

FortiPass

Intelligent Password Strength & Security Tester

FortiPass helps users create safer passwords using OWASP rules, breach checks, and real-time feedback.

Presented By :

Farah Toumi

Thouraya Harrabi

Molka Braham

Presented To :

DR. Manel Abdelkader



Table of Contents

1

Introduction

2

Main Concepts

3

Theoretical Backgrounds &
Standards

4

FortiPass Functional
Flow

5

Advantages / Limitations of
FortiPass

6

Conclusion

Introduction



In today's world, passwords are the first line of defense against cyber threats. But not all passwords are created equal. A “password strength tester” is a system that analyzes how secure a password is by checking it against various rules and patterns. Its job is to detect weak passwords before attackers do.

Weak passwords make systems vulnerable to brute-force attacks, dictionary attacks, and social engineering. That's why we want to educate users and enforce good practices through this tool.

We're aligning our solution with OWASP guidelines, which are globally recognized standards for web application security. This is where FortiPass comes in !

FortiPass is an advanced password strength testing tool that we designed to empower users in building safer digital identities.

Rooted in the principles of OWASP standards and real-time analysis, **FortiPass** goes beyond basic password validation. It uses breach intelligence, intelligent algorithms, and usability-focused design to educate users and enforce strong password habits.

MAIN CONCEPTS & THEORETICAL ASPECTS

a. OWASP Password Policy Requirements FortiPass enforces industry standards for password strength by validating passwords based on a minimum length (e.g., 12+ characters), character diversity (uppercase, lowercase, symbols, numbers), avoidance of common passwords, dictionary words, and public information, and by ensuring the password does not contain parts of the username or email.

b. Password Entropy Password entropy measures the unpredictability of a password using the formula $\text{Entropy} = \log_2(R \cdot L)$, where R is the character space and L is the password length. A higher entropy value indicates a stronger password.

c. Levenshtein Distance This algorithm compares the similarity between the password and personal data such as username or email. It helps prevent the use of passwords that are too similar to easily guessed personal information.

d. zxcvbn Algorithm zxcvbn, developed by Dropbox, is a machine-learned password strength estimator that evaluates password strength based on real-world usage patterns and common attack vectors.

e. Breach Intelligence Integration FortiPass integrates with the HaveIBeenPwned API to check if a password has been exposed in data breaches. It uses a k-anonymity model for secure, privacy-preserving queries.


f. Passphrase Encouragement Instead of encouraging users to create complex random strings, FortiPass promotes the use of long, memorable passphrases such as "farah_thouraya-molka@tbs" which are both secure and user-friendly.

Theoretical Background and Standards

FortiPass is built upon the OWASP Password Policy Project, which outlines best practices for secure password creation and management.

These standards emphasize password length over complexity, recommending a minimum of 12 characters. Unlike outdated practices, OWASP discourages mandatory uppercase/lowercase/symbol combinations and instead promotes passphrases that are both easy to remember and difficult to crack. It also recommends avoiding common passwords, checking for previous breaches, and not imposing password expiration policies without a valid reason.

Theoretical foundations also include entropy-based analysis, which estimates the randomness and predictability of a password. Entropy is often calculated using pattern-matching algorithms like zxcvbn, which simulates real-world guessing strategies rather than just calculating pure statistical randomness. Additionally, k-anonymity protocols are used when integrating breach data sources such as “Have I Been Pwned”, allowing FortiPass to check if a password has been compromised without exposing the user’s actual data.



FortiPass Functional Flow

- **◆ User Input:**
- User enters a password into the FortiPass interface.
- **◆ Validation Engine (Local Checks):**
 - Applies OWASP rules (e.g., length, passphrase, complexity).
 - Computes password entropy using pattern-matching algorithms .
- **◆ Breach Intelligence Check (External API):**
 - Password is hashed.
 - A partial hash is sent to breach checking API using k-anonymity.
 - API returns match if password has been exposed in known breaches.
- **◆ Result Aggregation:**
 - Combines results from local checks and breach check.
- **◆ Real-Time Feedback:**
 - If all conditions are met → strong password .
 - If issues are found → Recommendations for improvement.
- **◆ End of Flow:**
- Password is either approved or suggestions are provided.
- **Goal:** educate user and strengthen password practices.

Unique Value Proposition of FortiPass

What Makes FortiPass Unique?

- Goes beyond basic checks (uppercase, digits, symbols)
- Context-aware analysis: detects user info (email, username) in passwords
- Live breach intelligence: alerts if password appears in real-time leaks
- Preserves privacy using k-anonymity
- Adaptive feedback system: explains password weaknesses and gives clear improvement tips
- Promotes passphrases: long, memorable, and secure word combinations
- Developer-friendly: customizable rules and checks for various use cases
- Scalable for both individual users and enterprise environments

Advantages of FortiPass

FortiPass offers multiple benefits. It aligns perfectly with OWASP standards, promoting modern password practices that balance security and usability.

By integrating breach intelligence, FortiPass goes a step beyond local validation, helping users avoid compromised passwords. Its real-time feedback ensures that users understand the reasons behind password failures and learn to create stronger passwords over time. It also supports the use of passphrases, improving memorability without sacrificing security.

Overall, FortiPass is not just a validator, it is an educational tool that helps users build safer digital identities.

Limitations and Challenges

Despite its advantages, FortiPass has a few limitations. First, it depends on external APIs for breach checking, which may not work offline. Second, it does not function as a password manager or storage system—it is only a strength tester. The tool also relies on user cooperation; if users ignore feedback, the system can't enforce changes. Lastly, while the design is user-friendly, some users may still find security advice confusing or choose weak passwords out of convenience.

Comparison with Existing Tools

Compared to other popular password checkers like Zxcvbn, Google Password Strength Meter, or NordPass Checker, FortiPass stands out in several ways.

Unlike Zxcvbn, which does not check for previously breached passwords, FortiPass integrates breach intelligence directly. Google's checker often lacks passphrase encouragement and transparency in scoring, while NordPass offers breach checks but not real-time educational feedback.

FortiPass combines the best features of all these tools and improves upon them by offering clear explanations, flexible rules, and high privacy standards.



Conclusion

FortiPass is an advanced, OWASP compliant password strength testing tool that empowers users to adopt safer password practices through education, intelligent design, and breach awareness. It combines theoretical concepts like entropy, real world breach data, and adaptive feedback mechanisms to deliver a powerful yet user-friendly solution. While not a replacement for secure storage or multi-factor authentication, FortiPass fills a critical gap in digital hygiene by helping users create stronger, smarter passwords with confidence.

