

Password Security Assessment Tool for Small Businesses

Kelmit Rivera Rivera

Master in Computer Science

Advisor: Jeffrey Duffany, Ph.D.

Polytechnic University of Puerto Rico

Graduate Project EXPO, May 2026

Abstract — Passwords are still the most common method to control access to computer systems, data, networks, and applications. Properly chosen, strong, and managed passwords can be an effective first-line defense against unauthorized access. This project presents the development, implementation, and testing of a password assessment tool that provides a security score based on best practices and guidelines and classifies a password, as either weak, moderate, or strong. The assessment tool, using rule-based logic, computed user's passwords scores and evaluated them in length, character alteration, variety, dictionary word sequence, repeated characters, and number series and based on these factors is how their classification was given. The tool was tested with sample passwords, results recorded, analyzed, and evaluated to provide recommendations and a guide for increasing password security. The purpose of the research is to increase password security awareness and to provide an easy-to-use password assessment tool for organizations and individuals.

Key Terms — Authentication, Cybersecurity, Password Assessment, Password Security, Small Business.

INTRODUCTION

Passwords are still one of the most frequently used forms of access control in business systems, email and social media accounts, online shopping sites, banking applications, and system administrative accounts. They are widely deployed because they are simple for users to understand and use. However, average passwords and simple security questions based on them can be easily guessed by other users if dedicated enough time. Additionally, users often reuse the same password,

or slight variations of it, so a password obtained from one service or website can open an account or accounts on others. Passwords can be intercepted, attacked, or stolen [1], [2].

Small businesses are particularly vulnerable because most don't have overarching password policy management, single sign-on technologies, or stronger forms of protection against identity theft. With such infrastructure, the responsibility falls on the users, who frequently choose passwords that are easy to remember, but also easy to hack. In the case of guessed passwords, hackers typically do so by entering many passwords that are related to the business, specific names, special dates, and keyboard patterns.

Cybersecurity experts suggest that businesses use multi-factor authentication on their administrative, email, and networking accounts as an absolute minimum, and would prefer that every account used the additional layer of security [3], [4].

The most secure passwords are those that can be neither guessed nor cracked. While there are some that might consider multi-factor, such as fingerprint recognition or other biometric characteristics, sometimes that is not 100 percent secure either. Therefore, it is recommended to have at least one biometric and at least one knowledge-based factor, such as a password for good security layer.

The purpose of this project was to design a simple and user-friendly interface for small business owners and users to test the strength of their passwords. The project involved developing a browser-based prototype capable of allowing users to test passwords and receive a score, classification, checklist, and recommended guidelines. The prototype was developed using HTML, CSS and JavaScript.

BACKGROUND

Authentication is the process of verifying a user's identity. One common method of authentication involves the use of a "knowledge-based factor", such as a password. When stored safely, passwords can be an effective security tool. Yet, when shared or weak, they are the most common way for hackers to gain access.

Passwords based on familiar words can be compromised in a brute force attack using a list of common words or could also be guessed by someone who knows the user well. In some cases, passwords based on a common number sequence can be quickly guessed by an attacker.

Aside from concerns over malicious email attachments and malware as weapons against small and medium-sized businesses, there is also concern over the use of stolen credentials and the use of vulnerabilities. As Verizon's 2025 Data Breach Investigations Report (DBIR) mentioned, the most common initial action in a breach against a small or medium-sized organization was abuse of stolen credentials, and the second most common was use of vulnerabilities. Therefore, with an eye to authentication best practices, it is everyone's concern [5].

Small businesses may lack the means to implement sophisticated identity and access management tools. Consequently, a basic assessment solution can, at least, raise awareness and help educate users. A tool as simple as a password security assessment can show users why their personalized password may be weak, moderate, or strong. Additionally, it shows users that password security works better only when paired with multi-factor authentication with a password manager, plus a unique password for every account is highly recommended [2], [3], [4].

This project does not aim to demonstrate how a complete industrial-grade authentication system is developed. Instead, its purpose is to illustrate how a password can be checked and to demonstrate a few security concepts while using the assessment tool.

Small businesses that had been a victim of a previous cyber-attack generally rely on passwords to safeguard their IT systems, business data, accounts, and other confidential information. There is simply no way to tell how strong a password may be until tested. Short, weak, common, and easy to guess passwords can pose no real hurdle to an employee intent on undermining IT security.

This project focuses on the development of a simple and easy-to-use password-checking tool. The web interface tool allows small sized organizations and businesses to generate passwords that mimic the security features of their accounts or systems and have employees test those passwords withing the tool. The system then immediately lists the good and bad attributes of these passwords.

Having a visual assessment tool can solve the problem by providing feedback instantly to the users, like showing a score, a classification, a checklist, and recommendations which will help users understand why they are being assessed in the first place rather than just being asked to "create a stronger password".

EQUIPMENT AND MATERIALS

This project incorporates hardware and software components required for the development of the tool.

Hardware Components

This is a browser-based project; therefore, no cybersecurity hardware is required. This project can be developed and demonstrated on a normal laptop or desktop computer, keyboard and mouse, and a display monitor.

The computer was used for the project files, to run the prototype locally, take screenshots, and write the research report.

Software Components

The software components used in this project are simple and readily available. The password checking tool was implemented as a web-based prototype, allowing users to directly open it in their browser and test it.

The project files were created and edited mostly using Visual Studio Code, where the HTML, CSS, and JavaScript code was written in one workspace. Then a web browser was used to run and test the prototype. Since the tool is browser-based, there was no need for a web server or database. HTML is used to structure the interface, such as the title, password input field, buttons, score table, checklist, and recommendation sections. CSS is responsible for developing the layout look presentable by controlling colors, layout, spacing, cards fonts, and the overall visual aspect. JavaScript was used to perform the password assessment reading the test password, checking it against predefined rules, calculating the score, classifying the password, and displaying recommendations.

METHODOLOGY

The approach used in this project is design and simulation methodology. No real passwords, systems or business account information are used; instead test passwords are used to show how the tool works in assessing password strength.

The project was developed through six phases: research, requirements, system design, prototype implementation, testing, and results.

Research Phase

The project began by examining what industry guidelines say about password management, user authentication, and general cybersecurity for small businesses. Sources such as NIST, CISA, the FTC, and Verizon were reviewed to find out what the current standards are for password length, what best practices to use when creating a new password, what multi-factor authentication is, and what the risks are when your credentials are compromised [1, 2, 3, 5].

Requirements Definition

The second phase of the development process outlined the requirements of the resulting tool as a document of use for a small business user. These requirements were translated into design criteria that specified that the tool needed to be easy for a small business user to use, safe for demonstration in an

academic setting, and suitable for inclusion in a written report and academic poster. The functional requirements were:

- Allow the user to test password.
- Analyze password in the browser.
- Check for length, uppercase letters, lowercase letters, numbers, special characters, common patterns, and repeated characters.
- Assign a security score.
- Classify the password as weak, moderate, or strong.
- Display a checklist of passed and failed criteria.
- Recommendations for improvement.

System Design Phase

The third phase focused on the dashboard interface design, which includes a password input field, an “Analyze Password” button, a score panel, a classification result, a checklist, and a recommendation section (as shown in Figure 1).

The dashboard was designed to be simple and readable. Since the project is for small business users, the interface is free of technical overload and provides easily understandable feedback.

Figure 1
Password Security Assessment Tool Main Interface
(Browser: Microsoft Edge)

Prototype Implementation Phase

The fourth phase involved developing the prototype. HTML, CSS, and JavaScript were used to develop the interface and its interactivity. HTML was used to create the structural framework, CSS was used to design the dashboard, and JavaScript performed the logic of scoring the selections.

The JavaScript logic will evaluate the entered test password based on several conditions and each condition will add to the score and the final score is used to display the password's strength.

Simulated Testing Phase

The fifth phase was to test the tool with simulated password examples, test cases were prepared with weak, moderate, and strong examples of passwords.

Results Testing Phase

The last phase of the tool assessment checked whether the tool recognizes password weaknesses and provides an adequate number of recommendations, and whether the tool recommends the user to choose a stronger password. Focusing on the following metrics:

- Security score
- Weak, moderate, or strong classification
- Number of weaknesses detected
- Recommendations generated
- Consistency of tool output

SYSTEM LOGIC

The assessment works by a simple point system. Table 1 shows the password criteria assessed by the tool, such as length, upper/lower case, numbers, symbols, common words, and repeated characters. For each different requirement met by a test password, the password is assigned a point. Once the score has been determined, the tool then maps the password to one of three categories (weak, moderate, or strong), as shown in Table 2. This helps the users understand their password's strengths and weaknesses and have knowledge on how to better pick a password with higher security standards.

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

The assessment formula used was:

- Password Security Score = Sum of Satisfied Criteria Values.

This approach was chosen because it is transparent and explainable. A user can see what attributes increased the score and which shortcoming decreased it. The scoring system is not meant to be a complete password cracking resistance model. It is an educational and evaluation-based model intended to demonstrate critical password weaknesses and increase better password practices.

PROTOTYPE OPERATION

The developed prototype operates through a simple sequence of steps, which are demonstrated in the following section that is illustrated in Figure 2.

First, the user enters a password in the input field (see Figure 3) and clicks the "Analyze Password" button. The next page contains the JavaScript program. It starts by reading the entered password in the tool, then assesses the password checking it against the set criteria., produces a security score, and based on the score the tool then produces a password strength classification, finally then presents a password strength check list with all the comments and needed recommendations. Refer

to Figure 4 that presents an example of a Weak password assessment, Figure 5 for a Moderate password assessment, and Figure 6 for a Strong password assessment.

The prototype does not store passwords, does not send the password to a server, and it does not create a new password for the user. Everything happens locally within the browser.

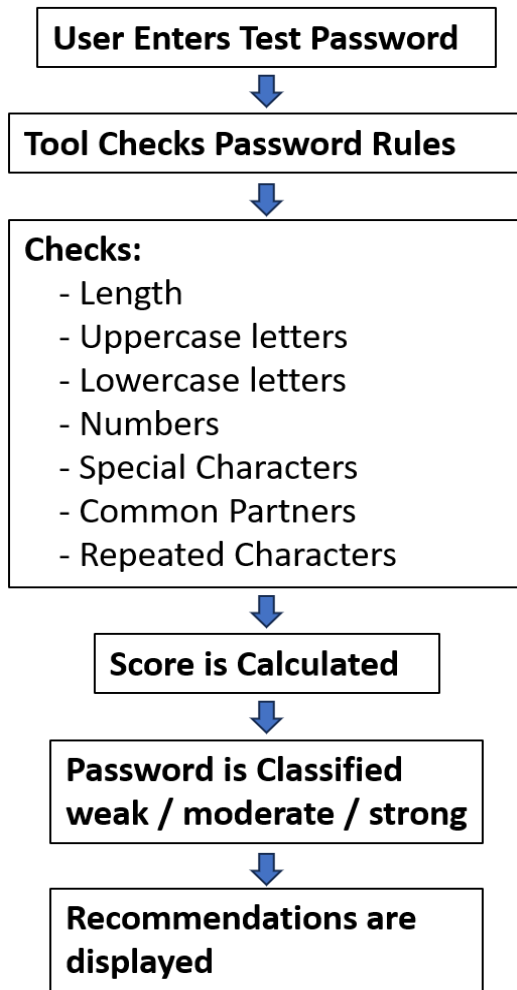


Figure 2
Password Assessment Workflow

Figure 3 shows the 'Enter a Test Password' screen. It includes a title, a warning message 'Do not enter real passwords. This tool is for test passwords only.', a text input field containing 'Enter test password', and two buttons: 'Analyze Password' and 'Clear'.

Figure 3
Password Input Screen

Figure 4 displays the 'Assessment Result' for a weak password. The score is 30/100, and the classification is 'Weak'. The 'Password Checklist' lists seven items, all of which are violated by the password 'password123'. The 'Recommendations' section provides six suggestions to improve the password.

Figure 4
Weak Password Assessment Result

Figure 5 displays the 'Assessment Result' for a moderate password. The score is 60/100, and the classification is 'Moderate'. The 'Password Checklist' lists seven items, with three violations. The 'Recommendations' section provides six suggestions to improve the password.

Figure 5
Moderate Password Assessment Result

Enter a Test Password

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

Analyze Password

Clear

Assessment Result

Score: 95/100
Classification: **Strong**

Password Checklist

- Password has 12 or more characters.
- Password contains uppercase letters.
- Password contains lowercase letters.
- Password contains numbers.
- Password contains special characters.
- Password does not contain common password patterns.
- Password does not contain repeated character patterns.

Recommendations

- Use multi-factor authentication for important accounts.
- Use different passwords for different accounts.

Figure 6
Strong Password Assessment Result

TESTING SCENARIOS

The tool was tested using simulated password examples that were intentionally chosen to represent weak, moderate, and strong passwords that people commonly use, as shown in Table 3. These examples did not contain any real passwords and were solely used to test out the tool. The test cases helped demonstrate how the score and classification are affected by different characteristics of passwords.

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

RESULTS AND DISCUSSION

The simulation test results indicated that the password security assessment tool was able to classify test passwords into weak, moderate and strong categories, as shown in Table 4.

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

Weak passwords got low scores because they were based on dictionary words, keyboard sequences, repeated characters, or known simple number sequences. Passwords such as “password123”, “admin2024”, and “qwerty12345” are dangerous, as these are some of the first passwords attackers will try in a dictionary or credential attack [1, 2].

Moderate passwords are not the best but also not the worst. They received a mid-range score because, although some criteria were met, like the length and variation, others did not. For instance, the password “Summer2026” has uppercase letters, lowercase letters, and numbers and is at least eight characters long. However, it doesn’t contain any special characters.

Strong passwords earn higher scores, as do passwords that include a combination of uppercase and lowercase letters, numbers, and special characters. For example, “RiverCloud!58”, and “SecureVault#78” are strong passwords and would earn higher scores on the security score as they satisfy most of the criteria used by the password assessment tool.

The tool also ensures a fairer evaluation than if it were done manually by a user. If a user does it manually, a password can be wrongly thought of as

being strong by one user just because there are a number and a symbol, while another user can know that it's still easy to guess. The tool has all test passwords scored by the same criteria.

CONCLUSION

In this project, a simple password security assessment tool was developed for small businesses. The tool checks the user's passwords against predefined password criteria, returns a security score, and categorizes the password according to the checklist. It also makes suggestions for weak passwords and how to improve them.

In today's current situation, passwords and credential safety are a well-known problem. Especially for small businesses and companies with only a handful of employees, in which it is, unfortunately, too hard to get and utilize proper security tools. A simple low-cost awareness raising tool can ensure a good risk assessment and maybe increase further security investments.

With this simulation, weak, moderate, and strong passwords can be clearly distinguished. Hopefully, such an assessment only helps fill the gap of poor password practices in those environments and allows getting solid results from appropriate existing systems that otherwise could be undermined by weak passwords. The developed tool has no specific requirements except for having a local browser, visual studio code which is accessible online and can be downloaded for free, and a working desktop.

In general, the project provides a practical, achievable cybersecurity design that can be used for awareness and training, and for a basic assessment of password risks.

FUTURE WORK

For future work, there are a few ideas for additional new features for the password security tool:

- Update and expand the tool's current functionality and test passphrases. For example, the test for passphrases should be updated to test

stronger passphrases (as per current security best practices for longer passwords and passphrases [1], [2]), to include testing passphrases containing spaces.

- Add Password Policy Templates and/or a recommended list of password managers. For example, add or provide as a separate tool that can link training to the password security employee training for a small business password policy length, multi-factor authentication, and account lockout recommendations.
- New Feature Ideas or Concepts. For this future development project, in addition to the updated and new features examples listed above, additional new or makeover tool version third, fourth, and/or fifth new feature concepts for the initial future development of the password security tool would include "Breached" password checking" capability and "Training Analytics".

REFERENCES

- [1] D. Temoshok et al. "Digital Identity Guidelines: Authentication and Authenticator Management." National Institute of Standards and Technology, Special Publication 800-63B-4, July 2025. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf>
- [2] Cybersecurity and Infrastructure Security Agency. (2025). *Formulate Strong Passwords and PIN Codes* [Online]. Available: <https://www.cisa.gov/resources-tools/training/formulate-strong-passwords-and-pin-codes>.
- [3] Federal Trade Commission. (2025). *Cybersecurity for Small Business* [Online]. Available: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity>.
- [4] Cybersecurity and Infrastructure Security Agency. (2025). *Good Security Habits* [Online]. Available: <https://www.cisa.gov/news-events/news/good-security-habits>.
- [5] Verizon Business. (2025). *2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot* [Online]. Available: <https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf>.