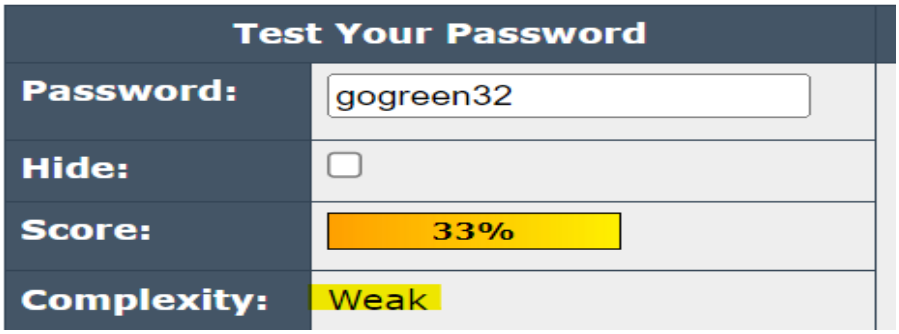
Cyber Security Internship

Task 6 – Create a strong password and evaluate its strength

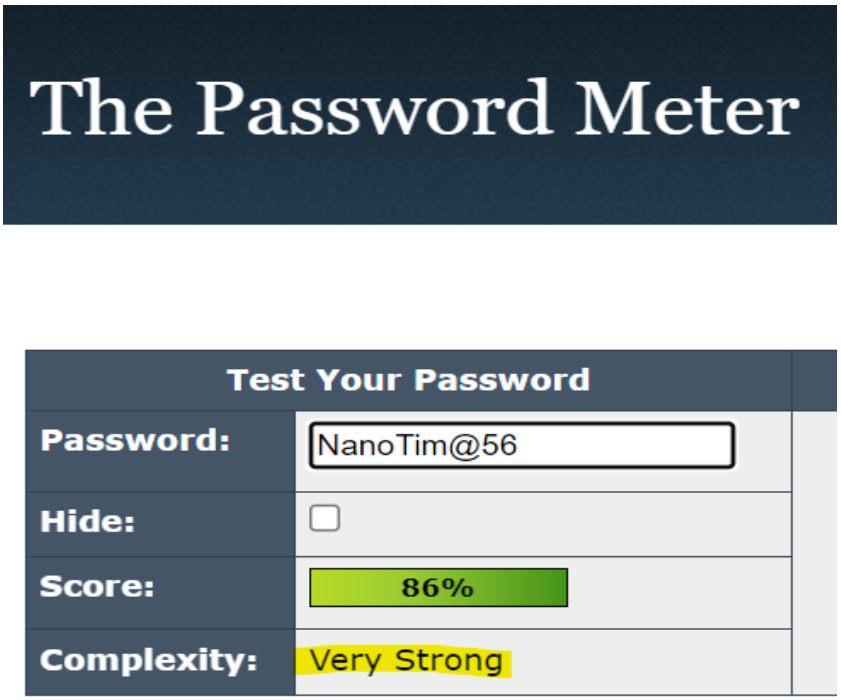
1. Creating multiple passwords with varying complexity:
   - gogreen32 — lowercase + simple numbers
   - NanoTim@56 — upper + lower + numbers + symbol
   - qert@#WER — mixed random
   - ASnjbvgWE@!BH — highly complex
   - password@1 — common pattern

2. Evaluating the above passwords with a free password strength checker tool:

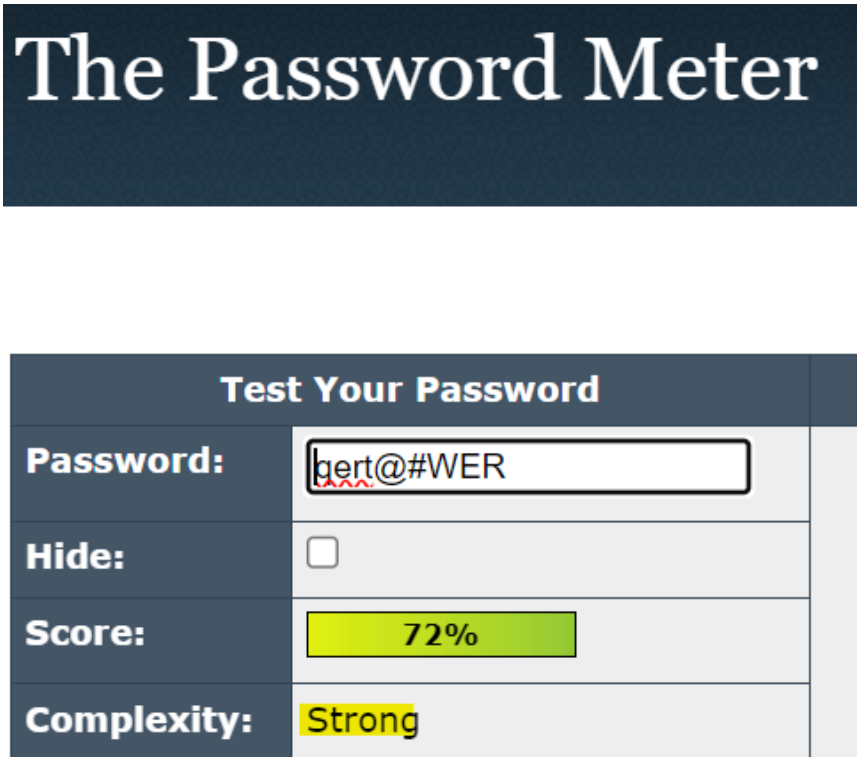
   - Password 1 – gogreen32



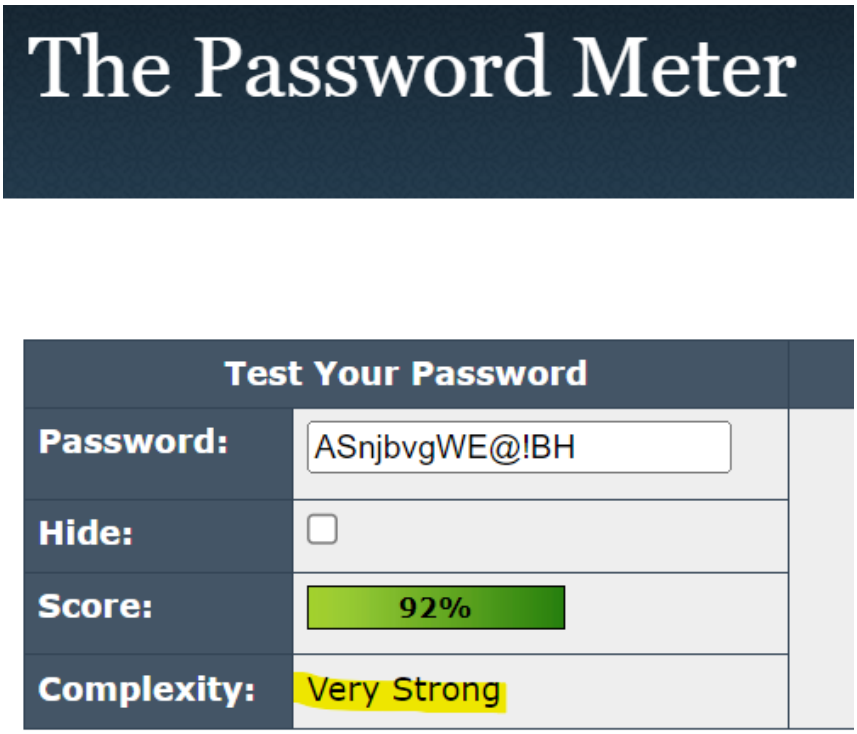
- Password 2 - NanoTim@56



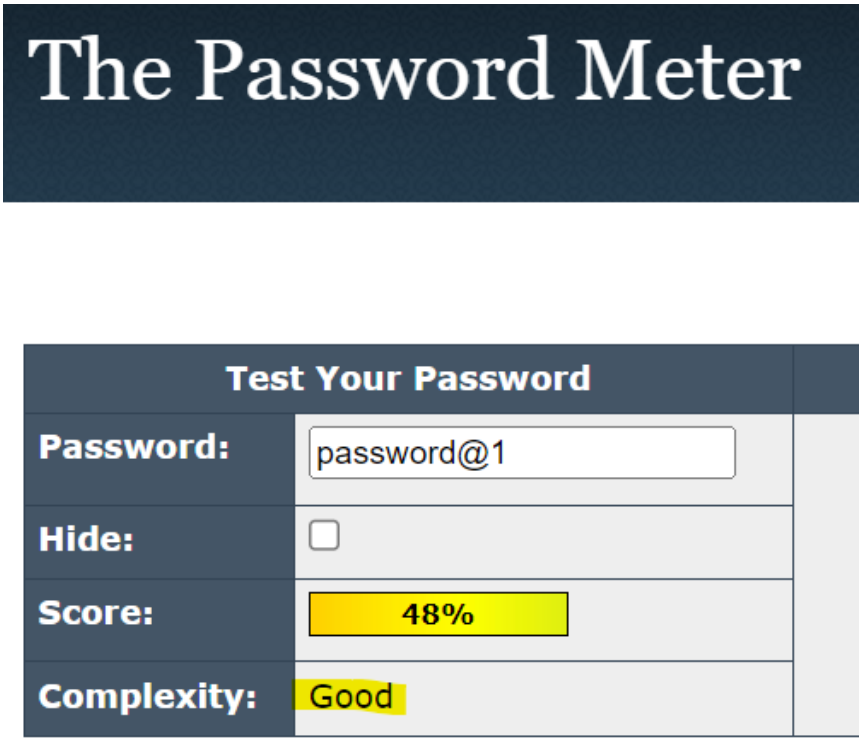
- Password 3 - qert@#WER



- Password 4 - ASnjbvgWE@!BHS



- Password 5 – password@1



3. By analyzing the test passwords, we had identified some best practices for strong passwords
   - Use **12-16+** characters
   - Include **uppercase + lowercase + numbers + symbols**
   - Avoid **dictionary words, names, dates & patterns**
   - Never use: **password123, Admin@123, welcome@2026**
   - Use **random string generators or password managers**
   - Use **unique passwords** for every site
   - Enable **2FA/MFA** wherever possible
   - Prefer **passpharses** like: **Con-tect-342-@**

4. From the above evaluations we had learned:
   - Password length increases security more than complexity alone
   - Dictionary words drastically reduce strength even if symbols are added
   - Randomized patterns outperform meaningful words
   - Common password formats are frequently used and quickly cracked
   - High entropy = long cracking time
   - Password strength checkers penalize:
     1) Repetitive patterns
     2) Sequential numbers or letters
     3) Known common words
5. Researching some Common Password Attacks:

   A. Brute Force Attack:

   → Attackers tries every possible combination

   → Short/ simple passwords can be easily cracked

   → long random passwords are almost impossible

   B. Dictionary Attack:

   → Uses a list of common words and variations

   → Passwords like Nick123. password@123

   C. Credential Stuffing

   → If one account is breached, attackers use the same password on other sites

D. Hybrid Attack

→ Combination of dictionary and random modifications

→ Example trying “Password@123” instead of “Password”

6. This is how password complexity affects in a security posture:

   Higher Complexity = Higher Entropy = Longer Crack Time