CYBER SECURITY INTERNSHIP

Task 6: Create a Strong Password and Evaluate Its Strength

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

Tools: Online free password strength checkers (e.g., passwordmeter.com).

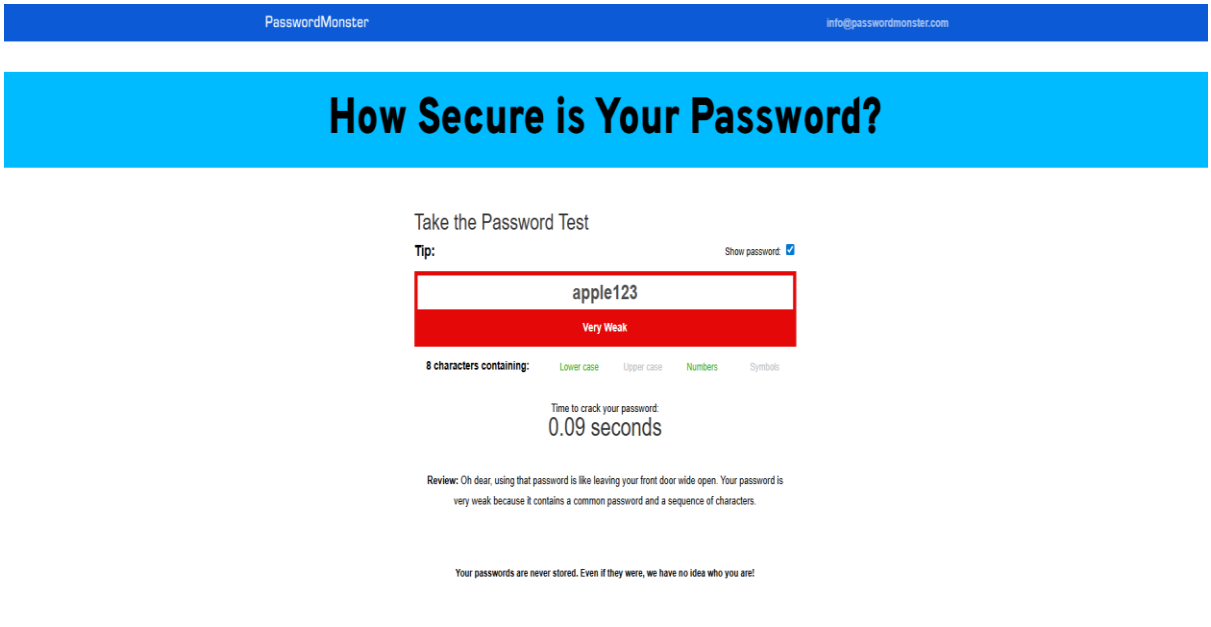
Deliverables: Report showing password strength results and explanation

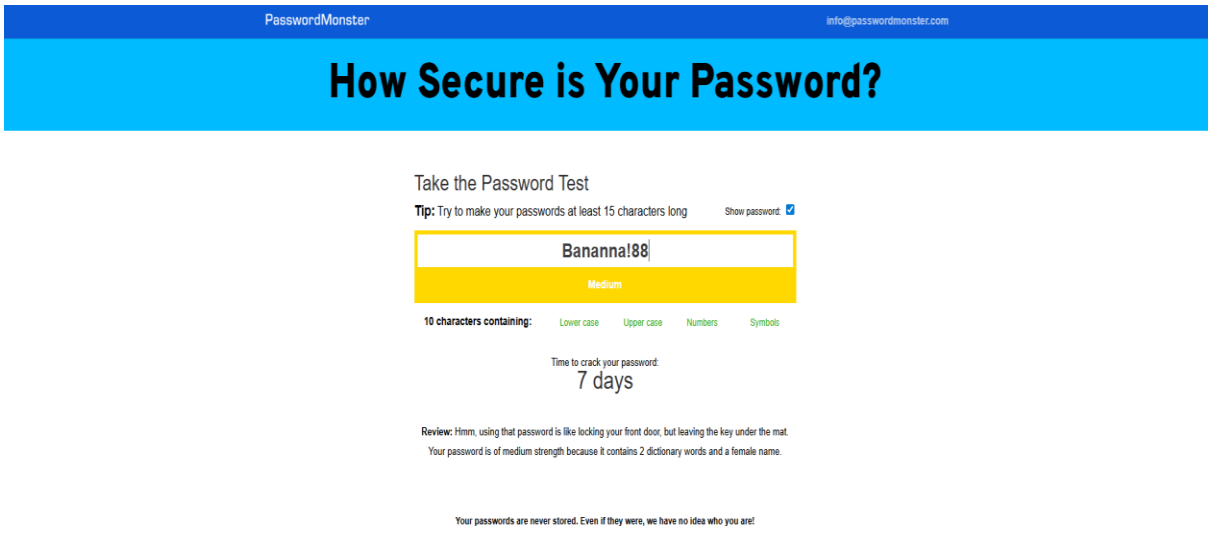
1–2. Generate Multiple Passwords of Varying Complexity

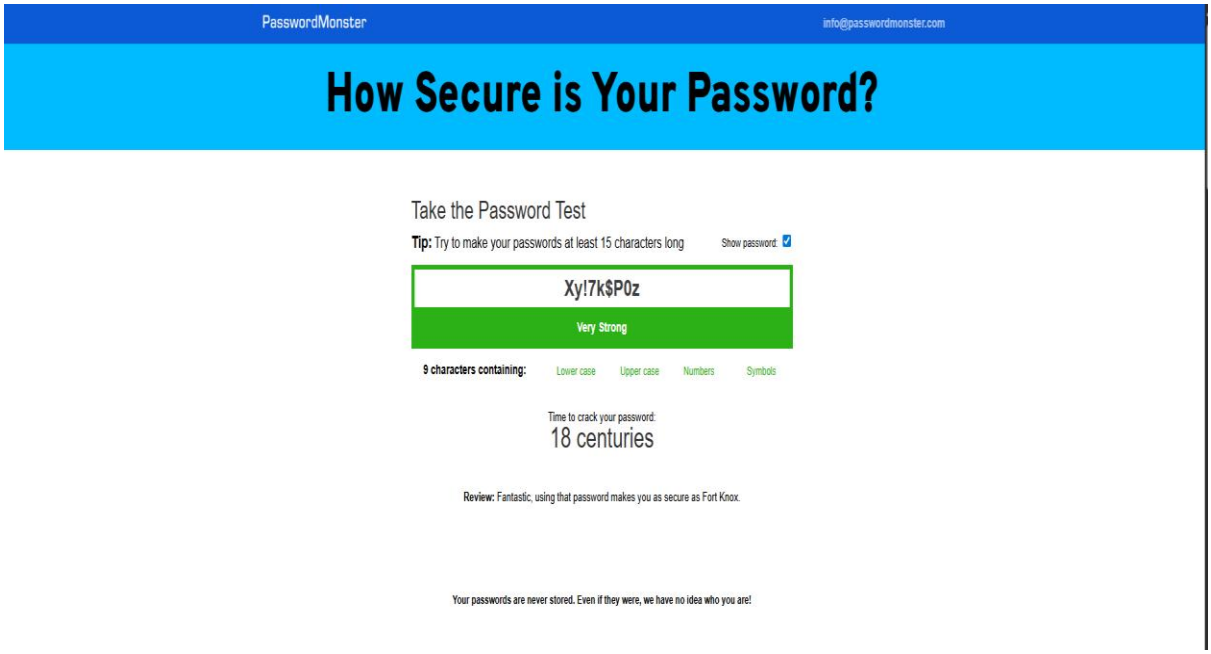
Password	Complexity Level	Features Used
apple123	Low	Lowercase + numbers
Banana!88	Medium	Mixed case + symbol + numbers
Xy!7k$P0z	High	Mixed case + symbols + numbers
7Cq!wLp@N4xM	Very High	Mixed case + symbols + numbers, long length
correcthorsebatterystaple	High (Memorable Phrase)	Long phrase (no symbols or numbers)

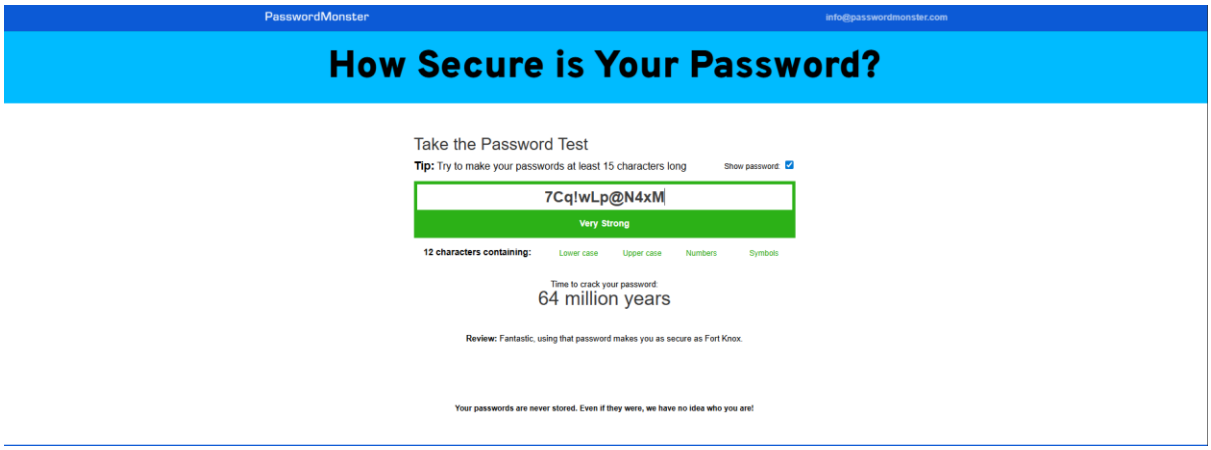
3–4. Test Passwords on a Strength Checker

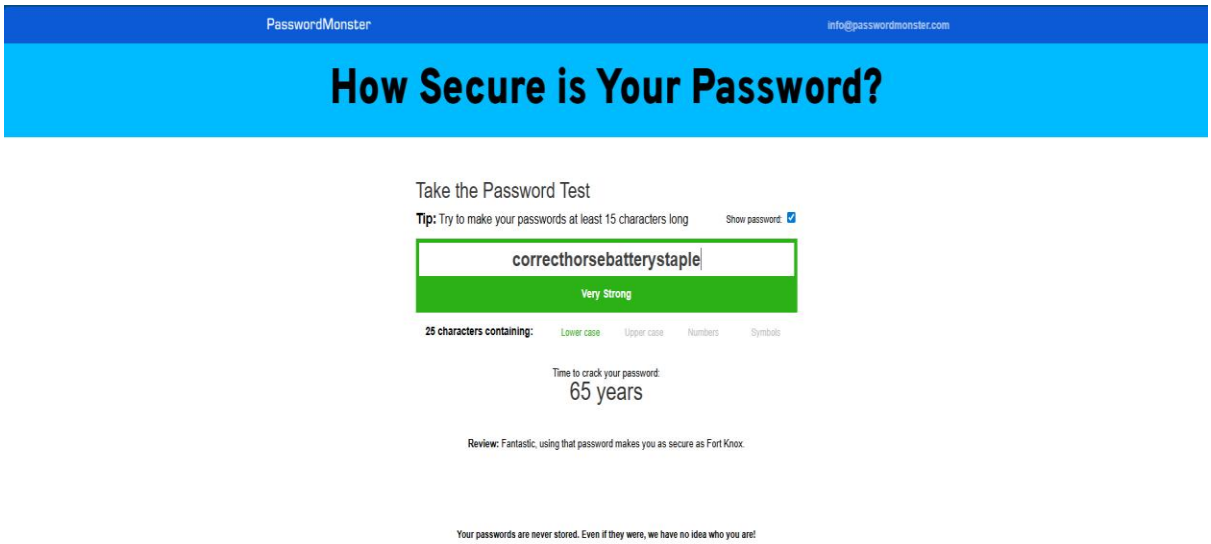
Tool Used: Password Strength Meter


PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip:
Show password:
apple123
Very Weak
8 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
0.09 seconds
Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password and a sequence of characters.
Your passwords are never stored. Even if they were, we have no idea who you are!


PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
Bananna!88
Medium
10 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
7 days
Review: Hmm, using that password is like locking your front door, but leaving the key under the mat. Your password is of medium strength because it contains 2 dictionary words and a female name.
Your passwords are never stored. Even if they were, we have no idea who you are!


PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
Xy!7k$P0z
Very Strong
9 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
18 centuries
Review: Fantastic, using that password makes you as secure as Fort Knox.
Your passwords are never stored. Even if they were, we have no idea who you are!


PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
7Cq!wLp@N4xM
Very Strong
12 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
64 million years
Review: Fantastic, using that password makes you as secure as Fort Knox.
Your passwords are never stored. Even if they were, we have no idea who you are!


PasswordMonster
info@passwordmonster.com
How Secure is Your Password?
Take the Password Test
Tip: Try to make your passwords at least 15 characters long
Show password:
correcthorsebatterystaple
Very Strong
25 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
65 years
Review: Fantastic, using that password makes you as secure as Fort Knox.
Your passwords are never stored. Even if they were, we have no idea who you are!

Password	Estimated Strength	Feedback
apple123	Weak	"Too short and predictable; easy to guess."
Banana!88	Moderate	"Better, but still vulnerable to common attacks."
Xy!7k$P0z	Strong	"Uncommon combination of characters; safer."
7Cq!wLp@N4xM	Very Strong	"Difficult to crack, especially with length."
correcthorsebatterystaple	Strong	"Strong due to length, even though no symbols."

5. **Best Practices for Strong Passwords**

- Use **12+ characters** whenever possible.
- Mix **uppercase, lowercase, numbers, and symbols**.
- Avoid **dictionary words or common phrases**, unless length is extreme (passphrases).
- Do **not reuse passwords** across sites.
- Consider using a **password manager** to store complex passwords securely.

6. Tips Learned from Evaluation

- Password **length** contributes more to strength than symbols alone.
- **Randomness** is more effective than clever patterns (e.g., P@ssw0rd123 is weak).
- **Passphrases** can be both strong and memorable.
- Even complex-looking passwords may be weak if based on patterns or common substitutions.

7. Common Password Attacks

- **Brute Force Attack**: Tries every possible combination. Longer and more complex passwords make this attack impractical.
- **Dictionary Attack**: Uses lists of common words and phrases. Passwords like "banana88" are vulnerable.
- **Credential Stuffing**: Uses leaked usernames/passwords from other sites.
- **Phishing**: Trick users into revealing passwords.

8. Summary: How Password Complexity Affects Security

Password complexity is a major deterrent against automated attacks like brute-force and dictionary attacks. The more characters, types of characters, and randomness used, the harder it is for an attacker to guess or compute the password. Complexity increases **entropy**, which directly correlates with password **strength and resistance to attacks**.