

Name: satya chaitanya yerninti

Email: satyachaitanya21@gmail.com

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

Tools used: passwordmeter.com

Password strengthening:

Password strengthening involves creating long, unique passwords with a mix of uppercase letters, lowercase letters, numbers, and symbols. It is also crucial to use a [password manager](#) to store unique passwords for each account and enable [multi-factor authentication](#) whenever possible. Avoid using personal information, common words, or predictable patterns that are easy for attackers to guess.

Creating a strong password

- **Make it long:** Aim for at least 12 characters, with 14 or more being even better.
- **Use a mix of character types:** Combine uppercase and lowercase letters, numbers, and special symbols (e.g., @, #, %).
- **Avoid personal information:** Don't use birthdays, names, addresses, or pet names that can be easily found online.
- **Don't use common words or patterns:** Steer clear of dictionary words, consecutive letters (like "abc"), or repeated characters (like "aaa").
- **Consider a passphrase:** A memorable phrase made of several random words is often longer and more secure than a single password (e.g., "CoffeeTableBookSunshine").

Keeping strong password

Test Your Password		Minimum Requirements				
Password:	<input type="text" value="EeSaalaCupNamdhe@202"/>	<ul style="list-style-type: none"> Minimum 8 characters in length Contains 3/4 of the following items: <ul style="list-style-type: none"> Uppercase Letters Lowercase Letters Numbers Symbols 				
Hide:	<input type="checkbox"/>					
Score:	<div><div>100%</div></div>					
Complexity:	Very Strong					
Additions						
	Type	Rate	Count	Bonus		
+ Number of Characters	Flat	$+(n^*4)$	<input type="text" value="21"/>	+ 84		
+ Uppercase Letters	Cond/Incr	$+\left((len-n)^*2\right)$	<input type="text" value="4"/>	+ 34		
+ Lowercase Letters	Cond/Incr	$+\left((len-n)^*2\right)$	<input type="text" value="12"/>	+ 18		
+ Numbers	Cond	$+(n^*4)$	<input type="text" value="4"/>	+ 16		
+ Symbols	Flat	$+(n^*6)$	<input type="text" value="1"/>	+ 6		
+ Middle Numbers or Symbols	Flat	$+(n^*2)$	<input type="text" value="4"/>	+ 8		
+ Requirements	Flat	$+(n^*2)$	<input type="text" value="5"/>	+ 10		
Deductions						
- Letters Only	Flat	$-n$	<input type="text" value="0"/>	0		
- Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0		
- Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="8"/>	- 1		
- Consecutive Uppercase Letters	Flat	$-(n^*2)$	<input type="text" value="0"/>	0		
- Consecutive Lowercase Letters	Flat	$-(n^*2)$	<input type="text" value="8"/>	- 16		

Weak password

Test Your Password		Minimum Requirements			
Password:	<input type="password" value="iloveyou143"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols			
Hide:	<input type="checkbox"/>				
Score:	<div>47%</div>				
Complexity:	Good				
Additions		Type	Rate	Count	Bonus
Number of Characters	Flat	$+(n*4)$	<div>11</div>	+ 44	
Uppercase Letters	Cond/Incr	$++((len-n)*2)$	<div>0</div>	0	
Lowercase Letters	Cond/Incr	$++((len-n)*2)$	<div>8</div>	+ 6	
Numbers	Cond	$+(n*4)$	<div>3</div>	+ 12	
Symbols	Flat	$+(n*6)$	<div>0</div>	0	
Middle Numbers or Symbols	Flat	$+(n*2)$	<div>2</div>	+ 4	
Requirements	Flat	$+(n*2)$	<div>3</div>	0	
Deductions					
Letters Only	Flat	$-n$	<div>0</div>	0	
Numbers Only	Flat	$-n$	<div>0</div>	0	
Repeat Characters (Case Insensitive)	Comp	-	<div>2</div>	- 1	
Consecutive Uppercase Letters	Flat	$-(n*2)$	<div>0</div>	0	
Consecutive Lowercase Letters	Flat	$-(n*2)$	<div>7</div>	- 14	
Consecutive Numbers	Flat	$-(n*2)$	<div>2</div>	- 4	
Sequential Letters (3+)	Flat	$-(n*3)$	<div>0</div>	0	