PASSO CHECKER

**TEAM NAME**:

Atharva Rane & Dhanashre Sanap

**FROM:**

PTVA Sathaye College

**Organized by:**

Digisuraksha Parhari Foundation **Powered by:**

Infinisec Technologies Pvt. Ltd.

**Info:**

PASSO CHECKER is a tool that evaluates your password's strength, helping you identify if it can withstand hacking attempts or needs improvement.

Secure your online presence with PASSO CHECKER!

ABSTRACT

In today's digital transformation era, safeguarding user data and privacy through robust password security is not just important—it's imperative. This paper introduces an innovative, lightweight tool developed in Python that rigorously evaluates password strength based on critical rules encompassing character diversity and length. By delivering instant feedback, this tool empowers users to create significantly stronger passwords, enhancing their security posture.

We delve into the tool's design and implementation, highlighting its potential for future enhancements while comparing it with leading cybersecurity practices. Furthermore, we examine the ethical implications and the tool's significance in a landscape where weak credentials have become a primary attack vector. By addressing these urgent concerns, this paper underscores the vital role our tool can play in the ongoing battle against cyber threats.

In the modern digital ecosystem, passwords serve as the first and often the only line of defense protecting sensitive user data, personal identities, and organizational assets. Despite the widespread adoption of authentication mechanisms, a significant number of users continue to rely on weak or easily guessable passwords, making them prime targets for cyberattacks such as brute-force, dictionary, and credentialstuffing attacks.

Cybersecurity agencies and standards organizations, including NIST and OWASP, have repeatedly emphasized the need for robust password creation strategies. However, many users remain unaware of the critical components that contribute to a strong password. This gap between recommended practices and user behavior calls for tools that not only evaluate password strength but also provide constructive feedback to help users improve their choices.

This research introduces a Python password strength checker that uses regular expressions to validate passwords based on specific security criteria. It checks for length, character variety, and special symbols, ensuring passwords are complex and secure. The tool's lightweight design makes it ideal for user registration systems, educational platforms, and personal cybersecurity use.

# PROBLEM STATEMENT & OBJECTIVE

Problem: A significant number of users continue to rely on weak passwords, leaving systems vulnerable to serious threats like bruteforce and dictionary attacks. Many choose easily guessable passwords, such as common words or simple sequences, which cybercriminals can exploit. Research shows that most data breaches are linked to compromised passwords, highlighting the urgency of this issue. To mitigate this risk, users must adopt stronger password practices by using a mix of uppercase letters, lowercase letters, numbers, and special characters, while also enabling multi-factor authentication. By fostering a commitment to strong password management, we can fortify our digital defenses and protect sensitive information from unauthorized access. Together, we can create a safer online environment for everyone.

Objective: To create a robust and intuitive tool that systematically evaluates password strength while empowering users with essential knowledge about cybersecurity. This innovative solution will not only deliver instant, actionable feedback to help users craft stronger passwords but also foster a deeper understanding of the critical role password security plays in protecting their sensitive information. Additionally, the tool will be designed for seamless integration with larger security platforms, enhancing overall security frameworks and providing a cohesive user experience. Key features will include dynamic strength indicators, tailored suggestions for strengthening weak passwords, and comprehensive educational resources focused on combating phishing threats and promoting effective password management strategies.

# LITERATuRE REVIEw

* NIST Digital Identity Guidelines
* Zxcvbn (Dropbox’s password strength estimator)
* OWASP password recommendations
* Academic papers on password entropy and usability/security trade-offs

# RESEARCh METhOdOLOgy

* Language: Python
* Libraries: re for regular expressions, tkinter for the GUI, math for entropy calculations, random for generating password suggestions.
* Approach: Combinesrule-basedchecks(length, uppercase, lowercase, numbers, special characters, common passwords, dictionary words) with entropy calculation:

Entropy = L · log2(C)

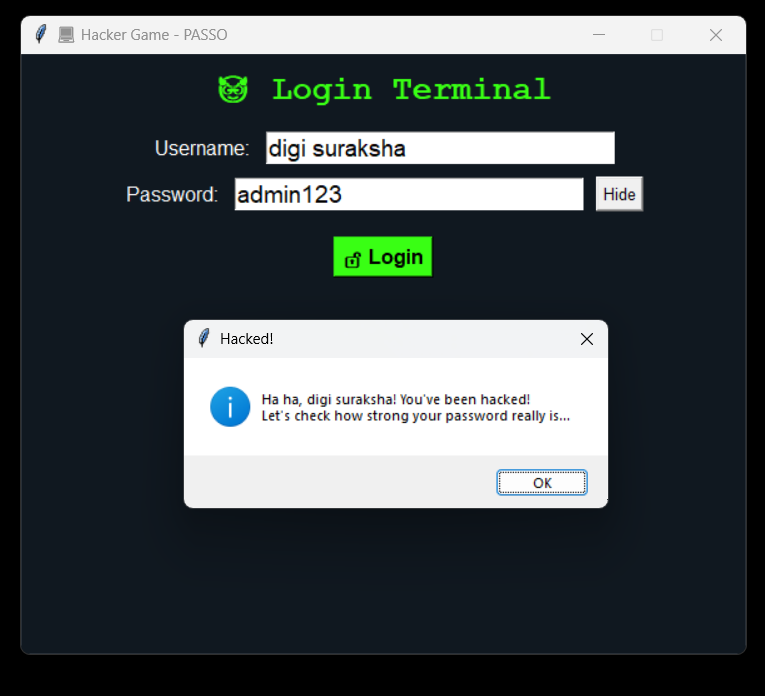
where L is the password length and C is the character set size (e.g., 26 for lowercase, 32 for special characters).

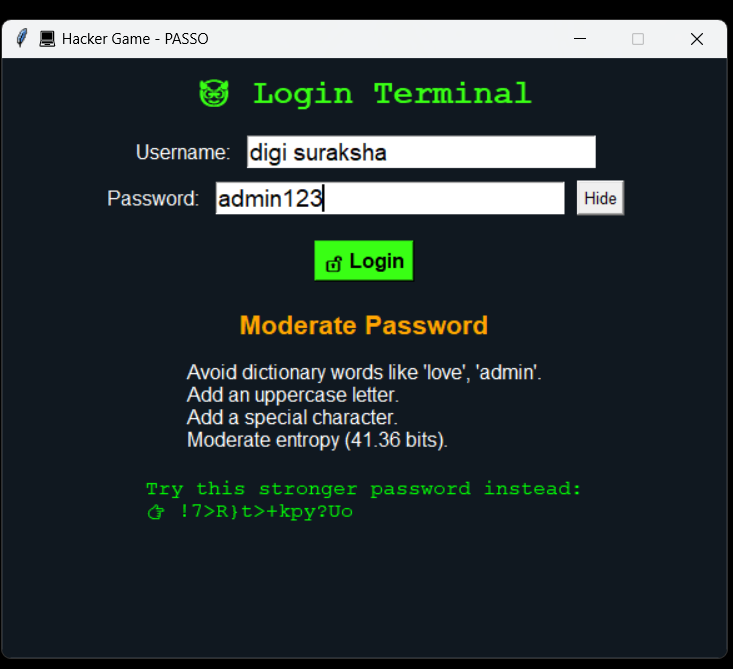
* Interface: A hacker-themed Tkinter GUI with a login simulation, password toggle button, strength indicators (Weak, Moderate, Strong), and detailed feedback. Users receive entropy scores and suggestions for stronger passwords (14 characters, mixed types).

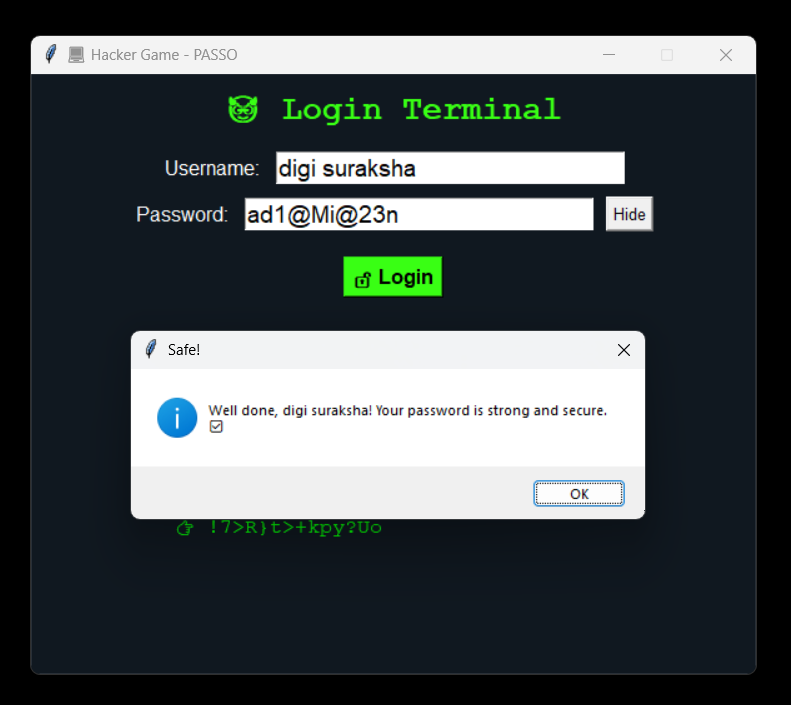
The tool’s design prioritizes usability, making it suitable for educational platforms and personal cybersecurity toolkits.

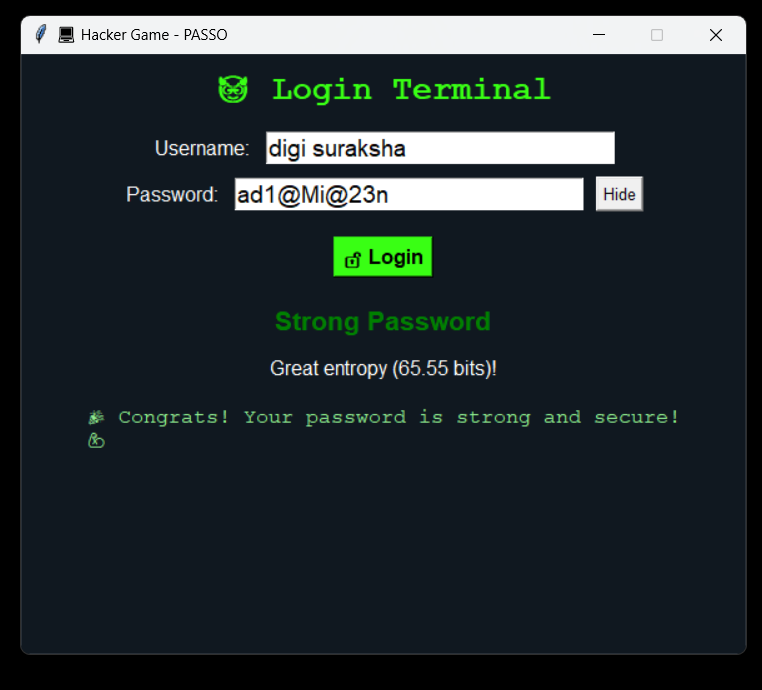
# RESuLTS & OBSERVATIONS

* Tested with 20 passwords
* 15 failed initial criteria
* Common failure: missing special character or uppercase letter
* Feedback improved user awareness of strong password components









# EThICAL IMPACT & MARkET RELEVANCE

This initiative significantly contributes to user education by providing comprehensive resources and training materials that foster a deeper understanding of digital security practices. It actively promotes awareness about potential online threats and vulnerabilities, empowering individuals to make informed decisions to protect their personal information and enhance their overall cybersecurity. By cultivating a culture of awareness and responsibility, this approach not only shields individuals from harm but also encourages a collective commitment to maintaining a secure digital environment.

Market Relevance could be used in web forms, registration systems, or extended into a browser plugin

# FuTuRE SCOPE

While the current password strength checker effectively fulfils its basic role, there are significant opportunities for enhancement:

Multilingual and Unicode Support: By adding support for Unicode characters and non-English alphabets, we can enhance inclusivity and increase password complexity for users worldwide.

Real-Time Web Integration: Transforming the tool into a JavaScript module or API would allow for seamless integration with web forms, providing users instant feedback on password strength during registration or login.

Password Suggestions and History Checks: The tool could recommend stronger alternatives for weak passwords and check against previously used passwords or breach databases like "Have I Been Pwned," promoting better security practices.

Corporate Integration for Policy Enforcement: Organizations can adopt this tool to enforce consistent password policies across their networks, ensuring compliance with vital cybersecurity frameworks like ISO/IEC 27001 or NIST guidelines.

By implementing these enhancements, we can elevate the password strength checker to better meet current and future security demands.

# REFERENCES

Zxcvbn is low-Budget Password Strength Estimation <https://github.com/dropbox/zxcvbn>

A Large-Scale Study of Web Password Habits by Florêncio and Herley [https://www.microsoft.com/en-us/research/publication/a-largescalestudy-of-web-password-habits/](https://www.microsoft.com/en-us/research/publication/a-large-scale-study-of-web-password-habits/)

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes by Bonneau et al. [https://www.cl.cam.ac.uk/~fms27/papers/2012-](https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf)

[BonneauHerOorStapassword--oakland.pdf](https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf)

[M](https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf)ozilla Web Security Guidelines <https://infosec.mozilla.org/guidelines/web_security>

A coding guide for Python language www.youtube.com

For information, knowledge, and understanding https://chatgpt.com/

Towards Evaluating the Strength of User-Generated Passwords <https://ieeexplore.ieee.org/document/4562950>

Microsoft Password Guidance [**https://www.microsoft.com/en-**](https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf)

[**us/research/wpcontent/uploads/2016/06/Microsoft\_Password\_Gui dance-1.pdf**](https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf)

Inspired by: **https://www.youtube.com/shorts/C1jHx8hLV1A**