



# Password Security Assessment Tool for Small Businesses

Author: Kelmit Rivera Rivera  
Advisor: Jeffrey Duffany, Ph.D.  
Master in Computer Science  
Graduate Project EXPO, May 2026

## Abstract

I created a simple assessment tool to use in the browser so that small businesses can check their passwords and get a sense of their relative strength. They can also see how a password if currently used online could be improved. The assessment tool provides a simple security score based on the estimated time it would take to crack the password, and provide recommendations as shown in Figure 2. It also reports the classification of the password as weak, moderate or strong as shown in Table 2. The passwords themselves are not generated, stored, transmitted or processed.

## Introduction

With passwords still being used for many business systems, email accounts, cloud services and administrative login accounts and more, opportunities for a bad actor to gain unauthorized access continue to exist. This project is meant to be a straightforward application to help raise a user's awareness of their password's exposure risk and offer some simple features to test password security in specific scenarios as shown in Table 3.

## Background

As shown in Table 4, a weak password is typically easy to guess for a number of reasons. It is short and comprised of simplistic, familiar words. A keyboard pattern password is easy to guess as well as a password with repeated characters. Passwords with numbers but in a very obvious pattern is also a characteristic of weak passwords. Small businesses lack sophisticated identity tools and have no formal password guidelines for employees. NIST, CISA, FTC, and Verizon have published guidelines.

## Problem

Small businesses require an easy approach for allowing end users to realize what kind of weak password behavior they are following, and how to change it to a strong password using the assessment criteria as shown in Table 1 & 2.

## Methodology

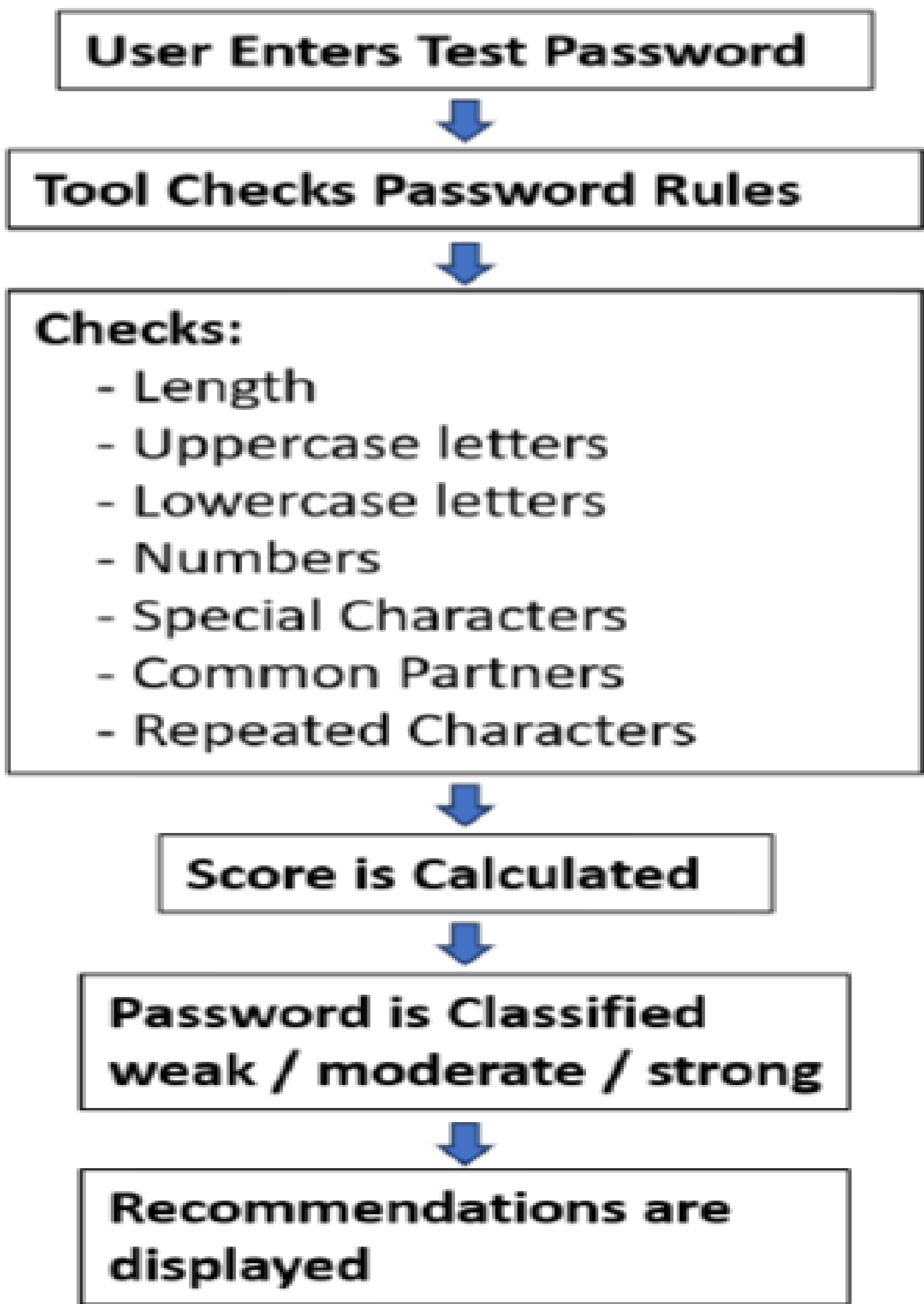
Table 1: Password Assessment Criteria

| Criteria                     | Description                                                   | Score |
|------------------------------|---------------------------------------------------------------|-------|
| Length 12 or more characters | Longer passwords reward more points                           | 25    |
| Uppercase letters            | Detects A-Z letters                                           | 10    |
| Lowercase letters            | Detects a-z letters                                           | 10    |
| Numbers                      | Detects numbers used                                          | 10    |
| Special characters           | Detects the use of symbols                                    | 10    |
| No common patterns           | Avoids the use of admin, password, qwerty, or 12346           | 20    |
| No repeated characters       | Avoids the use of repeated letters or numbers like aaa or 777 | 10    |

Table 2: Password Strength Classification

| Score  | Classification | Password Results   |
|--------|----------------|--------------------|
| 0-39   | Weak           | Not recommended    |
| 40-69  | Moderate       | Needs improvement  |
| 70-100 | Strong         | Satisfies Criteria |

Figure 1: Password Assessment Workflow



## Results and Discussion

Figure 2: Password Assessment Tool Interface with Weak Password Results

### Enter a Test Password

Do not enter real passwords. This tool is for test passwords only.

Analyze Password Clear

### Assessment Result

Score: 30/100  
Classification: **Weak**

### Password Checklist

- Password is shorter than 12 characters.
- Password does not contain uppercase letters.
- Password contains lowercase letters.
- Password contains numbers.
- Password does not contain special characters.
- Password contains a common or predictable pattern.
- Password does not contain repeated character patterns.

### Recommendations

- Use at least 12 characters.
- Add at least one uppercase letter.
- Add a special character such as !, @, #, or \$.
- Avoid common words such as password, admin, qwerty, or welcome.
- Use multi-factor authentication for important accounts.
- Use different passwords for different accounts.

Table 3: Simulated Password Test Cases

| Case | Example        | Classification | Reason                     |
|------|----------------|----------------|----------------------------|
| 1    | Password123    | Weak           | Common /predictable        |
| 2    | admin2024      | Weak           | Common term / year         |
| 3    | qwerty12345    | Weak           | Predictable pattern        |
| 4    | Summer2026     | Moderate       | Mixed / no special letters |
| 5    | MyCar2026      | Moderate       | Mixed / no special letters |
| 6    | RiverCloud!58  | Strong         | Long and varied            |
| 7    | SecureVault#78 | Strong         | Long and varied            |

Table 4: Sample Test Results

| Case | Score | Classification | Weakness                   |
|------|-------|----------------|----------------------------|
| 1    | 30    | Weak           | Common /short              |
| 2    | 30    | Weak           | Common / short             |
| 3    | 30    | Weak           | Common pattern / short     |
| 4    | 60    | Moderate       | Short / no special letters |
| 5    | 60    | Moderate       | Short / no special letters |
| 6    | 95    | Strong         | No major weakness          |
| 7    | 95    | Strong         | No major weakness          |

## Conclusions

The password security assessment tool is a safe method for overall password check-up it will raise your awareness of password score, classification, and provide you with a checklist along with recommendations for a strong password. This tool is very helpful for small business training as it shows why a password falls under weak, moderate, strong classification.

## Future Work

Some improvements that can be done to the tool could involve having it check longer passphrases and passwords that include spaces. Adding some simple password policy examples, like minimum length, multi-factor, and account lockout. In addition to that, I could compare the results obtained with this assessment tool against other free online password strength testers such as "Bitwarden" and "Password Strength Meter" in order to evaluate the differences in scoring, classification, and overall accuracy to better improve this tool. Lastly, a future version might also include an option of assessing if the password provided by the user has been previously breached online and be able provide notification of it.

## Acknowledgements

Advisor: Jeff Duffany  
Polytechnic University of Puerto Rico  
Computer Science Department  
Graduate Project EXPO 2026

## References

[1] NIST, Digital Identity Guidelines: Authentication and Authenticator Management, 2025.  
[2] CISA, Formulate Strong Passwords, 2025.  
[3] FTC, Cybersecurity for Small Business, 2025.  
[4] CISA, Good Security Habits, 2025.  
[5] Verizon Business, 2025 Data Breach Investigations Report: SMB Snapshot, 2025.