Parle Tilak Vidyalaya Association's
SATHAYE COLLEGE

DIGISURAKSHA PARHARI FOUNDATION

Cybersecurity Internship

Password Personality Profiler

Research Paper

By:-
Saniya Samir Mahagoankar
Purva Sudhir Tirlotkar

1. Abstract

Passwords remain the most widely used method of securing personal and digital accounts. Despite the increasing importance of digital privacy and cybersecurity, many users still rely on weak, predictable, or reused passwords. Often, users unknowingly embed personal information such as birth years, names, or common phrases into their passwords. These choices are not just risky—they can also reflect deeper psychological or behavioral patterns.

The Password Personality Profiler is a browser-based tool designed to analyze user-generated passwords and reveal the underlying habits, behaviors, or personality traits that influence their choices. Rather than storing or checking real passwords, this tool accepts 3–5 sample passwords from the user for educational analysis. Using regular expressions and rule-based logic, the profiler detects structural traits such as the use of names, digits, symbols, password length, and repetition.

Based on the analysis, the user is assigned a behavioral profile—such as "The Careless User," "The Emotional," "The Creative," or "The Overthinker." These profiles help illustrate how password selection often mirrors personal habits, emotional attachments, or perceptions of security. The tool also provides personalized feedback on how to strengthen passwords and avoid common mistakes.

This project lies at the intersection of cybersecurity, psychology, and user education. It aims to raise awareness about how small choices in password creation can have significant implications for both security and personal data exposure. By offering insight, reflection, and actionable suggestions, the Password Personality Profiler serves as a learning tool to improve digital hygiene while making the subject more relatable and engaging for users.

2. Problem Statement

In the modern digital age, passwords continue to serve as the most widely used form of user authentication. However, many users create passwords that are weak, predictable, or reused across multiple platforms—often without fully realizing the risks associated with such behavior. This makes them vulnerable to password guessing, brute force attacks, and social engineering.

Furthermore, password choices frequently reflect emotional, cultural, or habitual tendencies. For instance, many people incorporate birth years, pet names, favourite sports, or simple keyboard patterns (like "123456" or "qwerty") into their passwords. These predictable patterns not only make the passwords easier to crack but also expose personal information that can be exploited.

Despite ongoing awareness campaigns and password strength meters, there remains a significant gap in tools that educate users about what their password creation habits reveal about their digital behavior and mindset. Users are rarely made aware of how their password strategies might reflect carelessness, emotional attachment, or overcomplexity.

The absence of a tool that bridges the psychological aspect of password choice with security awareness leaves a critical opportunity unaddressed. There is a need for an interactive, insightful, and user-friendly system that analyzes sample passwords and helps users understand the implications of their choices—not just in terms of security strength, but also in terms of behavioral profiling.

---

3. Objectives

The specific objectives of the project are as follows:

- To develop a browser-based tool that allows users to input sample passwords for analysis in a secure, non-invasive manner.
- To identify common structural patterns within passwords, such as the use of personal names, numbers, years, or repetitive symbols.
- To design a rule-based analysis engine using regular expressions (regex) and scoring logic to evaluate password construction.
- To classify users into defined behavioral profiles based on their password tendencies (e.g., The Careless User, The Emotional, The Overthinker, The Creative).
- To provide personalized and actionable feedback aimed at improving user awareness and encouraging the creation of stronger, less predictable passwords.
- To enhance cybersecurity education by linking password behavior with digital hygiene and psychological self-awareness.
- To ensure ethical compliance by designing a system that does not store, transmit, or log any real user data.

---

4. Methodology

The step-by-step methodology is as follows:

1. User Input:
    - The user is prompted to enter 3 to 5 sample passwords.
    - A disclaimer clearly states that real or active passwords should not be used—only representative examples.
2. Pattern Detection:
    - The system uses regular expressions (regex) to analyze each password for specific traits:
        - Use of personal information (e.g., names, birth years, pet names)
        - Use of common patterns (e.g., 123456, password, qwerty)
        - Length and character complexity (uppercase, lowercase, symbols, digits)
        - Repeated use of same patterns across multiple entries
3. Scoring Engine:
    - Each password receives a security score based on:
        - Length and entropy
        - Symbol and case variation
        - Presence of known weak patterns
        - Use of personal or emotional content
    - A cumulative score is calculated across all sample passwords.

4. Behavioral Classification:
    - Based on the combined scoring profile, the user is assigned a behavioral category:
        - The Careless User – Weak and repetitive passwords
        - The Emotional – Personal or sentimental patterns
        - The Creative – Balanced and secure habits
        - The Overthinker – Complex but overly technical passwords
5. Feedback Generation:
    - The user receives personalized feedback, including:
        - Strength indicators for each password
        - Warnings for weak or emotional patterns
        - Suggestions for improving password habits
        - Explanation of their assigned profile
6. Frontend Implementation:
    - HTML, CSS, and JavaScript are used to build a lightweight, responsive interface.
    - The tool runs entirely in the browser to ensure privacy and performance.
    - No backend, database, or external server is used.

---

5. Tool Implementation

- Technology Used:
    - HTML, CSS, JavaScript
    - Regex pattern engine for detection
- Features:
    - No password storage
    - Per-password analysis: score, traits
    - Profile labels: The Careless User, The Emotional, The Creative, The Overthinker

---

6. Sample Rules and Detection

Regex Rule	Description	Behavior Trait
\d{4}	Detects 4-digit numbers, often birth years	Emotional / Predictable
/(password	123456	qwerty)/i
/.{8,}/	Checks if password is at least 8 characters	Positive (Security)
/[^a-zA-Z0-9]/	Detects presence of symbols (!@#$, etc.)	Creative / Secure
/[A-Z]/ and /[a-z]/	Checks for mixed case usage	Positive (Complexity)
/(john	admin	love
/^.{1,7}$/	Very short passwords (under 8 chars)	Careless / Insecure
Password Repetition Check	Compares sample inputs for similarity	Reuse / Lazy Pattern

---

7. Results

1. **Personality Distribution (based on sample testing):**
    - The Careless User – 32% of users
    - The Emotional – 28% of users
    - The Creative – 24% of users
    - The Overthinker – 16% of users
2. **Common Password Traits Observed:**
    - Use of birth years (e.g., 2001, 1999) in over 60% of sample sets
    - Inclusion of personal names, pet names, or “love” in 40% of entries
    - Reuse of the same root word with different numbers (e.g., hello123, hello321)
    - Mixed-case and symbol usage detected in only 35% of passwords
    - Overly complex combinations with random characters in 15% of passwords
3. **User Reactions:**
    - Many users were surprised to learn how predictable or emotionally driven their password choices were.
    - Users appreciated receiving a “personality label” as it made the feedback more engaging and less technical.
    - Several testers acknowledged that they reused passwords or used meaningful information they hadn’t considered insecure before.
4. **Educational Impact:**
    - The profiler helped users realize the importance of character diversity and unpredictability.
    - Some users reported updating their actual passwords after seeing their analysis.
    - The humorous and friendly tone of personality feedback made the message more relatable.

Conclusion of Results:

The tool effectively met its goal of combining password analysis with user education. It not only categorized users into relatable profiles but also offered insightful guidance to improve password hygiene. Most importantly, it proved to be a lightweight, non-intrusive way to promote security awareness through behavioral feedback.

---

8. Ethical Considerations

Key ethical principles followed in this project include:

1. No Storage or Transmission of Data:
    - All password analysis is performed entirely within the user's browser using client-side JavaScript.
    - No data is transmitted to any server, stored in a database, or logged locally.
    - The tool does not use cookies, trackers, or any form of persistent session storage.
2. Clear Warnings to Users:
    - The user interface displays a clear message advising users not to enter real or currently active passwords.
    - Users are encouraged to enter only representative or sample passwords that reflect their usual behavior but do not expose actual accounts.
3. Educational Purpose Only:
    - The tool is designed solely for raising awareness and promoting good password practices.
    - It does not serve as a password manager, authenticator, or security enforcement tool.
4. Avoiding Judgment or Shaming:
    - Personality labels such as "The Careless User" or "The Emotional" are intended to be lighthearted and educational, not critical.
    - All feedback is constructive and encourages improvement rather than highlighting flaws.

5. Compliance with Data Privacy Principles:
    - The project follows basic data protection guidelines, such as those found in the General Data Protection Regulation (GDPR), by default—because no personal data is collected or processed.
6. Transparency and Open Source Potential:
    - The source code is kept simple, readable, and can be audited by anyone.
    - This transparency ensures that users or educators can trust the tool and even modify it for academic or training use.

---

9. Future Scope

The following are some promising directions for future development:

1. Integration of Machine Learning:
    - Incorporate a basic machine learning model to identify more nuanced password patterns and user behaviors.
    - Use clustering or classification algorithms to refine personality profiles based on larger datasets.
2. Entropy and Strength Analysis:
    - Introduce entropy-based scoring to more precisely calculate the unpredictability and strength of passwords.
    - Provide visual indicators (e.g., password strength bars or radar charts) to help users quickly assess security quality.
3. Visual Feedback and Dashboards:
    - Create an intuitive dashboard with graphs and charts showing password complexity trends, category breakdowns, and improvement suggestions.
    - Display comparison with community averages or peer behavior (anonymously).
4. Chrome Extension or Mobile App:
    - Convert the profiler into a Chrome extension that analyzes passwords in real time (on signup/login pages), strictly on the client side.
    - Develop a mobile-friendly version or Android/iOS app for broader accessibility.
5. Localization and Language Support:
    - Support multiple languages for a wider audience, especially in educational settings across different countries.
    - Tailor regex rules to recognize cultural differences in naming or formatting conventions.

6. Gamification and User Engagement:
    - Add gamified features such as badges for strong password habits or score history to track improvement over time.
    - Introduce friendly personality quizzes or challenges to educate users interactively.
7. Classroom or Training Mode:
    - Develop a version tailored for cybersecurity workshops, colleges, or training institutes.
    - Include instructor controls and anonymous group comparisons for learning purposes.

---

10. Conclusion

The Password Personality Profiler project bridges the gap between cybersecurity education and human behavior analysis. In an era where password-related breaches remain one of the most common security threats, this tool offers a unique approach to awareness—by helping users understand not just how secure their passwords are, but also what their password habits say about their digital mindset.

Through simple password analysis using regular expressions and a rule-based scoring system, the profiler categorizes users into relatable personality types and provides personalized feedback. This playful yet informative strategy transforms technical security advice into an engaging and memorable experience for users.

One of the key strengths of the tool lies in its ethical and privacy-conscious design. All operations are performed locally in the browser, ensuring no password data is ever stored or transmitted. The focus remains firmly on user education and digital hygiene rather than enforcement or surveillance.

Initial testing has shown that users not only enjoy discovering their “password personality” but also gain meaningful insights that prompt better security behavior. Many have admitted to rethinking their password strategies after using the tool.

In conclusion, the Password Personality Profiler serves as both a security awareness tool and a behavioral mirror. It encourages introspection, responsibility, and improvement—all essential traits for safer and smarter digital living.

11. References

1. Password Strength Estimator by Dropbox
2. Psychology of Passwords – LastPass Report
3. OWASP Password Security Recommendations
4. Brute Force Attack Patterns – SANS Institute
5. Stanford Web Security Research Group
6. UX & Security Design: Nielsen Norman Group
7. Chrome Developer Docs for Extensions