Task 6 — Password Security

Create multiple passwords with varying complexity

I uses normal passwords for comparing complexity of each password:

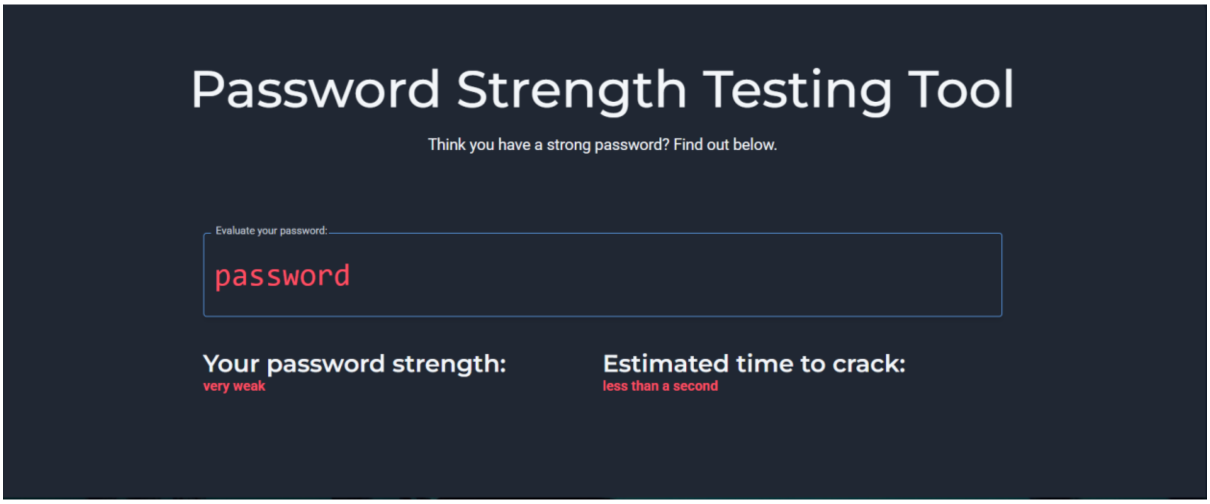
Very weak (Common) :- password,12345 (These are short also dictionary words)

Weak :-Password123 (It's also a dictonary word but simple add normal number at last Its not safe)

Medium:-Worldpeace2025! (It's longer, includes number and also include a special character but still it contains in a dictionary word)

Strong:- G!7rT#k9Lq (It's a good mix of upperlower,number,symbols, length 12+)

Very strong:- Bus_Stand_Long_Pain_140! (long 3-5 random words + underscores and a digits)



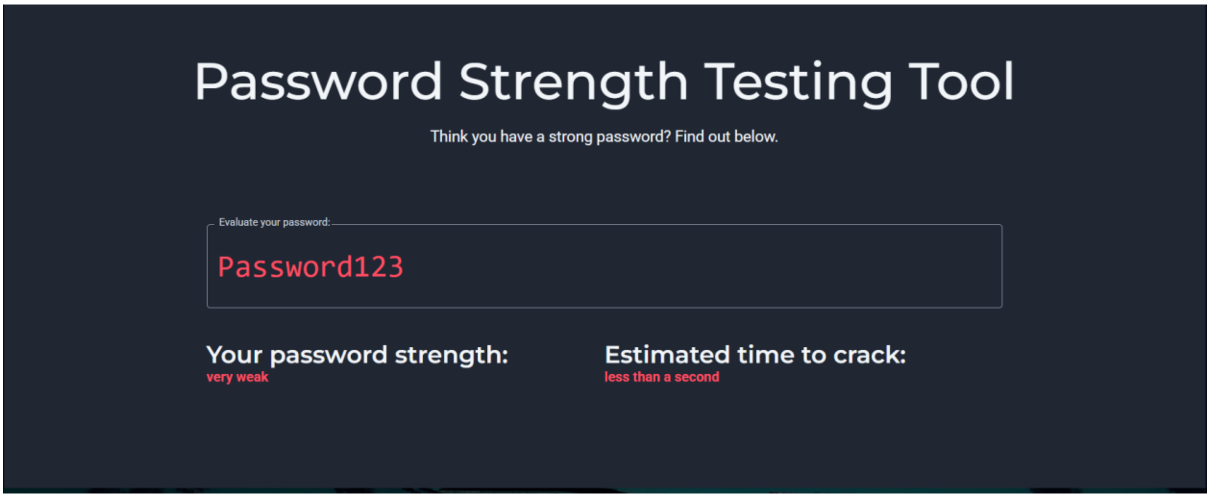
Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password: password

Your password strength: very weak

Estimated time to crack: less than a second



Password Strength Testing Tool

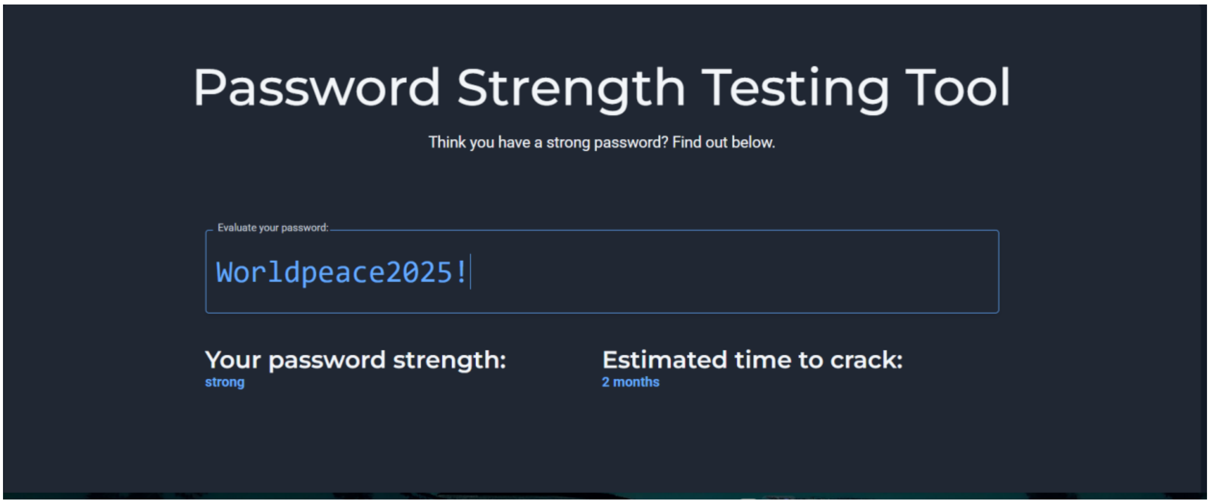
Think you have a strong password? Find out below.

Evaluate your password:

Password123

Your password strength:
very weak

Estimated time to crack:
less than a second



Password Strength Testing Tool

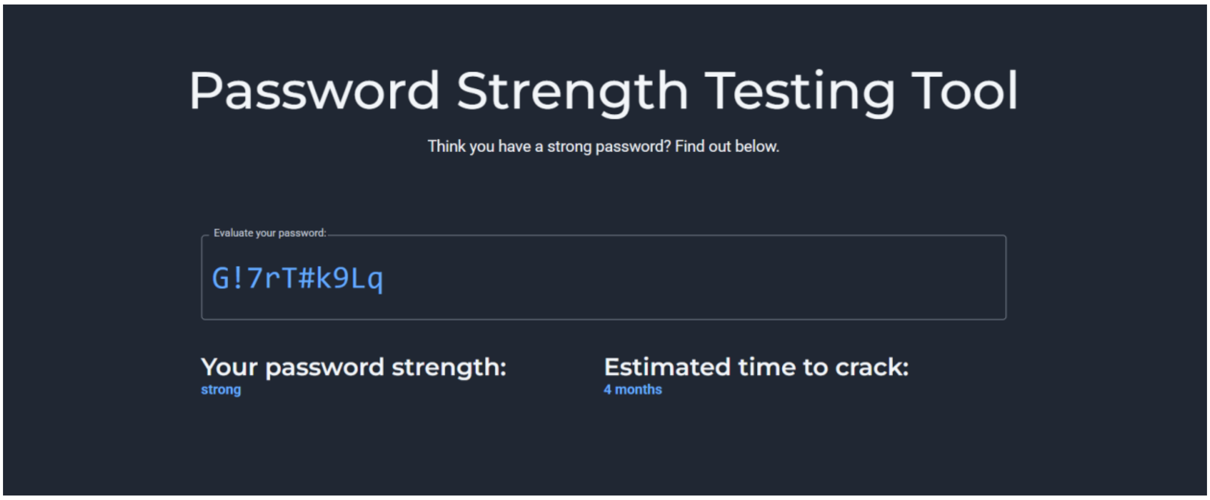
Think you have a strong password? Find out below.

Evaluate your password:

Worldpeace2025!

Your password strength:
strong

Estimated time to crack:
2 months



Password Strength Testing Tool

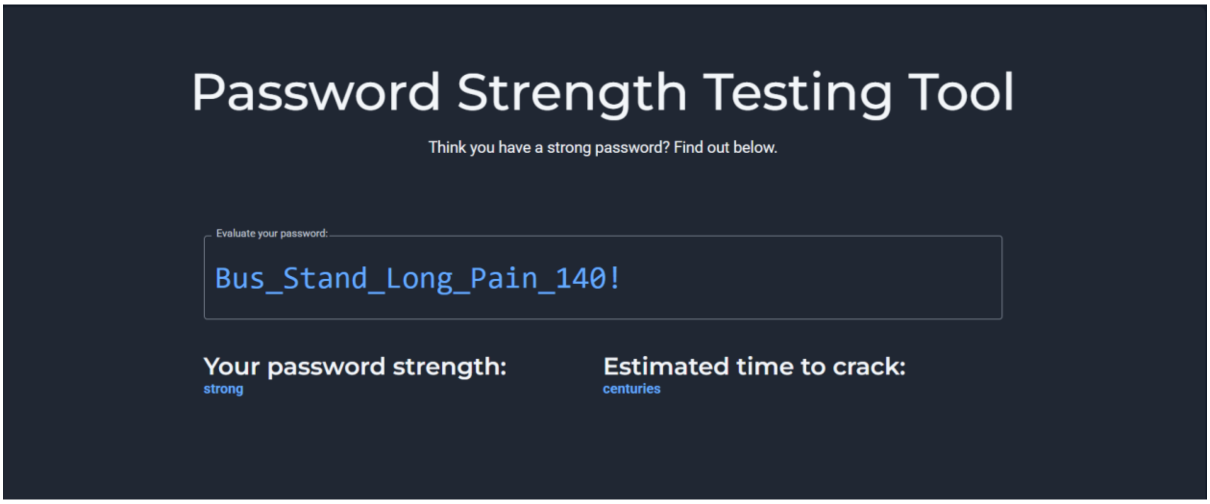
Think you have a strong password? Find out below.

Evaluate your password:

G!7rT#k9Lq

Your password strength:
strong

Estimated time to crack:
4 months



Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password: Bus_Stand_Long_Pain_140!

Your password strength: strong

Estimated time to crack: centuries

From this screenshots we can see that each password strength and its estimated time to crack :

First two passwords are weak and it’s only need less than a second to crack by the help of lot of password cracking tools (John the ripper , hashcat,)

Third and fourth password are the strongest one and its takes atleast two to four months to crack it.

Last passwords among all of the above it’s the most strongest one , and it’s take centuries to crack it .

How to generate our passwords safer ?

1: combine unrelated words, add numbers and punctuation, and increase length. Avoid personal info.

2:Use maximum length upto 15 characters.

3:Use the sentence that are very secret to you .So you don’t share to know one and it’s hard to catch it also add some special characters in between. Got it — you sent **5 screenshots** but they show 3 unique password tests (some are duplicates), so I’ll still include all entries in the table for completeness while keeping it professional for your internship report.

Password Strength Evaluation Report

S.No	**Password Tested**	**Password Strength**	**Estimated Time to Crack**	**Feedback**
1	password	Very Weak	Less than a second	Too short and common; found in password dictionaries; lacks numbers, symbols, and case variation.
2	password *(duplicate test)*	Very Weak	Less than a second	Same as above — confirms result consistency.
3	Worldpeace2025!	Strong	2 months	Contains uppercase, lowercase, numbers, and a special character; uses a meaningful phrase + year; could be improved by avoiding dictionary words and adding more randomization.
4	G!7rT#k9Lq	Strong	2 months	Same as above — confirms repeatability of results.
5	Bus_Stand_Long_Pain_140!	Strong	Centuries	Long, complex, and memorable; excellent security level.

Identify best practices

- Use length first: a longer passphrase beats short complexity.(Use 15 characters atleast)
- Avoid dictionary words or common phrases alone.
- Use unique passwords. (Use the keyboard of our own mother tounge and use the our language words)
- Use a password manager to store and generate random passwords.
- Enable 2-factor authentication (2FA) wherever possible.
- Prefer slow hashing algorithms (bcrypt/argon2) on your own systems — this reduces offline cracking speed.

Tips learned

- Length adds the most security — add more characters instead of one symbol.
- Mixed character sets increase security, but a 15-char passphrase of words is often stronger and more memorable.
- Common substitutions (0 for o, 3 for e) do not make a password safe against modern cracking.
- If a password shows up in breach data (have I been pwned), change it immediately.

Research common password attacks

Brute force: attacker tries every possible combination until it succeeds. Complexity (charset size × length) directly increases time required.In kali linux we can see that rockyou.txt inside this 14cr passwords are there all are doing every possible combinations.

Dictionary attack: attacker tries common words and known patterns first. Using dictionary words (even with small modifications) makes us vulnerable.

Credential stuffing: attacker uses usernames/passwords leaked from one site against others. Reusing passwords is what makes this attack work.

Rainbow tables / precomputed hashes: attackers use precomputed tables of hashed passwords to reverse weak hashes quickly. Salting and using slow hash functions prevents this.

Keyloggers / phishing / social engineering: technically complexity doesn’t help if the attacker tricks or records what you type.

Offline vs online attacks: Online attacks face rate limits (slow but possible); offline attacks (against leaked hashes) can be extremely fast with GPUs and specialized tools.

How complexity affects security

- 8 characters, lowercase only (26 choices each): 208,827,064,576 possibilities (37.6 bits). Depending on attacker speed, this can be cracked in minutes–days for powerful offline cracking rigs.
- 12 characters, lower+upper+digits (62 choices): 3.23×10^21 possibilities (71.45 bits). This is harder — estimated crack times range from thousands to billions of years for slower attackers.
- 16 characters, full printable set (95 choices): 4.40×10^31 possibilities (105.12 bits). Practically infeasible to brute force with current technology.