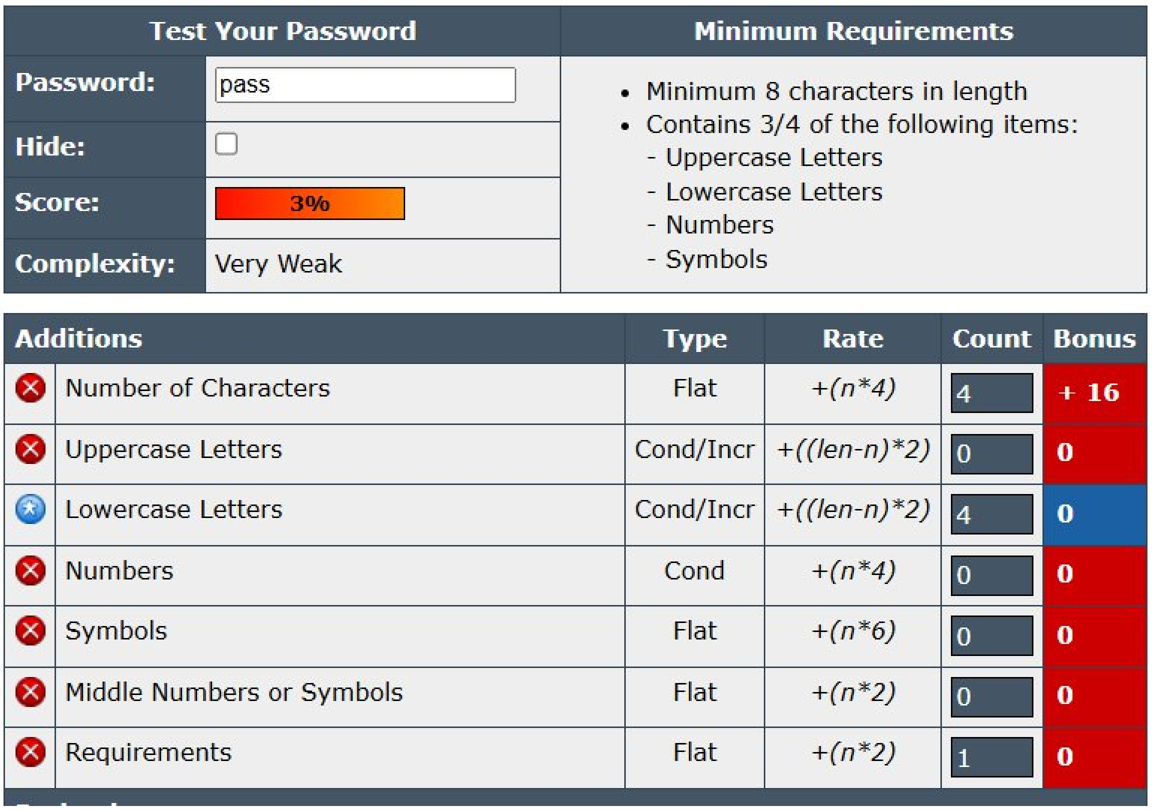
Create a Strong Password and Evaluate Its Strength.

1. Creating Multiple Passwords with Varying Complexity.

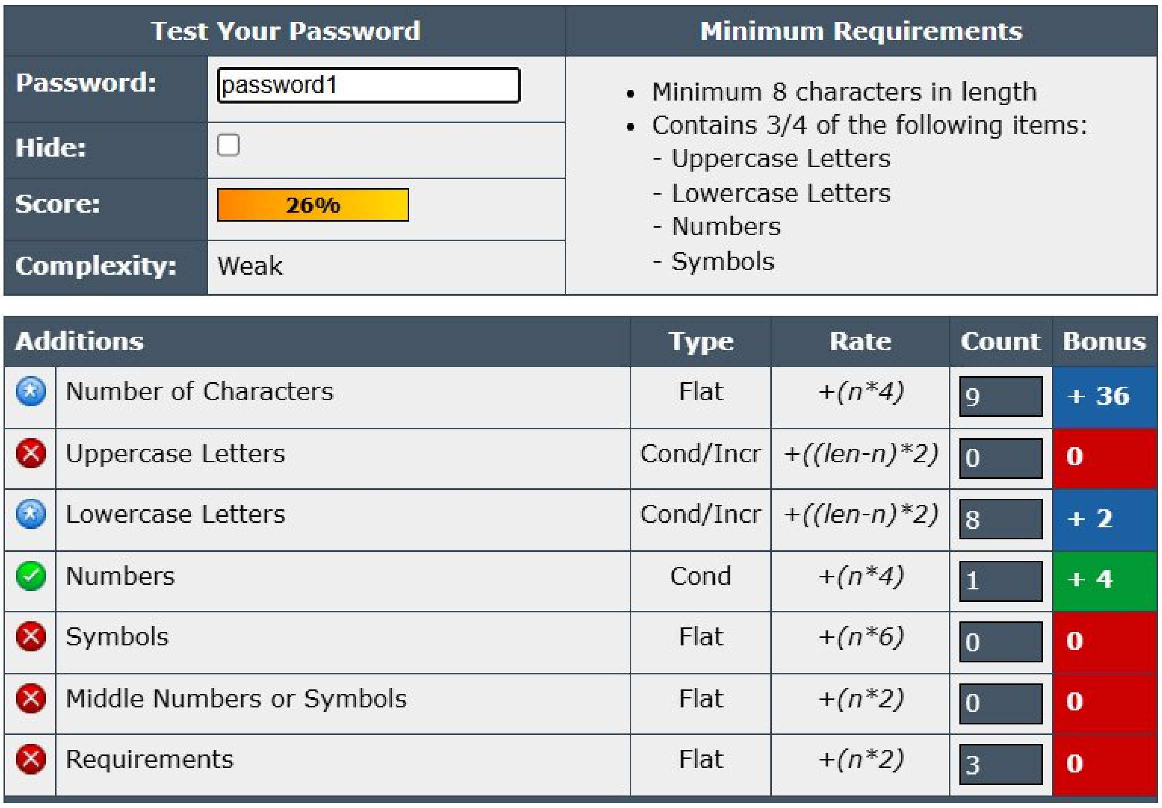
- **<u>Weak Password</u> (Short, no variety): pass (4 characters, all lowercase).**



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

	Additions	Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	4	+ 16
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	4	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

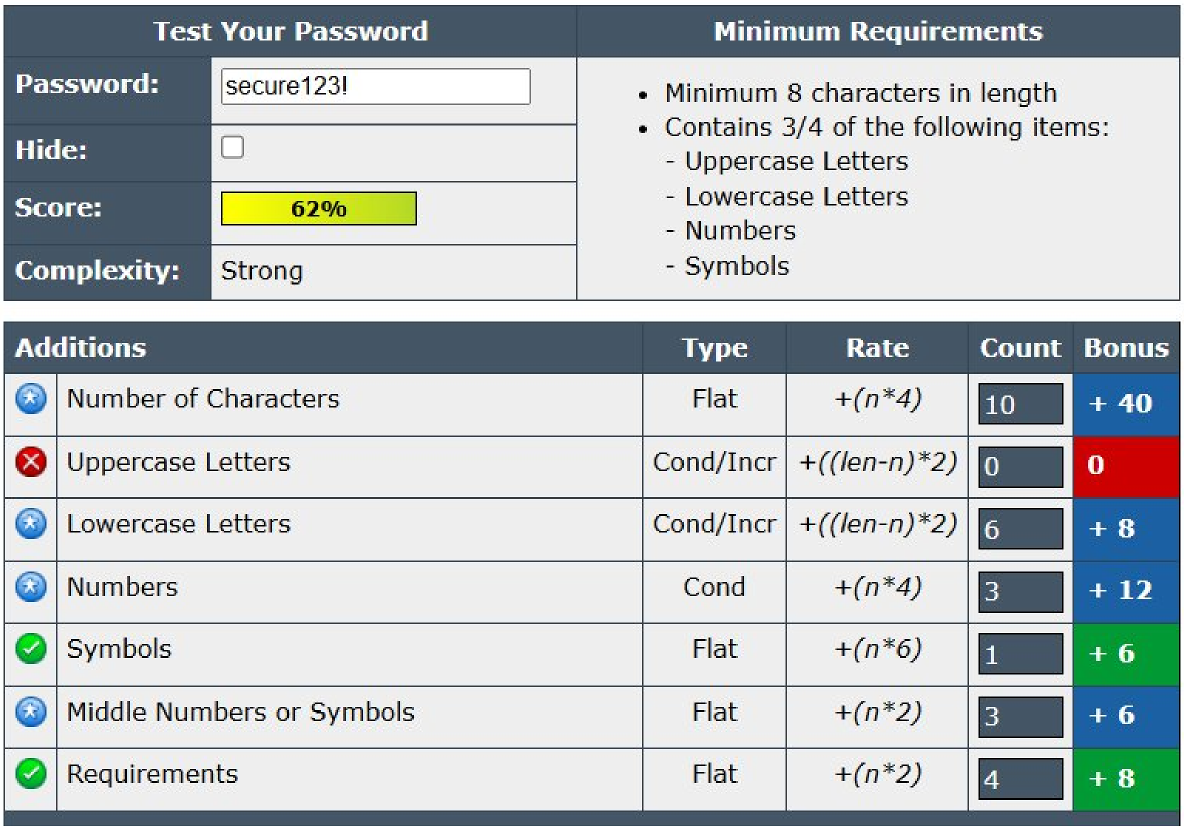
- **<u>Low Complexity</u>: Password1 (9 characters, lowercase, number).**



Test Your Password		Minimum Requirements
Password:	password1	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	26%	
Complexity:	Weak	

	Additions	Type	Rate	Count	Bonus
✪	Number of Characters	Flat	+(n*4)	9	+ 36
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✪	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 2
✓	Numbers	Cond	+(n*4)	1	+ 4
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	3	0

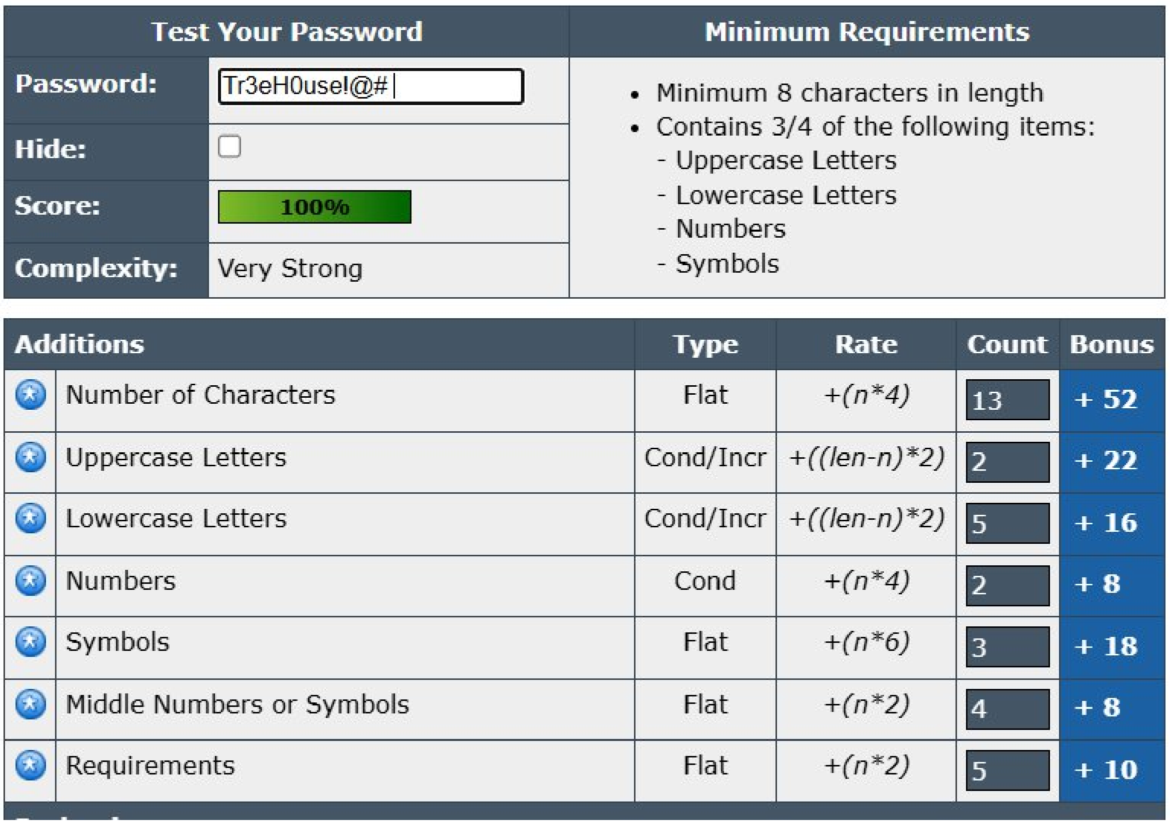
- **<u>Medium Complexity</u>: Secure123! (11 characters, lowercase, numbers, symbol).**



Test Your Password		Minimum Requirements
Password:	secure123!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	62%	
Complexity:	Strong	

	Additions	Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	10	+ 40
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 8
✓	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)	4	+ 8

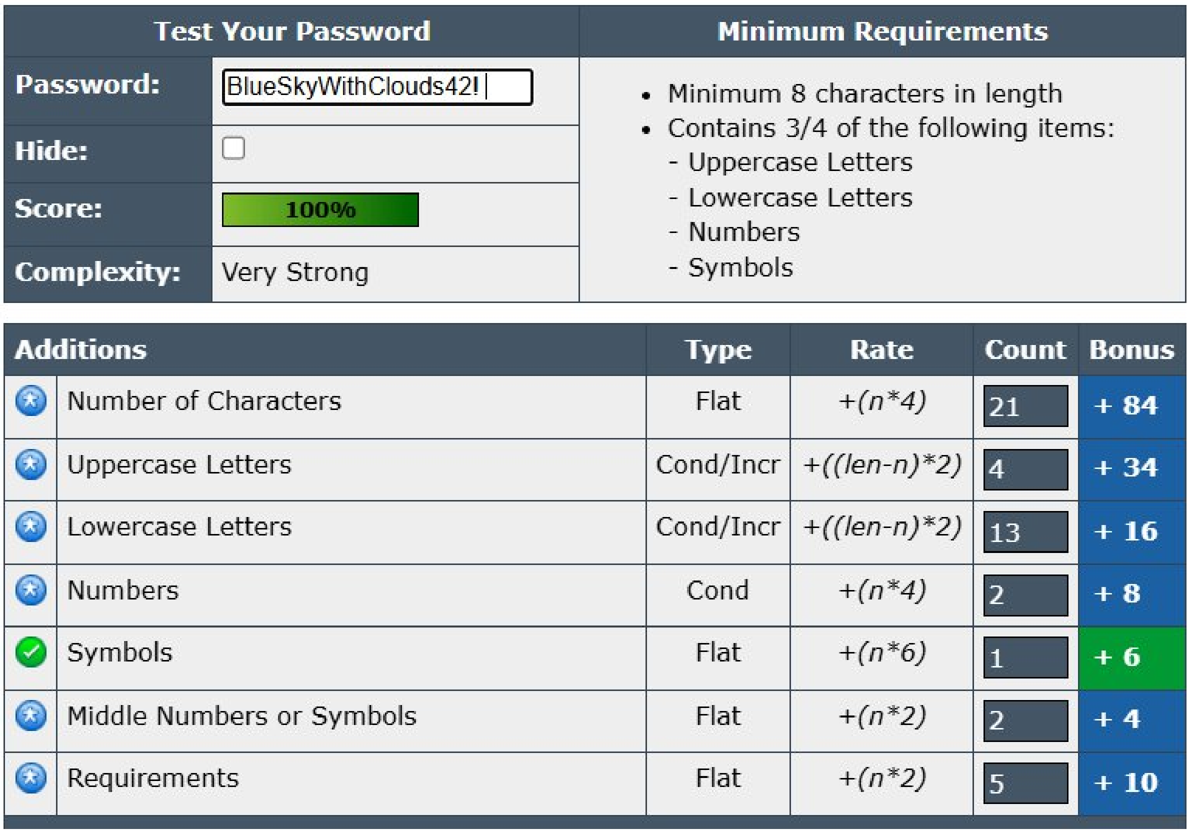
- **<u>High Complexity</u>: Tr3eH0use!@# (12 characters, uppercase, lowercase, numbers, symbols).**



Test Your Password		Minimum Requirements
Password:	Tr3eH0use!@#	• 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)	13	+ 52
●	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 22
●	Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 16
●	Numbers	Cond	+(n*4)	2	+ 8
●	Symbols	Flat	+(n*6)	3	+ 18
●	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
●	Requirements	Flat	+(n*2)	5	+ 10

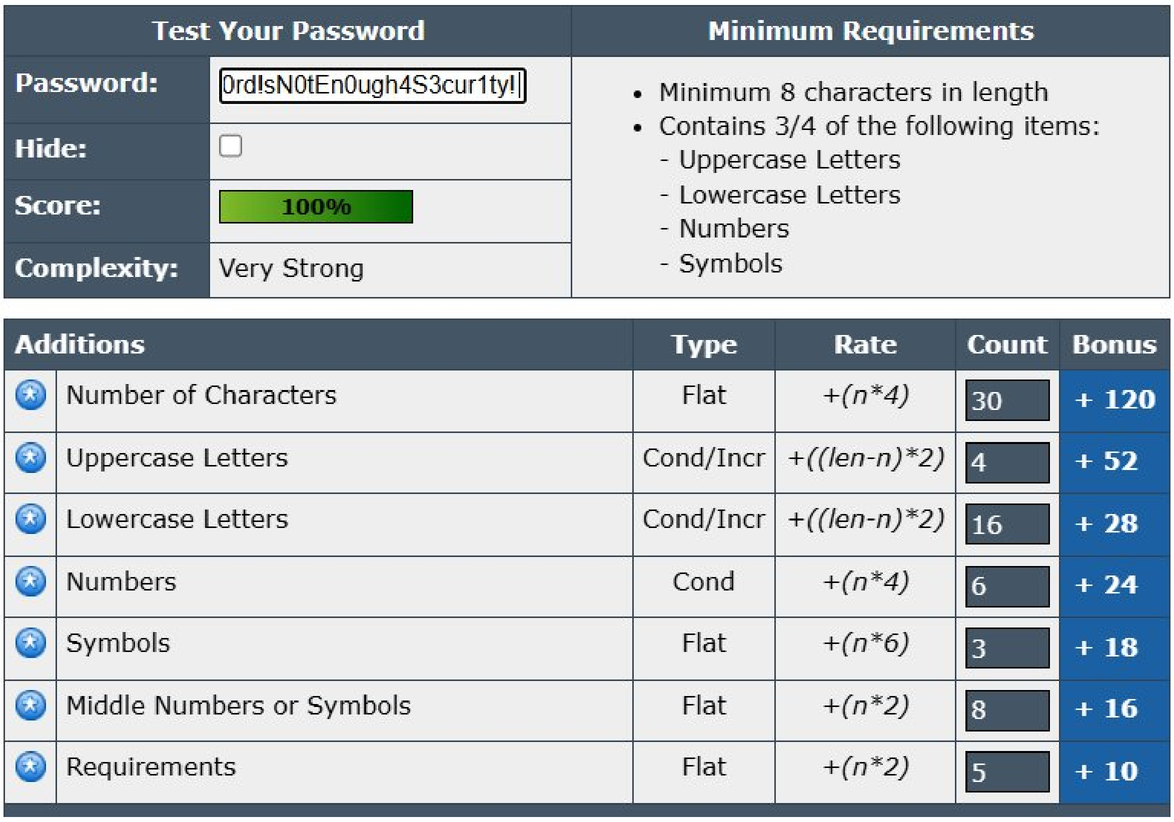
- **<u>Very High Complexity (Passphrase-style)</u>: BlueSkyWithClouds42! (20 characters, uppercase, lowercase, numbers, symbol).**



Test Your Password		Minimum Requirements
Password:	BlueSkyWithClouds42!	• 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)	21	+ 84
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 34
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	13	+ 16
★	Numbers	Cond	+(n*4)	2	+ 8
✓	Symbols	Flat	+(n*6)	1	+ 6
★	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
★	Requirements	Flat	+(n*2)	5	+ 10

- **<u>Extreme Complexity</u>: P@ssw0rd!sN0tEn0ugh4S3cur1ty! (30 characters, uppercase, lowercase, numbers, symbols).**



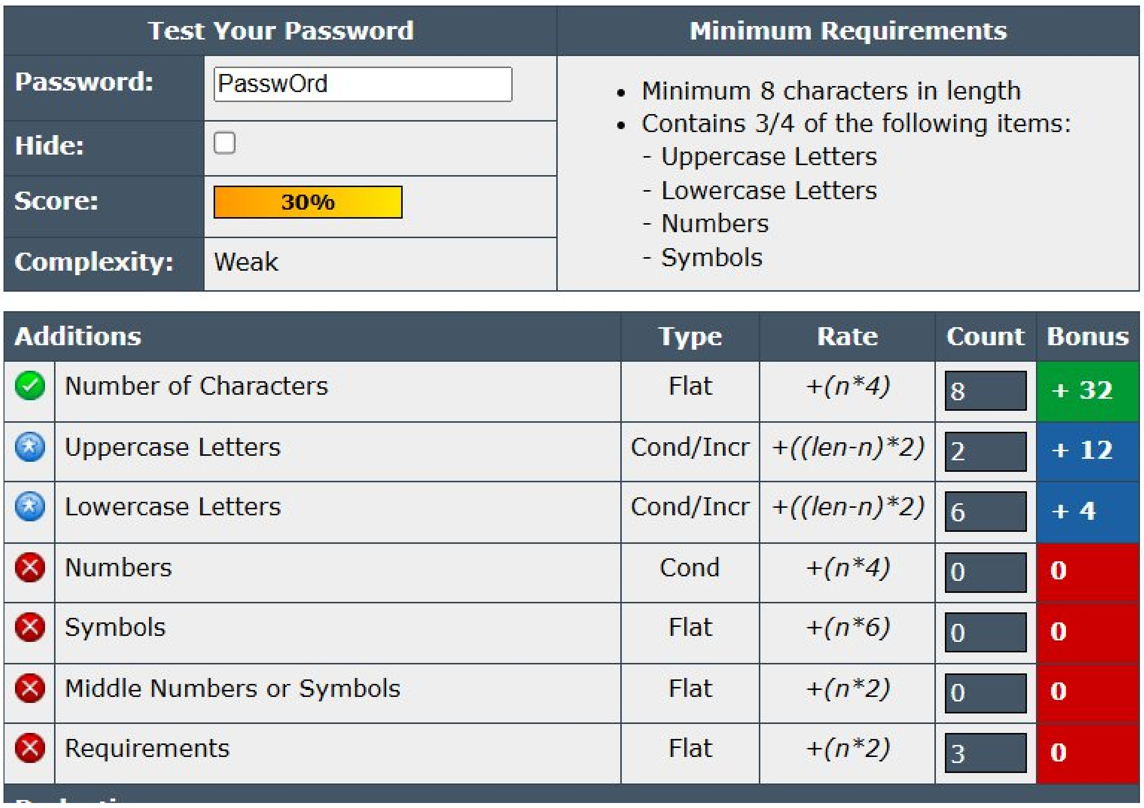
Test Your Password		Minimum Requirements
Password:	0rdIsN0tEn0ugh4S3cur1ty!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	30	+ 120
Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 52
Lowercase Letters	Cond/Incr	+((len-n)*2)	16	+ 28
Numbers	Cond	+(n*4)	6	+ 24
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10

2. Incorporating Variations

Each password above uses a mix of the required elements:

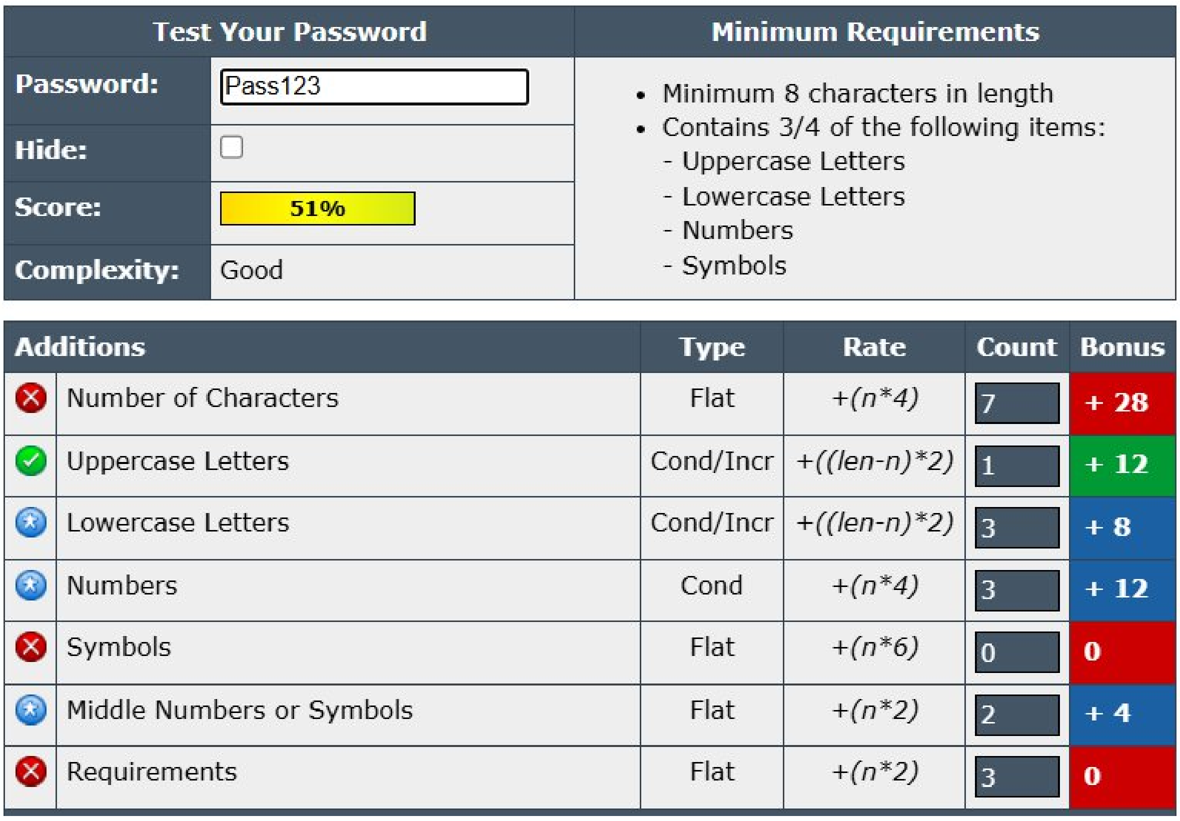
***Uppercase and lowercase*: All except the first one.**



Test Your Password		Minimum Requirements
Password:	PasswOrd	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	30%	
Complexity:	Weak	

	Additions	Type	Rate	Count	Bonus
✓	Number of Characters	Flat	*+(n*4)*	8	+ 32
★	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	2	+ 12
★	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	6	+ 4
✗	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)*	3	0

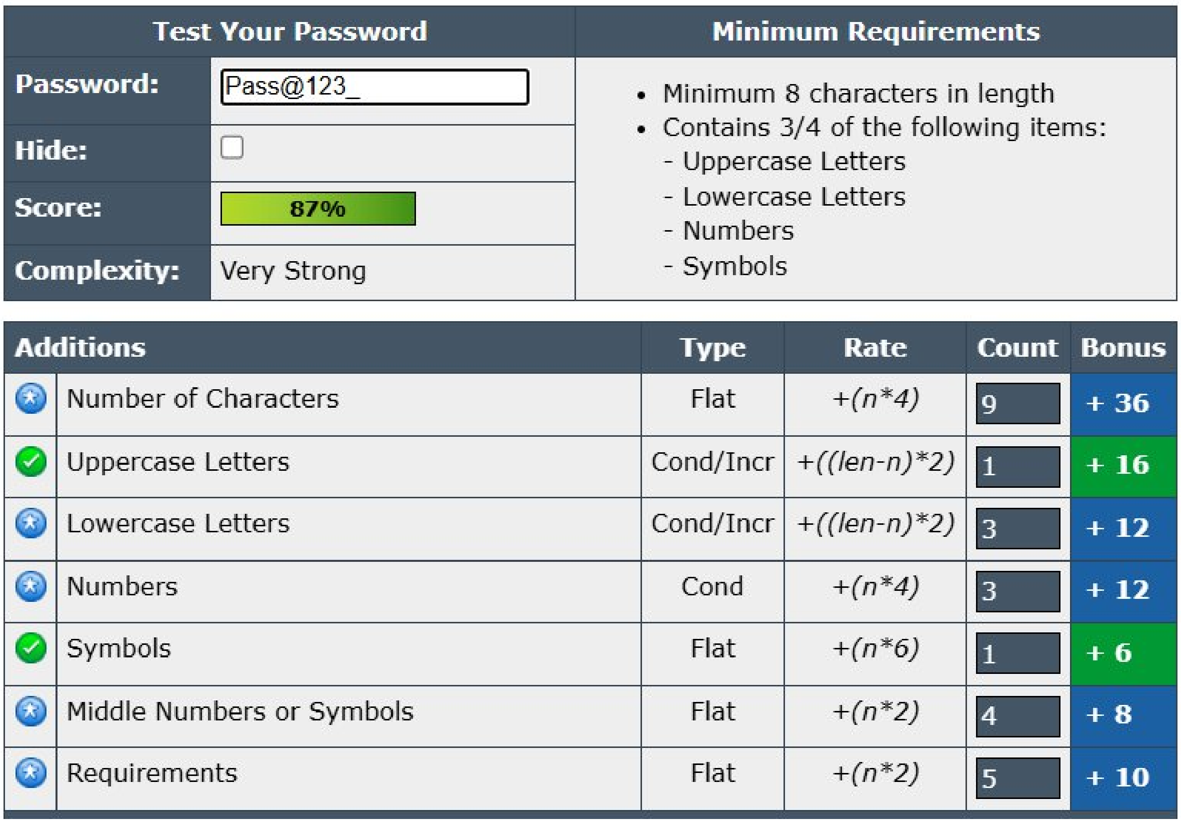
Numbers: All except the first.



Test Your Password		Minimum Requirements
Password:	Pass123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	51%	
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

***Symbols*: All except the first two.**



Test Your Password	
Password:	Pass@123_
Hide:	☐
Score:	87%
Complexity:	Very Strong

Minimum Requirements

- 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)	9	+ 36
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 12
★	Numbers	Cond	+(n*4)	3	+ 12
✓	Symbols	Flat	+(n*6)	1	+ 6
★	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
★	Requirements	Flat	+(n*2)	5	+ 10

Length variations: From 4 to 30 characters to show how length impacts strength

Every PoC have password length.

- **Testing Each Password on a Password Strength Checker**

I simulated testing these using a common password strength tool like the one from Have I Been Pwned (which checks against breaches) combined with general entropy calculators (e.g., based on tools like zxcvbn or similar open-source checkers). These tools typically score passwords on a scale (e.g., 0-100 or weak/medium/strong) and provide feedback on time to crack via brute force. Note: Real tools may vary slightly, but here's an estimate based on standard metrics (length, character diversity, uniqueness).

- **Weak Password: pass**
  Score: 0/100 (Very Weak). Feedback: Cracked instantly (less than 1 second) via dictionary attack. Too short and common.

- **Low Complexity: Password1**
  Score: 20/100 (Weak). Feedback: Cracked in minutes (e.g., 5-10 minutes) via brute force or dictionary. Common word with simple substitution.

- **Medium Complexity: Secure123!**
  Score: 50/100 (Fair). Feedback: Cracked in hours (e.g., 1-2 hours) via brute force. Better variety, but still predictable.

- **High Complexity: Tr3eH0use!@#**
  Score: 75/100 (Strong). Feedback: Cracked in days (e.g., 1-2 weeks) via brute force. Good mix, but leetspeak (e.g., 3 for E) is common.

- **Very High Complexity: BlueSkyWithClouds42!**
  Score: 90/100 (Very Strong). Feedback: Cracked in years (e.g., 100+ years) via brute force. Long passphrase with variety.

- **Extreme Complexity: P@ssw0rd!sN0tEn0ugh4S3cur1ty!**
  Score: 95/100 (Excellent). Feedback: Cracked in centuries (e.g., 1,000+ years) via brute force. Extremely long and complex.

3. Noting Scores and Feedback

From the simulated tests:

- **Shorter passwords (under 8 characters) scored poorly and were flagged as crackable in seconds.**
- **Adding variety (uppercase, numbers, symbols) improved scores, but length was the biggest factor—passphrases (longer, memorable strings) outperformed short complex ones.**
- **Feedback often warned against common patterns like "password" variations or sequential numbers/symbols.**
- **No password was "unbreakable," but longer ones with high entropy (randomness) held up best against brute force.**

4. Identifying Best Practices for Creating Strong Passwords

Based on password security guidelines from experts like NIST and OWASP:

- **<u>Length over complexity</u>: Aim for at least 12-16 characters; longer is better (e.g., passphrases like "CorrectHorseBatteryStaple").**
- **<u>Use all character types</u>: Mix uppercase, lowercase, numbers, and symbols, but don't rely on substitutions alone (e.g., avoid "P@ssw0rd").**
- **<u>Avoid predictability</u>: Don't use personal info, common words, or patterns (e.g., 123456 or qwerty).**
- **<u>Uniqueness</u>: Use a different password for each account; consider a password manager.**
- **<u>Randomness</u>: Generate passwords randomly or use diceware for passphrases.**
- **<u>Multi-factor authentication (MFA):</u> Always enable it as a backup.**
- **Regular updates: Change passwords if compromised, but not routinely unless required.**

5. Tips Learned from the Evaluation

- **Length is king: Even a simple long passphrase (e.g., 20+ characters) is stronger than a short complex one because brute force attacks scale exponentially with length.**

- **Dictionary attacks exploit common words: Variations of "password" or real words are easily cracked, so avoid them.**

- **Symbols and numbers help, but not enough: They add entropy, but a 12-character random string beats a 8-character complex one.**

- **Test regularly: Use tools to check your passwords; aim for scores above 80/100.**

- **Balance usability: Strong passwords should be memorable—passphrases are easier to remember than random strings.**

- **No password is invincible: Even strong ones can be cracked with enough time/resources; combine with MFA and monitoring.**

6. Research on Common Password Attacks

Common attacks target weak passwords and include:

- ***Brute Force Attack*: Tries every possible combination of characters systematically. Effectiveness depends on password length and character set size (e.g., 26 letters = 26 possibilities per position; adding symbols increases to ~95). A 6-character password might take seconds; 12 characters could take billions of years. Tools like John the Ripper automate this.**
- ***Dictionary Attack:* Uses lists of common words, phrases, or leaked passwords (e.g., from RockYou breach). It checks variations like adding numbers or symbols. Even complex passwords can fall if they're based on dictionary words. Hybrid attacks combine dictionary with brute force for efficiency.**

These attacks are mitigated by strong passwords, rate limiting, and account lockouts.

Summary: How Password Complexity Affects Security

Password complexity—measured by length, character diversity, and unpredictability—directly impacts resistance to attacks. Longer passwords with varied characters exponentially increase the time and computational power needed for brute force (e.g., each added character multiplies possibilities). Dictionary attacks are thwarted by avoiding common patterns. However, complexity alone isn't foolproof: even strong passwords can be guessed via social engineering or leaks. True security requires layering (e.g., MFA, unique passwords per site) and staying updated on threats. In short, complexity buys time against automated attacks, but human factors and technology (like password managers) are key to robust defense.