Task 6 – Password Strength Evaluation

Author: Anshikaa Pahilajani

Cyber Security Internship — Elevate Labs

Date: 30 September 2025

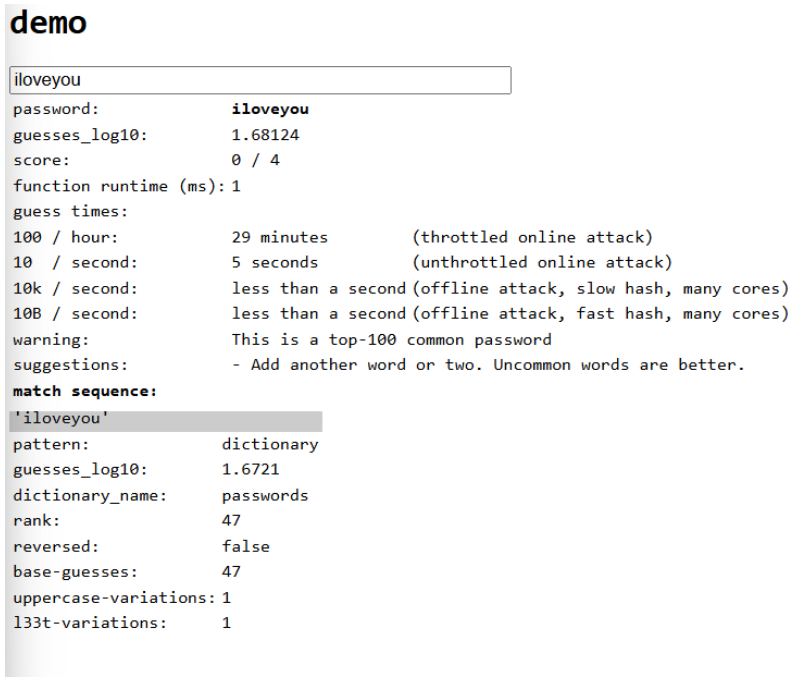
Introduction

Passwords are the first line of defense for securing accounts and sensitive data. Weak passwords are highly vulnerable to attacks such as **brute force** and **dictionary attacks**, while strong passwords reduce these risks.
In this task, I created different types of passwords, tested their strength using the [tryzxcvbn demo (Dropbox's zxcvbn estimator)], and recorded the results.

Password Testing Results

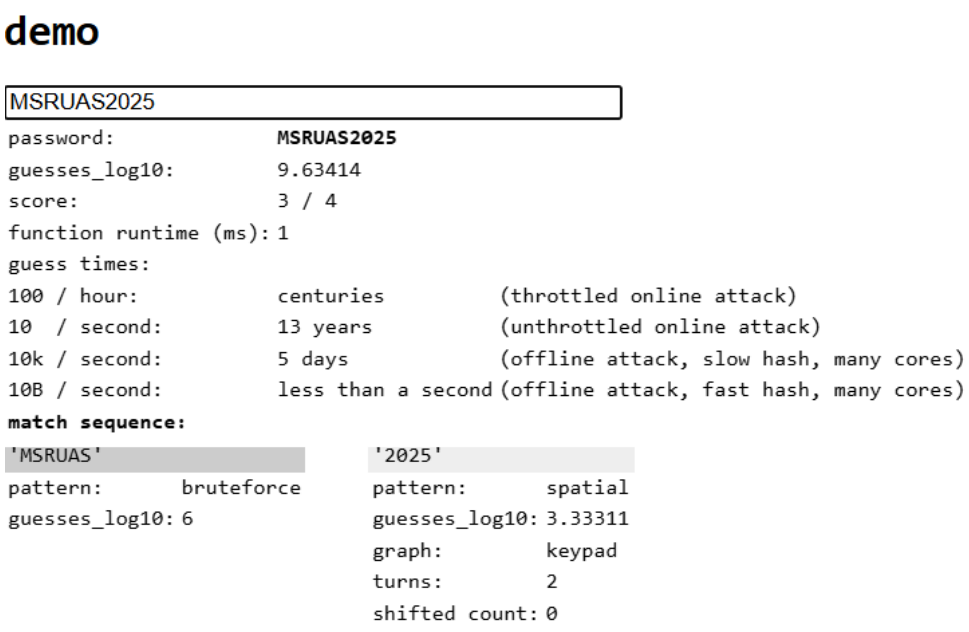
Password 1: qwerty

Password 2: iloveyou



Password 3: Admin@123

Password 4: MSRUAS2025



Password 5: India#75

demo

India#75

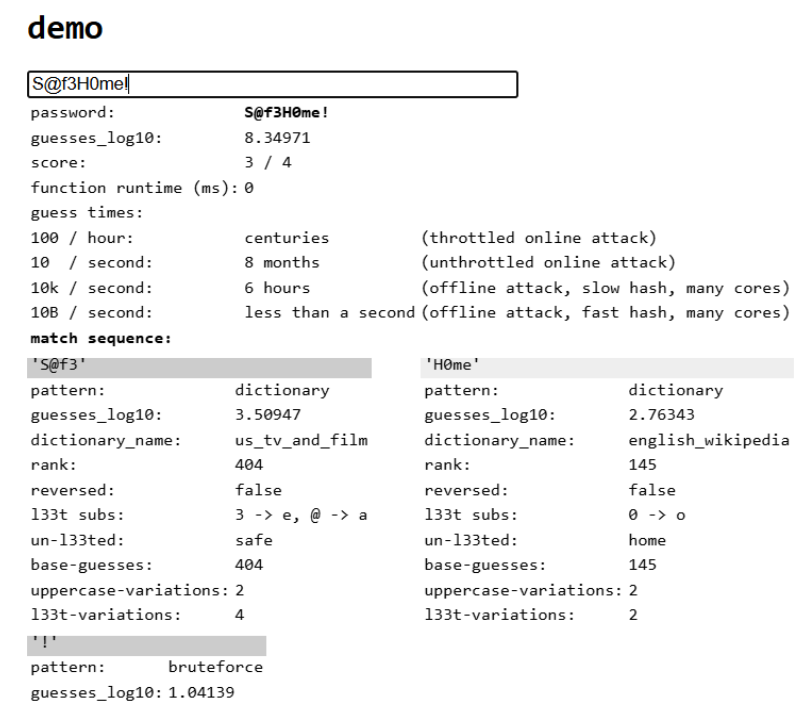
password: **India#75**
guesses_log10: 6.11461
score: 2 / 4
function runtime (ms): 1
guess times:
100 / hour: 1 year (throttled online attack)
10 / second: 2 days (unthrottled online attack)
10k / second: 2 minutes (offline attack, slow hash, many cores)
10B / second: less than a second (offline attack, fast hash, many cores)
suggestions:
- Add another word or two. Uncommon words are better.
- Capitalization doesn't help very much

match sequence:

'India'
pattern: dictionary
guesses_log10: 2.81023
dictionary_name: english_wikipedia
rank: 323
reversed: false
base-guesses: 323
uppercase-variations: 2
l33t-variations: 1

'#75'
pattern: bruteforce
guesses_log10: 3

Password 6: S@f3H0me!



demo

S@f3H0me!

password: **S@f3H0me!**
guesses_log10: 8.34971
score: 3 / 4
function runtime (ms): 0
guess times:
100 / hour: centuries (throttled online attack)
10 / second: 8 months (unthrottled online attack)
10k / second: 6 hours (offline attack, slow hash, many cores)
10B / second: less than a second (offline attack, fast hash, many cores)

match sequence:

'S@f3'
pattern: dictionary
guesses_log10: 3.50947
dictionary_name: us_tv_and_film
rank: 404
reversed: false
l33t subs: 3 -> e, @ -> a
un-l33ted: safe
base-guesses: 404
uppercase-variations: 2
l33t-variations: 4

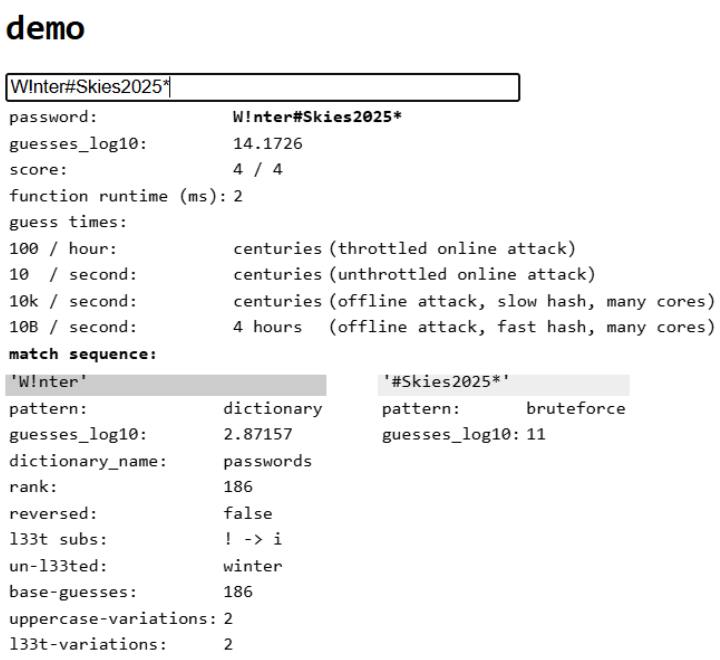
'H0me'
pattern: dictionary
guesses_log10: 2.76343
dictionary_name: english_wikipedia
rank: 145
reversed: false
l33t subs: 0 -> o
un-l33ted: home
base-guesses: 145
uppercase-variations: 2
l33t-variations: 2

'!'
pattern: bruteforce
guesses_log10: 1.04139

Password 7: Tr@vel#Fun2025

Password 8: R3d!Lotus$88

Password 9: W!nter#Skies2025*



Password 10: MyC@t$Sleeps!UnderTheSun#2025

Password Guidelines Learned

From the password strength tests, the following **best practices** were identified:

1. **Length matters** – passwords with 12+ characters are significantly stronger.
2. **Use all character types** – uppercase, lowercase, numbers, and symbols.
3. **Avoid dictionary words** – common words and phrases are easily guessed.
4. **Don’t reuse passwords** across different accounts.
5. **Passphrases are powerful** – multiple random words with symbols/numbers are easy to remember but hard to crack.
6. **Update passwords regularly** to reduce risk from breaches.
7. **Use a password manager** to generate and store strong, unique passwords.
8. **Enable Multi-Factor Authentication (MFA)** for extra protection.

Conclusion

Testing different passwords showed how quickly weak ones can fail against strength checks and how well-designed passwords resist attacks. By combining **length, randomness, and complexity**, and using **passphrases + MFA**, users can create secure passwords that protect accounts effectively.