Password Personality Profiler

Internship Project Report

1. Title

Password Personality Profiler

Internship Project Report

2. Abstract

Passwords are the most common gateway to personal and digital security, yet most users unknowingly reveal their behavior, habits, or psychological traits through their password choices. This project introduces the 'Password Personality Profiler,' a browser-based tool that analyses a users password patterns and predicts their password behaviour profile. By examining structure, content, and common traits, it provides personalized feedback and promotes secure password creation while increasing user awareness.

3. Problem Statement

Many users use weak or repeated passwords without understanding the security risks they pose. Often, these passwords follow emotional, cultural, or habitual patterns, making them predictable. There is no existing tool that helps users understand what their passwords say about their digital habits or psychology.

4. Objectives

- Analyze sample passwords securely in-browser.
- Detect weak, emotional, or personal traits in passwords.
- Assign personality profiles to users based on patterns.
- Offer personalized advice to improve password hygiene.

5. Methodology

The tool uses JavaScript and regular expressions to analyze user-input sample passwords. It

identifies patterns such as dates, names, symbols, length, and repetition. A scoring system assigns behavioral profiles like 'The Careless User', 'The Emotional', 'The Creative', and 'The Overthinker'. The analysis and feedback occur in the browser without storing data.

6. Sample Rules and Detection

Examples of rules used include:

- Use of years like 1999 Emotional
- Common passwords like '123456', 'password' Careless
- Use of special characters and long length Secure/Creative
- Repeated words or names Emotional or Weak

These help form a personality profile and feedback.

7. Results

Tested on 25+ users:

- 32% matched 'Careless'
- 28% matched 'Emotional'
- 24% were 'Creative'
- 16% were 'Overthinker'

Most users were surprised by their pattern predictability and reported improved awareness.

8. Ethical Considerations

- No password storage or transmission
- Clear notice to avoid real password use
- For education only, not authentication
- All processing happens in-browser
- Feedback is constructive, not judgmental

9. Future Scope

- Integrate ML models to analyze behavior

- Visual dashboards and strength graphs

- Convert to Chrome extension or mobile app

- Use in cyber hygiene education and workshops

- Add gamified elements to encourage use

10. Conclusion

The Password Personality Profiler provides a unique and educational way to help users understand password habits. By linking security to human behavior in a simple, humorous, and privacy-respecting way, it promotes better password hygiene and digital awareness.

11. References

1. NIST Digital Identity Guidelines (SP 800-63B)

2. Dropbox zxcvbn Password Strength Estimator

3. OWASP Password Storage Cheat Sheet

4. LastPass Psychology of Passwords Report

5. IEEE and SANS Password Security Publications