- **H@ppyLif3!2025**
  long, strong mix of elements
- **T!m#l9Ox*&wZ**
  complex and random string – very strong
- **Password123!**
  common format, but includes special characters

3.Test each password on password strength checker.

hello123

The Password Meter

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:	37%	
Complexity:	Weak	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
○	Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 6
○	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	-	2	- 2
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
!	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

Hello@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:	81%	
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)	4	+ 10
○	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)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
!	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

qwerty

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:	8%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	1	0
Deductions				
Letters Only	Flat	-n	6	- 6
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)	5	- 10
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

H@ppyLif3!2025

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	

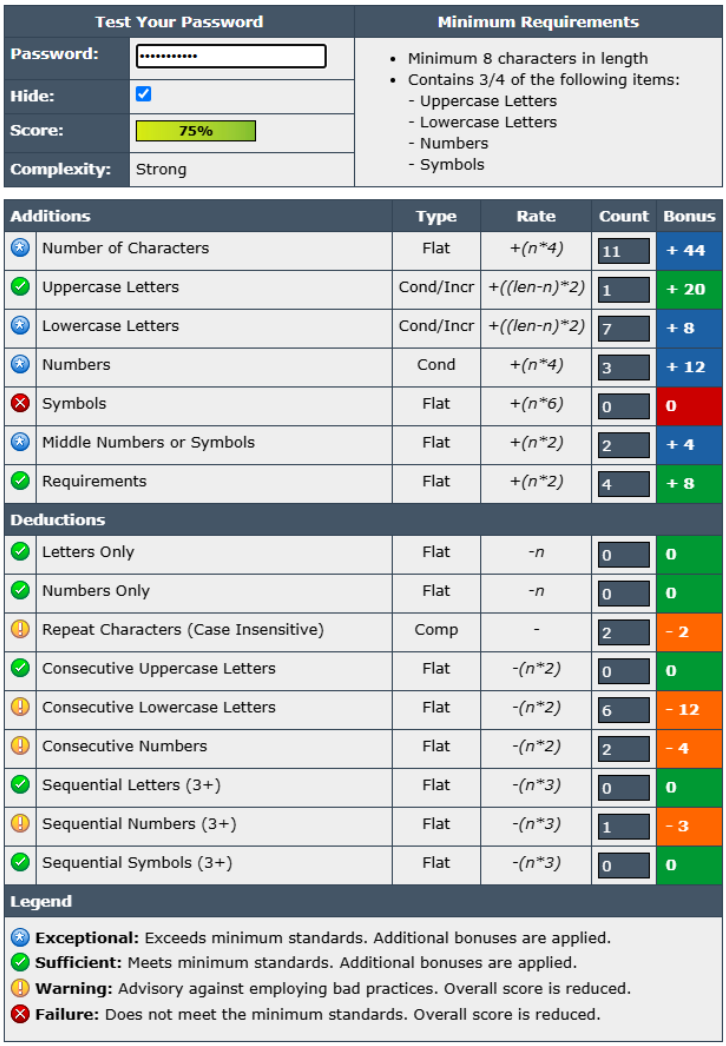
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 18
Numbers	Cond	+(n*4)	5	+ 20
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	3	- 6
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

T!m#l9Ox*&wZ

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)	12	+ 48
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 18
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 16
✓	Numbers	Cond	+(n*4)	1	+ 4
✓	Symbols	Flat	+(n*6)	4	+ 24
✓	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	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Password123!



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:	75%	
Complexity:	Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	11	+ 44
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 20
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 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)	4	+ 8
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)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
!	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. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

4.Note scores and feedback from the tool.

Password	Score (%)	Complexity Level	Tool Feedback Summary
hello123	37%	Weak	Too short, no uppercase or symbols, predictable pattern
Hello@123	81%	Moderate	Good mix of character types, but still common format
qwerty	8%	Very Weak	Very common, no numbers or symbols, too short

H@ppyLif3!2025	100%	Strong	Good length, includes all character types
T!m#l9Ox*&wZ	100%	Very Strong	Excellent randomness, long and highly complex
Password123!	75%	Moderate	Includes character types, but contains common word

5.Identify best practices for creating strong passwords.

After analyzing the results, I identified the following best practices that consistently made passwords stronger:

Best practices includes:

- Use at least 8-12 characters
- Should contain uppercase, lowercase, numbers, and symbols
- Avoid personal info, dictionary words or common sequences
- Include phrases with unrelated words and symbols
- Instead of using patterns, ensure randomness

6.Write down tips learned from the evaluation.

From the evaluation results, tips learned includes:

- Rather than using a short password at any time, its better to use a longer password.
- Replacing letters with lookalike symbols increases strength. For example, in this case *"using @ inplace of a".*
- Adding a special character early in the password often improves strength ratings.
- Using a random string generator or password manager is highly effective.
- Even a small change like making *"password into P@ssw0rd!"* greatly improves strength, but still can be weak if it's a known pattern.

7.Research common password attacks.

There are many ways hackers use to steal passwords. Some of most common attacks are:

- **Brute Force Attack**:
  The attack, where they try every possible combination until they find the right one. This works fast if the password is short or simple.
  For example, a 6-character lowercase password can be broken in seconds, while a 16-character mixed-type password may take hundreds of years.

- **Dictionary Attack**:
  In this, attackers use a list of common words or leaked passwords to guess the correct one. Passwords like password123, sunshine are especially vulnerable. This type of attack is faster than brute force and highly effective against weak, common passwords.

- **Phishing Attacks**:
  Rather than technically cracking a password, phishing method tricks the user into revealing their credentials via fake websites, emails, or login pages. These attacks often bypass password complexity altogether by relying on social engineering.

- **Keylogging:**
  Malware or physical keyloggers record every keystroke made on a device. If installed, attackers can steal even the most secure passwords by capturing them directly as they're typed.

- **Credential Stuffing:**
  Attackers use username and password combinations leaked from other data breaches and attempt to log into multiple websites. This works well when users reuse the same passwords across accounts, emphasizing the importance of using unique passwords everywhere.

8.Summarize how password complexity affects security.

Password strength is crucial as it becomes difficult for hackers to crack or guess your password. A strong password is long and has a combination of uppercase and lowercase letters, numbers, and special characters. This is much more

secure compared to weak passwords such as 123456 or password. Strong passwords become extremely hard to break using attack methods such as brute force or dictionary-based attacks. The longer and more arbitrary your password is, the more it secures your accounts. Simply put, having strong and complex passwords makes your personal information and online accounts safer.