Task 6 – Password Strength Evaluation Report

# 1. Objective:

To evaluate different types of passwords using online strength checker tools.

# 2. Tools Used:

• https://www.passwordmeter.com

# 3. Password Strength Results:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Password | Score | Complexity | Feedback |
| 1 | 1234 | 4% | Very Weak | Only numbers, short length |
| 2 | sunmoon | 7% | Very Weak | Only lowercase, no symbol or number |
| 3 | appleRail22@12 | 100% | Very Strong | Perfect mix of characters |
| 4 | apple22@12 | 74% | Strong | Missing uppercase letter |
| 5 | apple22 | 28% | Weak | No symbol, no uppercase |

# 4. Tips for Strong Passwords:

• Use at least 12 characters

• Add uppercase + lowercase letters

• Add numbers and symbols

• Avoid dictionary words

• Don’t reuse passwords

• Use passphrases or password managers

# 5. Password Attacks Overview:

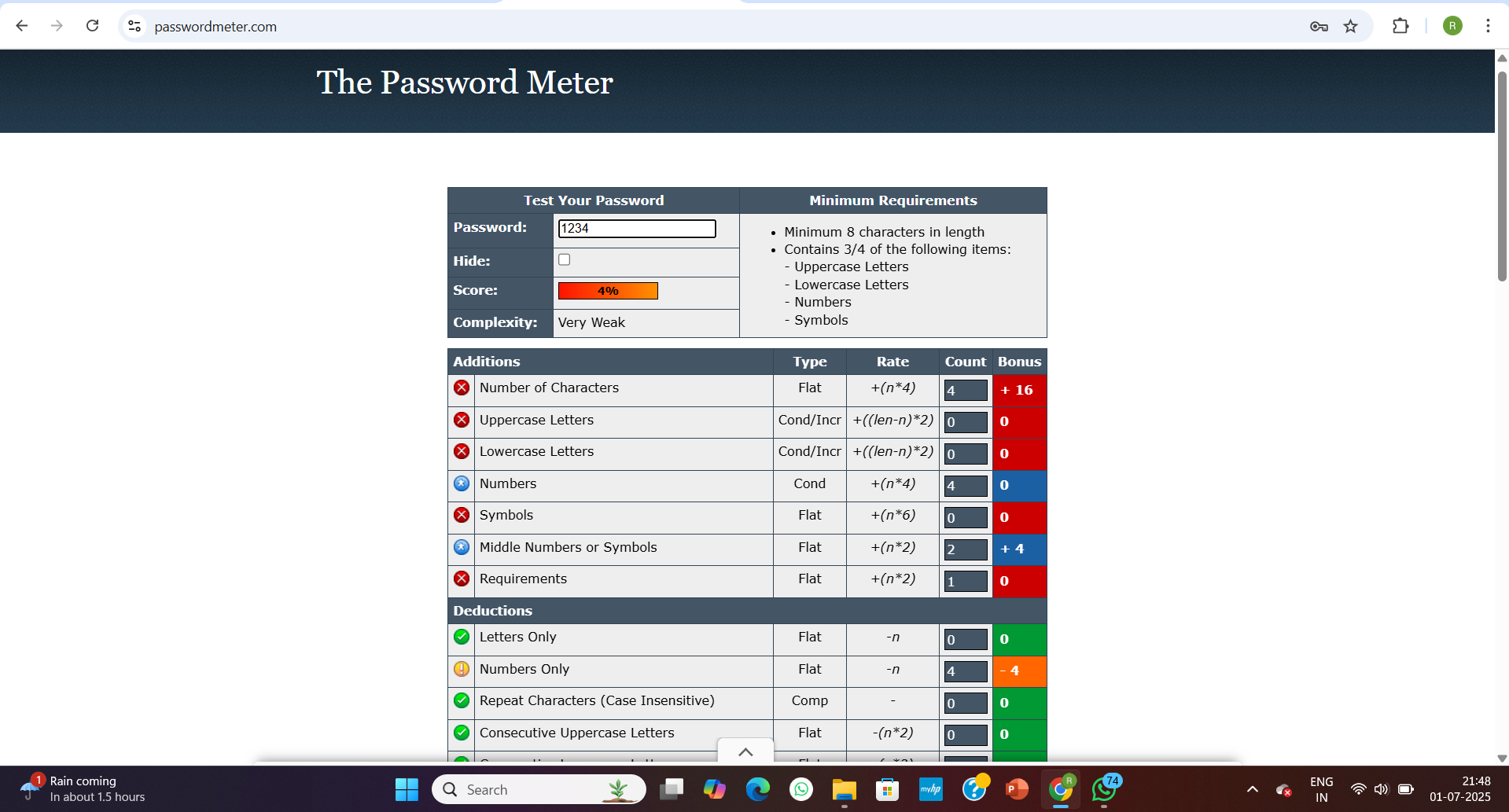
• Brute Force Attack: Tries all combinations; effective but slow.

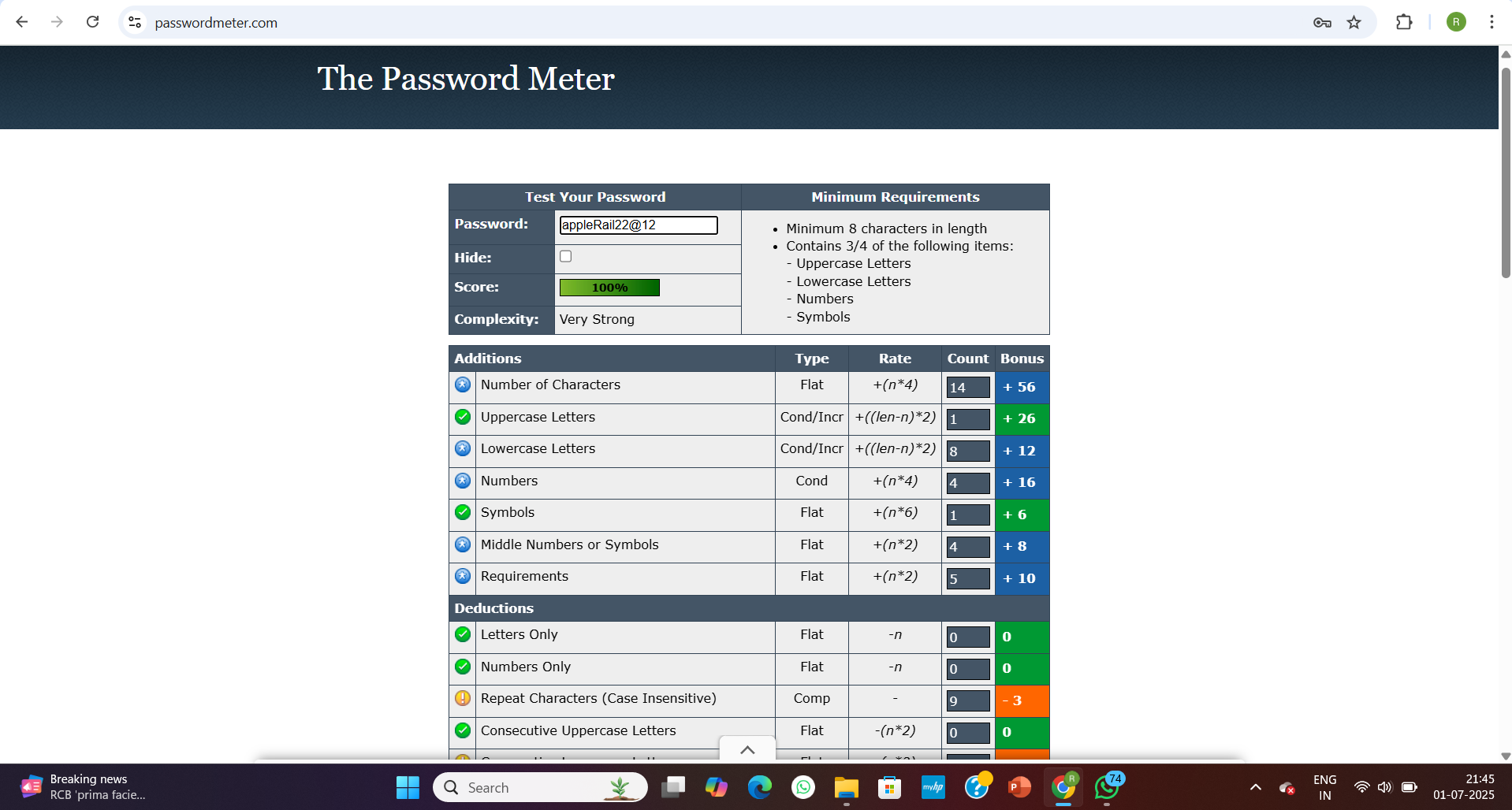
• Dictionary Attack: Uses list of common words; faster than brute force.

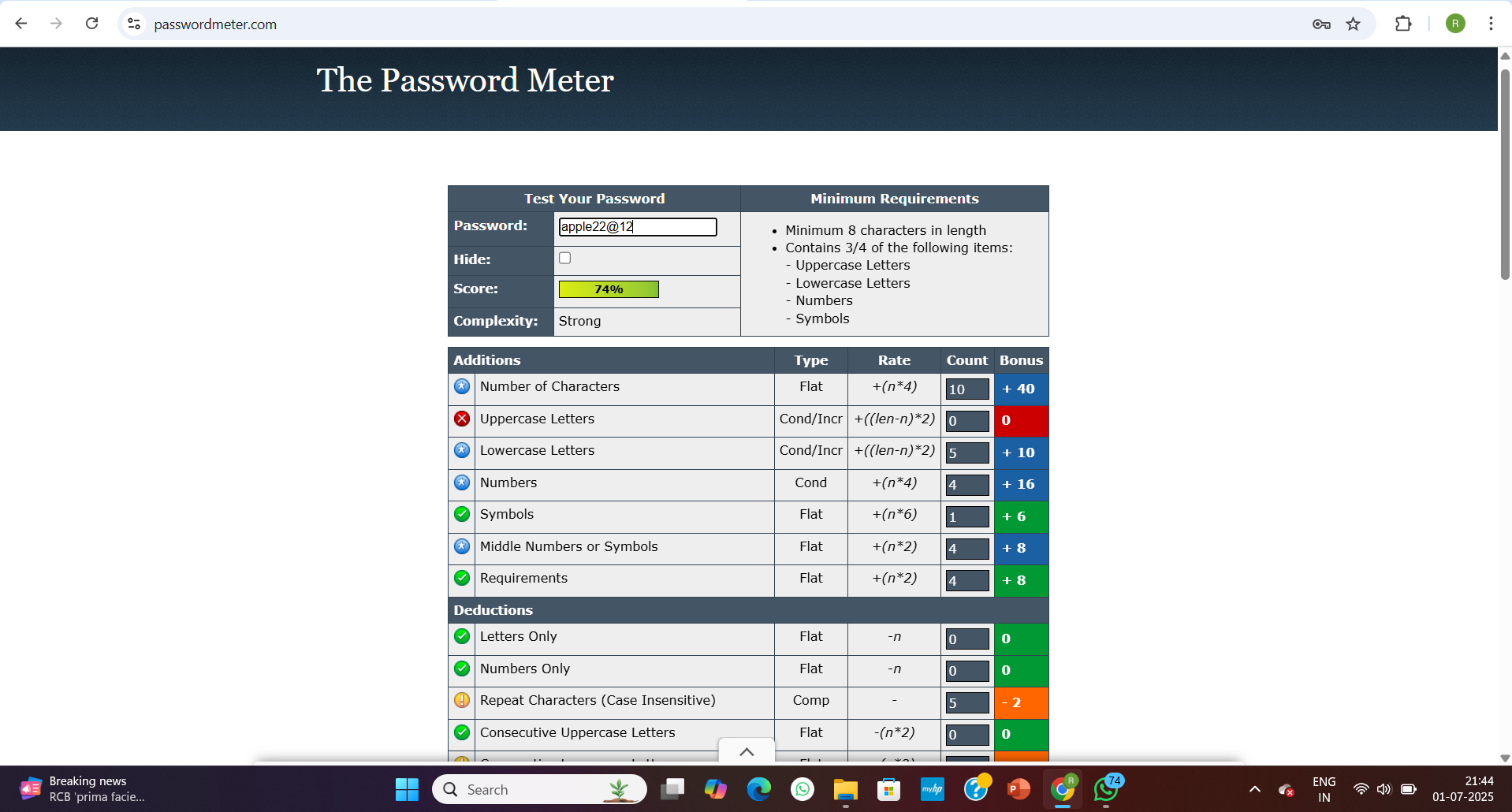
• Credential Stuffing: Uses leaked password data from breached websites.

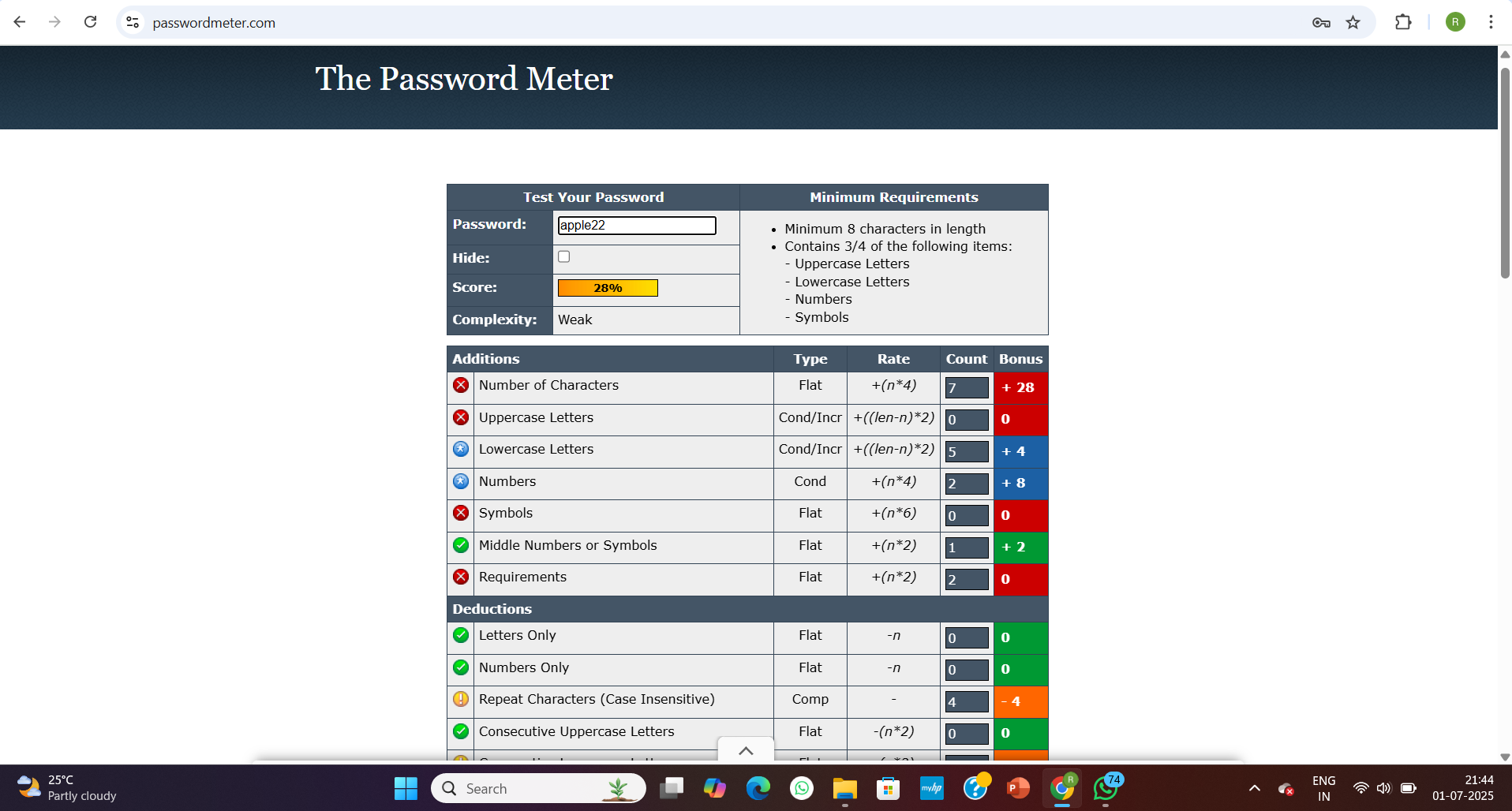
# 6. Screenshots:

Screenshots of the password strength evaluations are included separately.





# 7. feedback:

The website <https://www.passwordmeter.com> is a highly useful tool for evaluating the strength of passwords in real-time. It provides a clear and user-friendly interface where users can input passwords and instantly receive a percentage score along with a complexity rating such as "Very Weak", "Weak", "Strong", or "Very Strong". One of its best features is the detailed breakdown it gives—showing what components (like uppercase letters, symbols, or numbers) are present or missing, and how each element contributes positively or negatively to the overall score. The additions and deductions section is especially helpful for understanding the logic behind password scoring. However, the tool does not provide an estimated time to crack the password, which could have added extra insight into its security. Additionally, while the interface is functional, it lacks modern visual cues or graphical feedback that could enhance user experience. Despite that, the website performs well, is entirely client-side (meaning passwords are not sent to a server), and is an excellent resource for learning about password complexity during cybersecurity tasks. Overall, PasswordMeter.com is reliable and educational, making it ideal for internship projects and security awareness.