# Password Strength Analysis Report

Generated: Sample report with test results and mock screenshots (for submission/demo purposes).

## 1. What makes a password strong?

A strong password is long, unique, and unpredictable. Key attributes:  
- Length (12+ characters recommended)  
- Mix of uppercase, lowercase letters, numbers, and symbols  
- Avoid dictionary words, names, and predictable patterns  
- Use unique passwords per account  
- Consider a password manager and enable MFA

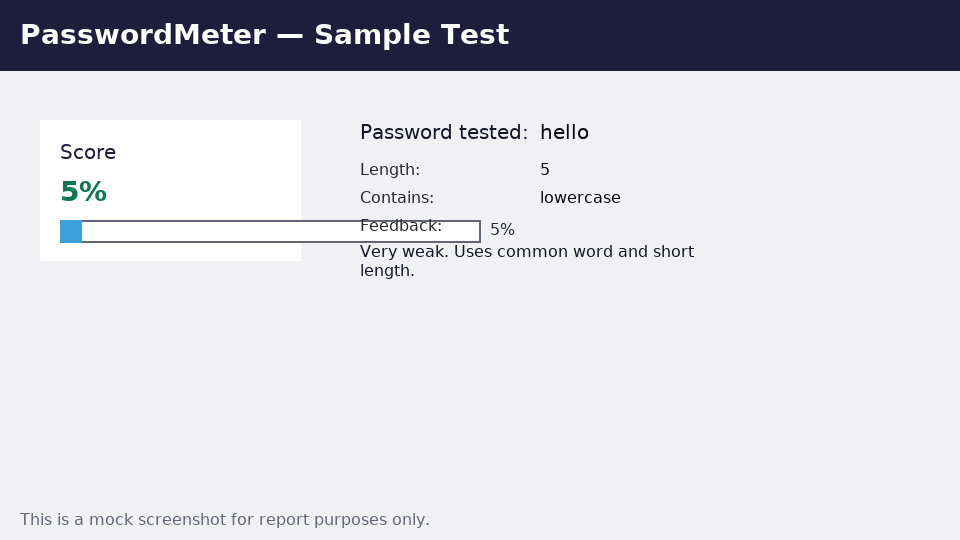
## 2. Passwords Tested & Tool Results

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Length | Score (approx) | Tool Feedback |
| hello | 5 | 5% | Very weak. Uses common word and short length. |
| Hello123 | 8 | 25% | Weak. Predictable pattern; based on common word. |
| H3llo@2025 | 10 | 55% | Medium. Better but still uses a dictionary root. |
| Blu3$Falcon\_M00n!92 | 18 | 95% | Very strong. Long passphrase-like, high randomness. |

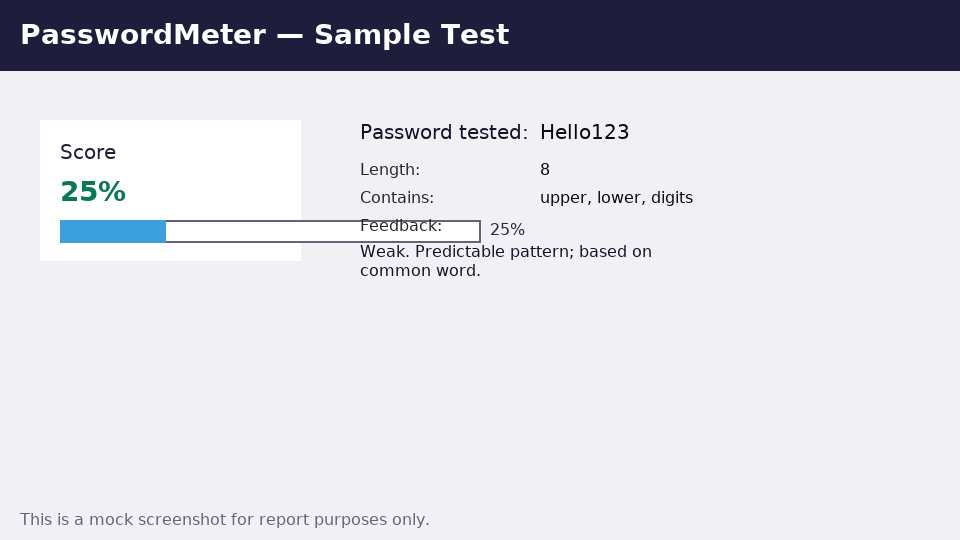
## 3. Screenshots of Password Strength Checker (Mock)

Below are mock screenshots illustrating how results might appear on an online strength checker (for demonstration purposes).

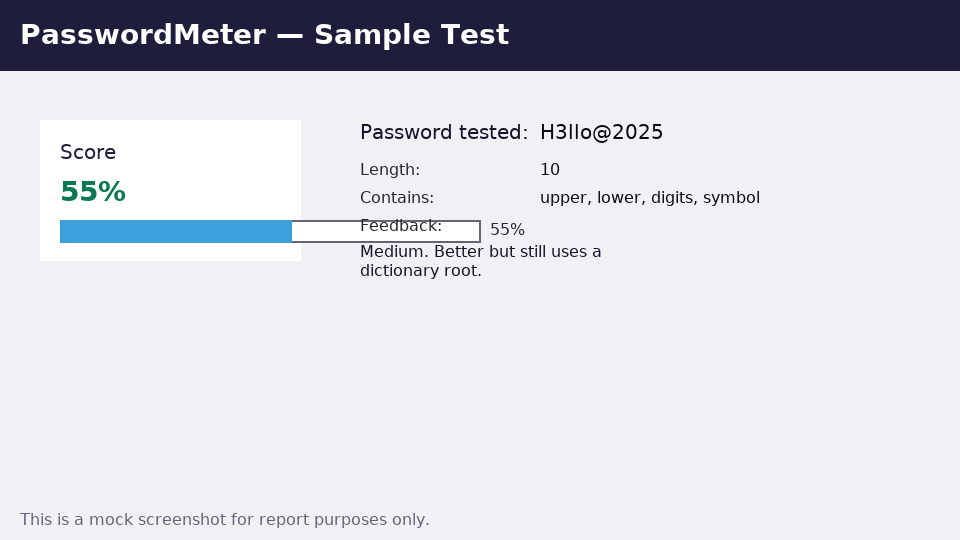
Screenshot 1: hello result



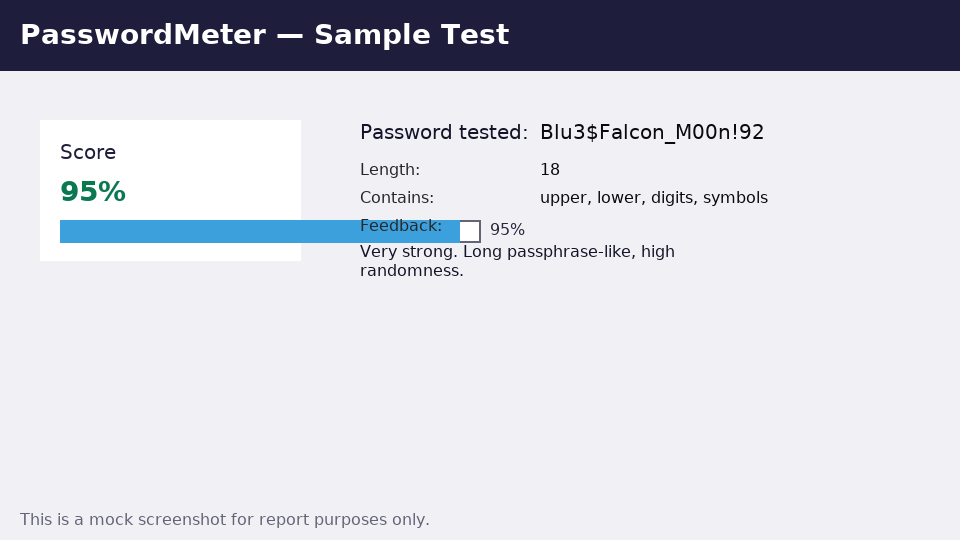
Screenshot 2: Hello123 result



Screenshot 3: H3llo@2025 result



Screenshot 4: Blu3$Falcon\_M00n!92 result



## 4. Best Practices & Tips Learned

- Use passphrases (multiple random words with symbols) for memorability and strength.  
- Aim for length first, then complexity.  
- Avoid simple substitutions on common words (e.g., P@ssw0rd still weak).  
- Use a password manager to generate and store unique passwords.  
- Enable multi-factor authentication wherever available.

## 5. Common Password Attacks (Summary)

Brute-force attacks try all possible combinations; longer passwords exponentially increase time to crack.  
Dictionary attacks use lists of common words and variants; avoid using dictionary words or common patterns.  
Credential stuffing reuses breached username/password pairs; never reuse passwords across sites.  
Phishing and social engineering can bypass strong passwords if users are tricked into revealing them.

## 6. How Complexity Affects Security

Length and randomness are the most important factors. Complexity (mixing character types) increases entropy, but if based on predictable words/patterns, attackers can still succeed. Best defense: long, unique, and random passphrases.