# *CRACKING THE CODE: A GUIDE TO ASSESSING PASSWORD STRENGTH*

Sumi S,
Department of Cyber Security,
Nehru College of Engineering and Research Centre,
Thrissur, India
*sumisudheer2001@gmail.com*

Soumya T,
Department of Computer Science Engineering,
Nehru College of Engineering & Research Centre,
Thrissur, India
*soumyanikshay@gmail.com*

***Abstract:*** The ever-expanding network environment has led to the development of numerous methods for processing and accessing information. Using a password is one of the most popular ways to safeguard and access information. Sensitive and crucial data should be protected with a password against unauthorized users who may get access to the system unintentionally or on purpose. Finding a strong compromise between a secure password and one that is memorable is the aim of this study.

***Keywords:*** Password strength, password meters

## *I. INTRODUCTION*

Password integrity is a vital line of defence against unwanted access to sensitive data in an era where cyber security breaches are becoming more common. It is impossible to overestimate the significance of having strong passwords, yet creating and remembering them is a significant difficulty for users of a variety of digital platforms. Consequently, the creation of strong password strength checks becomes essential to the continuous fight to strengthen cybersecurity. In order to improve the security posture of both individuals and organizations, this paper explores the topic of password strength checkers. This study intends to evaluate the effectiveness of current ways in mitigating security threats and to clarify the mechanisms underlying password strength assessment by a thorough investigation of existing methodology, algorithms, and technologies. By using case studies, theoretical frameworks, and empirical analysis, this research study aims to further knowledge about password security procedures and provide practical suggestions for the creation and implementation of stronger password strength checkers. Ultimately, the goal of this study is to enable people and organizations to strengthen their digital defences and protect against the ever-changing dangers posed by hostile actors by raising awareness and knowledge of this crucial component of cybersecurity.

## *II. LITERATURE REVIEW*

Passwords that are straightforward to remember are frequently generated by users, which also makes them simple to crack. In accordance with Lyastani, Acar, Fahl, and Backes (2020), employing John the Ripper, a password-cracking program, for creating stronger passwords based on straightforward dictionary terms is a fantastic way to employ mangling rules. The strength of the password can be examined in a few different ways. In the Vu et al. (2019) investigation, they attempted to break them utilizing the password strength. They looked at how much the passwords differed in strength. They calculated the period of time it took to crack each of the several passwords they used in their study in hopes of confirm each password's strength.

Using a password meter is a further way of determining the passwords' strength. A password meter is intended to compute various requirements that go into making up a strong password. In a study that appeared in 2021, Ur et al. examined the benefits and drawbacks of multiple password meters. Password meters are designed to measure a password's strength in terms of crack-time, bad to wonderful, or very fragile to very strong. With inspiration from the investigation of Ur et al. (2019), the password strength will be determined in this paper employing a password meter.

## *III. SYSTEM REQUIREMENTS*

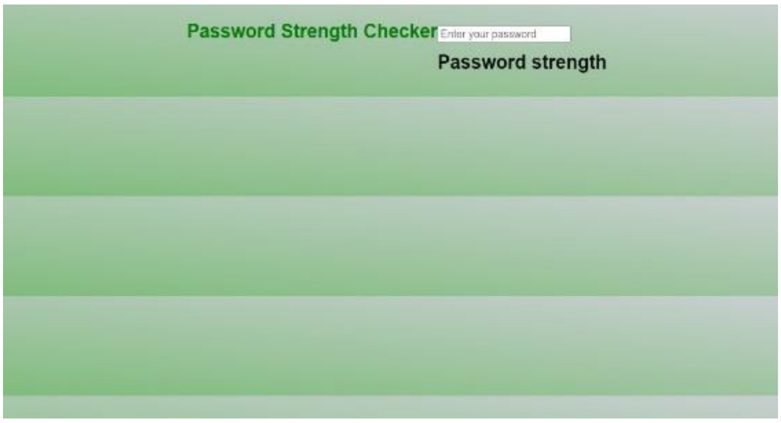
Programming Environment: Windows 11(2021)

Features: A sign up page with feature password strength checking using HTML, CSS and JavaScript.

- Visual Sudio Code

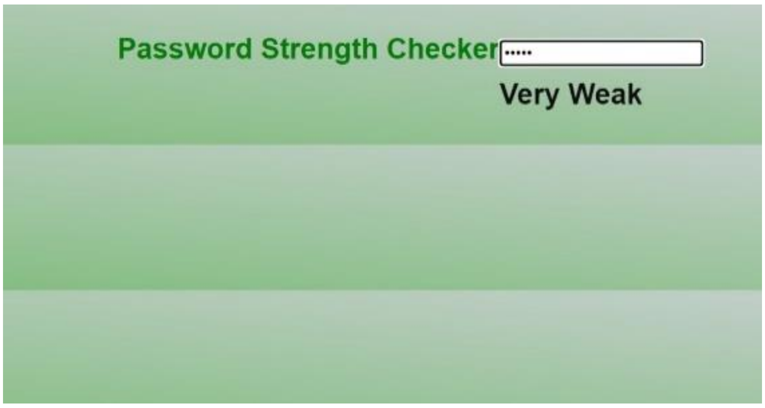
  Microsoft created Visual Studio Code, usually known as VS Code, which is a source-code editor available for Windows, Linux, and macOS. Support for debugging, snippets, code rewriting, intelligent code completion, and embedded Git are among the features. Users have the ability to modify the theme, keyboard shortcuts, preferences, and install functional extensions. A number of programming languages, including C, C#, C++, Fortran, Go, Java, JavaScript, Node.js, Python, Rust, and Julia, can be used with Visual Studio Code, a source-code editor. The Electron framework, which powers Node.js web applications powered by the Blink layout engine, is the foundation upon which it is constructed. The editor component (codenamed "Monaco") used in Azure DevOps is also utilized in Visual Studio Code.

The system requirements of a password strength checker usually entail figuring out what the minimal requirements are for a password to be deemed strong. These requirements frequently consist of elements like: Length: Determining the password's minimum length. Eight to twelve characters is the typical range, however longer passwords are usually safer. Character Complexity: Needing a variety of character kinds, including numbers, capital and lowercase letters, and special characters (such as!, @, #, $, %, and so on). This makes sure that it is difficult to figure out the password. Steer clear of common patterns: looking for recurring themes or easily guessed sequences, like "123456" or "password". Not Dependent on Username: Making certain that the password is unrelated to the username or any other readily available information.



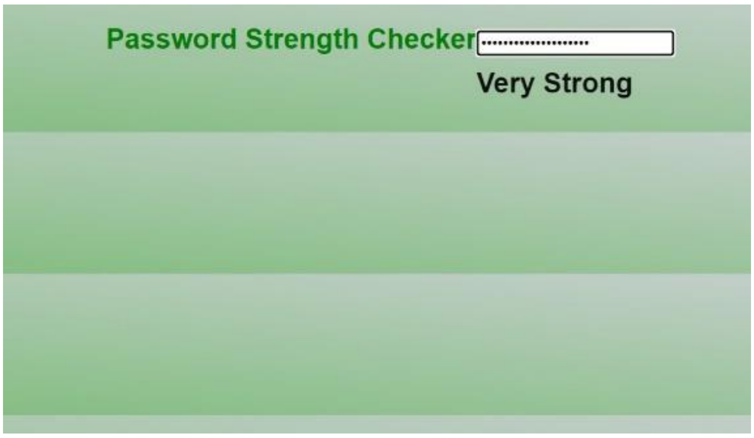
Password strength

***Fig. 1 sign up page***



Very Weak

***Fig. 2 Change in strength when password is typed***



Very Strong

***Fig. 3 Change in strength when password is typed***

## *IV. PROPOSED SYSTEM*

A strong interest exists in investigating and examining the memorability and strength of the password that the user has chosen. An effective password should be simple to remember, difficult to crack, and appropriate for the password user. During the process of searching through facts and theories, many diverse password creation procedures were found to be interesting for this experimental study. A strong interest exists in investigating and examining the memorability and strength of the password that the user has chosen. An effective password should be simple to remember, difficult to crack, and appropriate for the password user. During the process of searching through facts and theories, many diverse password creation procedures were found to be interesting for this experimental study. After selecting from a variety of password construction techniques, it was determined that three types of passwords could be created: modified passwords, associations passwords, and own set passwords. Consequently, the research question in this thesis is the appearance and content of a password and how important it is. After selecting from a variety of password construction techniques, it was determined that three types of passwords could be created: modified passwords, associations passwords, and own set passwords. Consequently, the research question in this thesis is the appearance and content of a password and how important it is.

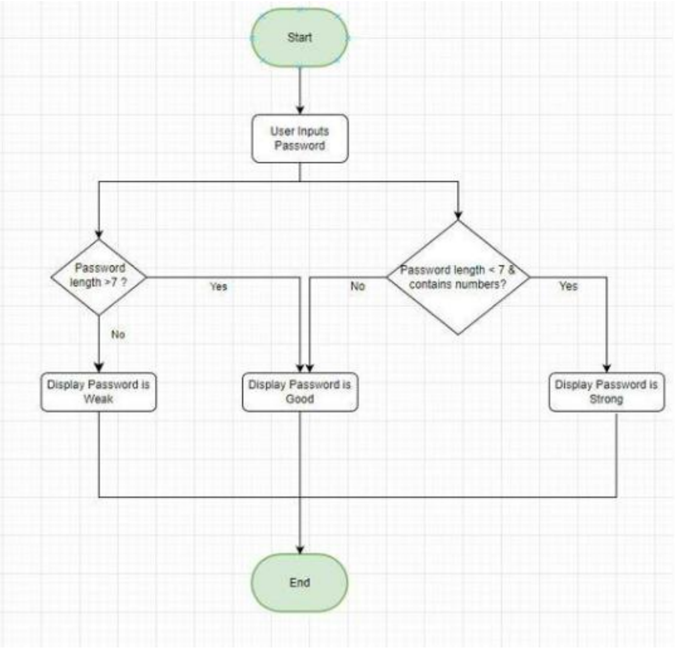


***Fig. 4 Block Diagram***

## *V. CONCLUSION*

The study that has been presented in the result and analysis serves as the foundation for the conclusion, which will be discussed in this chapter together with the thesis' response to the research question. Finding the association-, modified dictionary-, and self-set password that achieved the optimal balance between password strength and memorability was the aim of the study question. In terms of password strength and memorability, the modified password formulation was the least strong of all. The strongest passwords were made using the association password construction method, which was also very memorable. When coming up with a new password, care should be taken with its strength and memorability. A secure password should be difficult to figure out yet simple to remember. A successful and secure password relies heavily on the trade-off between strength and memorability. The crucial significance that password strength checkers play in encouraging users to create stronger passwords is one of the study's main conclusions. These tools provide insightful analysis and feedback by utilizing advanced algorithms and heuristic analysis, enabling users to make well-informed password decisions. Furthermore, the incorporation of contextual elements and user-centric design concepts has improved the usability and efficacy of password strength checks even more, enabling a broad acceptance and adoption among users with different levels of technical proficiency.

***Conflicts of Interest:*** "The authors certify that they have no competing interests with regard to this research."

## *REFERENCES*

[1]. Ahlberg, M. Blomberg, M & Davidsson, P. (2021). Passwords – The Achille's heel of information systems? Borås: University of Borås. June 2021 020-06468-5

[2]. Carnavalet, X. & Mannan, M. (2019). "A Large-Scale Evaluation of High-Impact Password Strength Meters", ACM Transactions on Information and System Security (TISSEC).

[3]. Merkow, S.M. & Breithaupt, J. (2020). Information security- principles and practices. 2nd edn., Indianapolis: Pearson Mitrović. Handbok i IT-säkerhet. 4th edn., Sundbyberg: Paina

[4]. Password Security: An Analysis of Password Strengths and Vulnerabilities. Katha Chanda. July 2016 International Journal of Computer Network and Information Security 8(7):23-30. Forget, A., Chiasson, S., Van Oorschot, P.C. & Biddle, R. (2008). Persuasion for Stronger Passwords: Motivation and Pilot Study" in Springer Berlin Heidelberg. Berlin: Heidelberg.

[5]. Likhitha, C., Ninitha, P. & Kanchana, V. (2016). DNA Bar-coding: A Novel Approach for Identifying an Individual Using Extended Levenshtein Distance Algorithm and STR analysis, International Journal of Electrical and Computer Engineering, pp. 1133-1139.

[6]. Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J. & Schultz, E. International Journal of Human - Computer Studies: Improving password security and memorability to protect personal and organizational information, pp. 744-757.