JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Stateless Graphical and Password Strength Checker

[1]Ganesh Boddupally, [2]Navya Koti, [3]Naveen Kumar Kura, [1]R Suhasini, [5]Reddyvari Venkateswara Reddy

[1]Student, [2]Student, [3]Student, [4]Assistant Professor, [5]Associate Professor
[1]Department of Computer Science Cybersecurity,
[1]CMR College of Engineering & Technology, Hyderabad, India

Abstract: Passwords serve as the primary defence mechanism for protecting our online accounts and sensitive data from unauthorized access. To address this critical issue, the proposed project introduces a novel password strength checker that integrates both textual and graphical authentication methods. The decision considers a number of important elements, including the length of the password, the diversity of characters used, and the complexity of patterns within the password. By analysing these elements, the checker provides users with valuable insights into the strength of their chosen passwords. Besides traditional textual authentication, the password strength checker incorporates a graphical authentication component. This innovative feature requires users to interact with a grid of images, selecting specific images in a predetermined sequence to authenticate their identity. This graphical authentication method adds an extra layer of security by making it significantly more challenging for potential attackers to guess or crack the password. By combining textual and graphical authentication mechanisms, the new password strength checker offers enhanced shielding hostile to a wide range of cyber threats. It empowers users to create and utilize strong passwords that are congenitally more buoyant to strikes such as brute force attempts or dictionary-based attacks. Overall, the primary goal of the password strength checker is to promote better password practices among users and mitigate the risks associated with weak passwords. By encouraging the usage of strong and secure password practices, the checker contributes to enhance overall cybersecurity posture and protecting sensitive information in an increasingly digitized world.

IndexTerms **– Password strength checker, Cybersecurity, Authentication methods, Textual passwords, Graphical passwords, Password complexity, Character diversity, Pattern complexity, Cyber threats, User authentication, Online security, Strong passwords, Vulnerability mitigation**

I. INTRODUCTION

In today's digital panorama, the protection of sensitive information and digital assets pivot on the strength of password security measures. Despite widespread awareness, the prevalence of weak passwords poses a persistent threat, leaving individuals and organizations vulnerable to cyber attacks. To address this challenge, we present a innovative solution: a multifaceted password strength checker integrating both textual and graphical authentication methods. This innovative tool aims to revolutionize password management practices, empowering users to adopt unassailable authentication strategies.

Our password strength checker offers a comprehensive assessment of password robustness by analyzing key factors such as length, character diversity, and pattern complexity. This holistic evaluation provides users with valuable insights into the security posture of their passwords, enabling informed suggestions to mitigate potential vulnerabilities and threats. Implementing our solution apart is the involvement of a graphical authentication component, adding traditional textual authentication methods. By requiring users to interact with a grid of images and select specific images in a predefined sequence, this novel approach introduces an additional layer of security, making it important more challenging for adversaries to compromise passwords. Through the integration of textual and graphical authentication mechanisms, our password strength checker represents a paradigm shift in online security practices. By encouraging the acquisition of strong and secure password practices aiming to avoid the risks associated with weak passwords, fortifying the overall cybersecurity posture of individuals and organizations.

In this project, we will search into the technical intricacies of our password strength checker, explaining its design principles, implementation details, and potential applications. Furthermore, we will explore the suggestions of our solution for cybersecurity practices and discuss the broader societal impact of fostering a culture of password security awareness. Ultimately, our endeavor seeks to give knowledge to users with the tools and necessary details to enhance their online security and safeguard their digital identities in an ever-evolving threat landscape. By promoting robust password practices, we aim to bolster resilience in anticipation of cyber ultimatum and cultivate a safer digital environment for all.

II. LITERATURE REVIEW

In this paper, the basic metrics for assessing password strength were reviewed by Gongzhu Hu, including entropy, NISTentropy, password quality index, and Levenshtein distance, as well as some password quality metrics developed at some popular service vendors. A password complexity metric that considers the composition patterns in a password in addition to the LUDS criteria was proposed by him. The tie-up between these meter were analyzed using the maximum information coefficient (MIC) and Pearson coefficient.[1] The resulting statistics show that the mass metrics are closely correlated except While traditional password metrics

like length and character set diversity are important, could Levenshtein distance be a beneficial additional factor to consider when evaluating password strength. Cracking tools employ a variety of techniques, including brute force attacks, transformation rules, dictionary attacks, and extensive table look-ups. These tactics are utilized to ascertain passwords through two types of outcomes: either the password is successfully found (via table look-up) or it remains elusive. Additionally, the time taken to unveil the password is gauged, particularly relevant in techniques like John the Ripper (JtR), which deploy multiple strategies simultaneously. Research findings suggest a direct correlation between the efficacy of password cracking and the strength measures implemented. In essence, stronger passwords tend to withstand cracking attempts more effectively, while weaker ones succumb more readily to these methodologies. Our dry runs fiercely propound that the strength metrics we developed are effective in evaluating the quality of passwords chosen by users. [2] The bottom line of their analysis comes to the simple advice to users: a long password with various kinds of characters (lower and uppercase letters, digits, and symbols) should be selected, as the length of password and size of charset being the two most critical parameters to the strength of the password in all the metrics we studied.

[3] The paper "Graphical Password Authentication System" introduces graphical passwords as a novel approach to computer authentication within the realm of digital security. It underscores the prevalent threat of shoulder surfing, where passwords are compromised through direct observation or recording during authentication processes. The paper proposes a solution comprising two primary components: user registration and login using a valid user ID and password, followed by image-based authentication. This approach aims to bolster security against shoulder surfing attacks. It delves deeper into the significance of computer security and the pivotal role that graphical passwords play in fortifying the authentication process. Addressing the problem statement, the paper underscores the inherent weaknesses of traditional alphanumeric passwords and stresses the momentousness of user responsibility in safeguarding information.

By Pathik Nandi & Dr. Preeti Savant, they highlights potential security threats such as dictionary attacks and Brute-force attacks, underscoring the need for robust authentication mechanisms.[4] The section on computer authentication provides a comprehensive overview of authentication processes, delineating between single-factor, two-factor, and multifactor authentication methodologies. It elucidates the exert of passwords, physical identification, and biometrics as key authentication factors, thereby contextualizing the role of graphical passwords within the broader authentication landscape. Graphical password authentication is thoroughly discussed, emphasizing its superiority in terms of usability and resilience against brute force and guessing attacks. Various graphical password schemes, including image-based and color-based authentication methods, are elucidated, highlights effectiveness in thwarting security threats. The proposed graphical password authentication system, encompassing user registration, login procedures, and authentication mechanisms using text-based, color-based passwords. This section serves as a roadmap for implementing the proposed solution. Finally, the related work section provides a comparative analysis of different password technologies, evaluating their security, and availability. The paper concludes by reiterating the significance of authentication in digital security and advocating for the adoption of graphical passwords as a viable solution to mitigate security threats, particularly shoulder surfing attacks. It underscores the cost-effectiveness and efficacy of graphical passwords as an alternative to traditional authentication methods, offering a transfixing disputation for their rampant adoption in digital security protocols.

III. METHODOLOGY

The proposed methodology for the password strength checker consists of several key components aimed at evaluating and enhancing the security of user passwords. Firstly, the textual analysis aspect focuses on assessing various attributes of the password, including its length, character diversity, and pattern complexity. Length is considered a fundamental factor, as longer passwords typically offer greater resistance to attacks. Character diversity is evaluated to gauge the visitant of different types of characters (e.g., uppercase, lowercase, digits, special symbols), which strengthens the password against dictionary-based attacks.

Additionally, the complexity of patterns within the password is examined to identify and mitigate the risk of predictable sequences. In conjunction with textual analysis, the methodology incorporates a graphical authentication component to further enhance security. Users are required to select specific images from a grid as fraction of the authentication process. This graphical authentication serves as an additional layer of protection against unauthorized access attempts, particularly by thwarting automated attacks and password cracking algorithms.

IV. LIMITATION OF EXISTING SOLUTIONS

1. Lack of Resistance to Advanced Attacks: Textual password strength checkers often lack mechanisms to defend against advanced attack techniques, such as phishing, social engineering, and keystroke logging. Without considering additional security layers like graphical authentication, these solutions may leave users vulnerable to sophisticated exploitation tactics employed by cybercriminals.

2. Limited User Experience: Text-based assessments may not provide a user-friendly experience, especially for the one who grapple with creating and remembering complex passwords. This limitation can steer to frustration among users and may discourage them from actively engaging in password security practices.

3. Accessibility Concerns: Portion of users, conspicuously those with visual or cognitive impairments, may encounter difficulties in using traditional text-based password strength checkers effectively. These solutions may not cater to diverse user needs and could inadvertently exclude certain demographics from accessing secure password management tools.

4. Limited Security Assessment: Traditional text-based password strength checkers primarily focus on attributes like length and character diversity, overlooking critical factors such as pattern complexity and graphical authentication. Ergo, they may not proffer a comprehensive evaluation of password security.

5. Vulnerability to Attacks: Textual passwords are susceptible to common cyber threats like dictionary attacks and brute-force methods. Without considering additional layers of security like graphical authentication, these solutions may fail to adequately protect against sophisticated attacks.

6. Inadequate User Engagement: Sole reliance on textual analysis for password assessment may result in an exiguity of user engagement. Users may not accrue ample dope or feedback to create strong passwords, leading to complacency and potentially weaker password choices.

7. Memory Burden on Users: Complex passwords generated merely based on textual analysis may be difficult for users to remember. This can lead to password reuse or the adoption of simpler, less secure passwords, undermining overall security efforts.

V. ARCHITECTURE

1. Frontend Components:

HTML : Provides the structure of the webpage, including sections for pattern strength checking, password strength authentication, and a contact form.

CSS : It Defines the styling and layout of the webpage elements to ensure a vividly appealing and user-friendly interface that could provide usability by users.

JavaScript : Implements the functionality for pattern strength checking, password strength checking, and potent updates of UI elements based on user input.

2. User Interaction: Users interact with the webpage to select a pattern, enter a password, and fill out the contact form.

3. Pattern Strength Checker:

HTML Structure : Contains a slice for selecting a pattern with a grid or lattice of cells.

JavaScript : Handles user interactions with the pattern grid (selection/deselection of cells). Calculates the strength of the selected pattern based on factors like length, uniqueness, and complexity. Updates the UI with the calculated pattern strength.

4. Password Strength Checker:

HTML Structure : Includes an input field for entering passwords and a chronicle of requirements for a strong password.

JavaScript : Validates the entered password against predefined requirements (length, uppercase, lowercase, numbers, special characters). Calculates the estimated time to crack the password using brute-force attack. Display password strength visually to user for feedback.

5. Contact Form :

HTML Structure: This contact form allows users to invade their name, Email address, a subject line, and their message.

JavaScript : Handles form submission and validation of the passwords. Sends the form data to a backend server for processing (not included in the provided code).

6. Pattern Strength Checking: Users select a pattern by clicking on the grid cells. JavaScript code evaluates chosen pattern's strength via diverse factors. The UI displays the calculated pattern strength to the user.

7. Password Strength Checking: Users enter a password in the input field. The JavaScript code validates the password against predefined requirements. It estimates the time to crack the password using brute-force attack. Visual feedback on password strength.

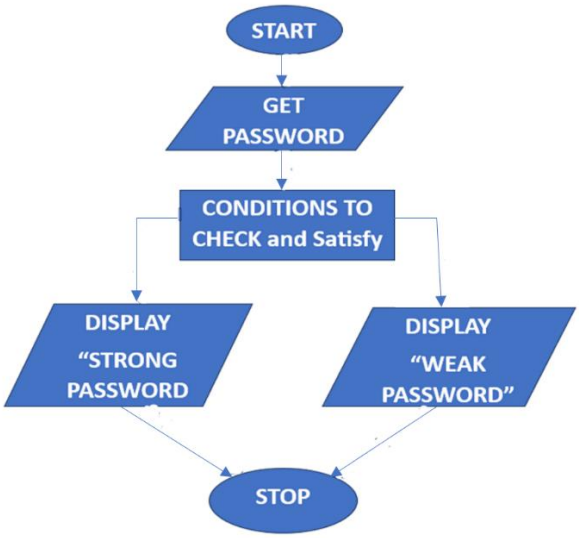

Fig.1 Flow of working

VI. RESULT AND DISCUSSION

The implementation of the password strength checker successfully integrates both textual and graphical authentication methods. Users can interact with the system to assess the strength of their passwords through pattern selection and textual analysis. The graphical component adds an extra layer of security, making it more challenging for potential attackers to compromise passwords. Additionally, the system provides valuable feedback to users, indicating the strength of their passwords and suggesting improvements where necessary. Overall, the password strength checker effectively evaluates password robustness and encourages users to adopt stronger authentication strategies.

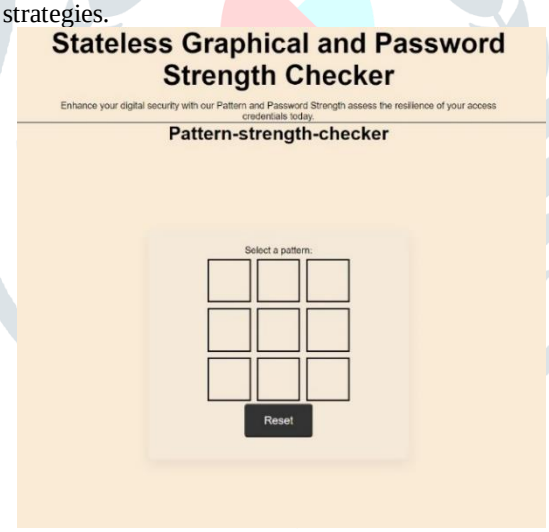

Fig. 1 Graphical password strength tester

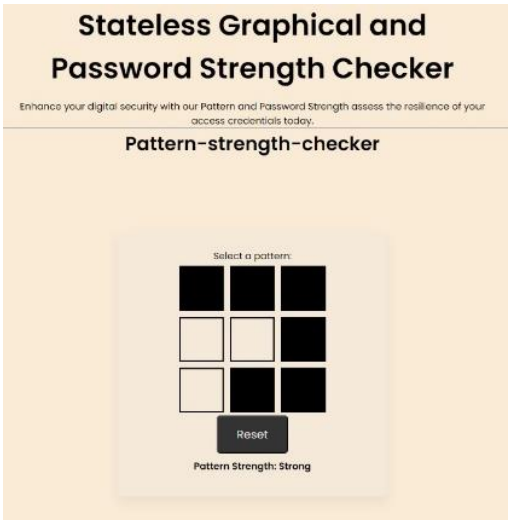

Fig. 2 Graphical password strength test result

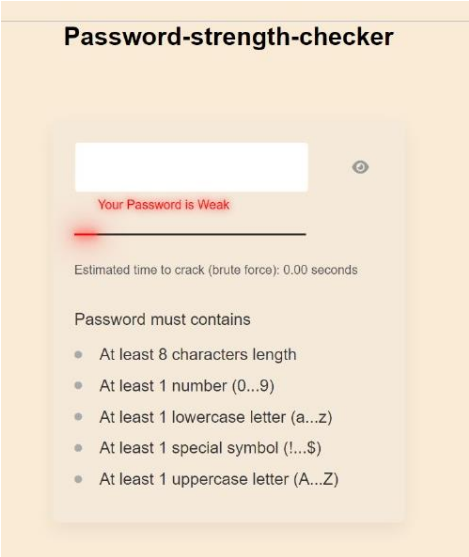

Fig.3 Textual password strength test

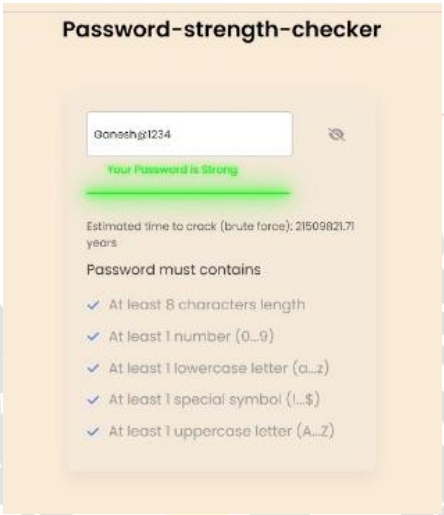

Fig.4 Textual password strength test result

VII. Acknowledgment

The Author is grateful to the CMR College of Engineering & Technology for providing better facilities and practical requirements.

References

[1] Discusses HCI (Human-Computer Interaction) and security systems according to a CHI Extended Abstracts workshop paper by S. Patrick, A. C. Long, and S. Flinn.
[2] Explores biometric authentication in a Computerworld article written by K. Gilhooly.
[3] Provides an overview of biometric identification by L. Jain, L. Hong, and S. Pankanti in a Communications of the ACM publication.
[4] Discusses memorable yet unrecallable passwords presented by D. Weinshall and S. Kirkpatrick in CHI conference proceedings.
[5] Explores user choice in graphical password schemes from a USENIX Security Symposium paper by D. Davis, F. Monrose, and M. K. Reiter.
[6] In a study by Jain et al. (2000), biometric identification was explored. Biometric identification refers to technologies that use unique physical or behavioral characteristics to identify individuals.
[7] "Hybritus: a password strength checker by ensemble illumination from the query feedbacks of websites".
[8] Password Strength Meter (passwordmonster.com)
[9] https://www.geeksforgeeks.org/graphical-password-authentication/
[10] https://www.ijraset.com/research-paper/graphical-password-authentication-system
[11] https://www.researchgate.net/publication/318154948_On_Password_Strength_A_Survey_and_Analysis