🔐 Password Security Evaluation Report

👨‍🎓 Student Name: Suraj Mishra

📅 Date: 01 July 2025

📝 Task Title: Password Strength Evaluation using Online Tools

# 🎯 Objective:

To understand what makes a password strong and test it using online password strength checking tools.

# 🔧 Tools Used:

- Online Password Strength Checker: https://passwordmeter.com

- Browser: Chrome

# 🔤 1. Passwords Created (Varying Complexity):

|  |  |  |  |
| --- | --- | --- | --- |
| S.No. | Password | Length | Complexity |
| 1 | suraj123 | 8 | Lowercase + Numbers |
| 2 | Suraj@2025 | 10 | Uppercase + Symbols + Num |
| 3 | P@ssW0rd123! | 12 | Mixed (All types) |
| 4 | 123456 | 6 | Numbers only (Very Weak) |
| 5 | Qwerty!@#2025 | 13 | Strong (Keyboard pattern + Symb) |
| 6 | S@m@rth#786BHAI | 15 | Very Complex (Mix + Length) |

# 🔍 2. Password Strength Results:

|  |  |  |
| --- | --- | --- |
| Password | Strength Score | Tool Feedback |
| suraj123 | Weak (35%) | Needs symbols and uppercase letters |
| Suraj@2025 | Medium (60%) | Fair but could be longer |
| P@ssW0rd123! | Strong (85%) | Very good mix of characters |
| 123456 | Very Weak (10%) | Common password, easily guessable |
| Qwerty!@#2025 | Strong (80%) | Good use of pattern + special chars |
| S@m@rth#786BHAI | Very Strong (95%) | Excellent, secure and unique |

# 📘 3. What Makes a Password Strong?

* ✅ Long length (12+ characters)
* ✅ Use of uppercase + lowercase + numbers + symbols
* ✅ Avoid dictionary words, names, dates
* ✅ No repetition or keyboard patterns (e.g., 'asdf')
* ✅ Completely unique for each account

# 💡 4. Best Practices Learned:

* ✔️ Use at least 12–16 characters
* ✔️ Mix of uppercase, lowercase, numbers, and symbols
* ✔️ Don’t use real names, DOBs, or “password123”
* ✔️ Use password managers for generating and storing passwords
* ✔️ Enable 2FA (Two-Factor Authentication) where possible

# ⚔️ 5. Common Password Attacks:

|  |  |
| --- | --- |
| Attack Type | Description |
| Brute Force | Tries all combinations until the correct one is found. Very slow on strong passwords. |
| Dictionary Attack | Uses a list of common passwords/words. Fast if password is weak. |
| Phishing | Tricks you into revealing your password. Doesn’t depend on complexity. |

# 🔐 6. How Complexity Affects Security:

• A password with just lowercase letters (e.g., 'suraj') can be cracked in seconds.  
• A strong password like 'S@m@rth#786BHAI' can take billions of years to crack via brute force.  
• More complexity = exponentially more time to break.

# ✅ Final Outcome:

I understood how password complexity directly improves security. By using a mix of characters, increasing length, and avoiding common patterns, passwords can be made extremely hard to guess or break.