

Task 6

Create a Strong Password and Evaluate Its Strength

Objective

To understand the key features of a strong password, create multiple passwords with varying complexity, evaluate their strength using online tools, and summarize best practices and findings.

Step 1–2: Passwords Created: -

<u>Passwords</u>	<u>Type</u>
Dhoni123#	Very strong
A36Ys@A	Strong
A36Ys@	Good
1234567890987456	Week

Step 3–4: Password Strength Evaluation: -

<u>Passwords</u>	<u>Strength Score (%)</u>
Dhoni123#	83%
A36Ys@A	65%
A36Ys@	58%
1234567890987456	24%

Step 5: Best Practices for Creating Strong Passwords

- Use at least 12–16 characters.
- Combine uppercase, lowercase, numbers, and symbols.
- Avoid personal information (names, birthdays).
- Do not use common or dictionary words.
- Use passphrases that are easy to remember but hard to guess.
- Never reuse passwords across accounts.

Step 6: Tips Learned from Evaluation

- Longer passwords increase strength significantly.
- Random character use adds complexity.
- Passphrases (e.g., 2bOrNot2B@2025!) are both strong and memorable.
- A mix of unrelated words and characters creates strong passwords.
- Password managers help store strong, unique passwords safely.

Step 7: Common Password Attacks

- **Brute Force Attack:** Tries every possible combination; short/simple passwords are easily cracked.
- **Dictionary Attack:** Uses a list of common words and known passwords.
- **Credential Stuffing:** Uses previously leaked credentials to access accounts.
- **Phishing:** Tricks users into revealing passwords through fake websites or messages.

Step 8: How Password Complexity Affects Security

- Simple passwords (like password123) can be cracked in seconds.
- Moderate passwords are better but still vulnerable.
- Strong passwords with complexity and length can resist cracking for years.
- Password complexity and uniqueness significantly reduce the risk of successful attacks.

Screen shorts: -

Test Your Password		Minimum Requirements
Password:	<input type="text" value="A@_wer1t\$\$!"/>	<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>100%</div>	
Complexity:	Very Strong	

Test Your Password		Minimum Requirements
Password:	<input type="text" value="A36yS@A"/>	<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>65%</div>	
Complexity:	Strong	

Test Your Password		Minimum Requirements
Password:	<input type="text" value="A36yS@"/>	<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>58%</div>	
Complexity:	Good	

Test Your Password		Minimum Requirements
Password:	<input type="text" value="1234567890987456"/>	<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>24%</div>	
Complexity:	Weak	

