IT 360 PROJECT

EntriGuard

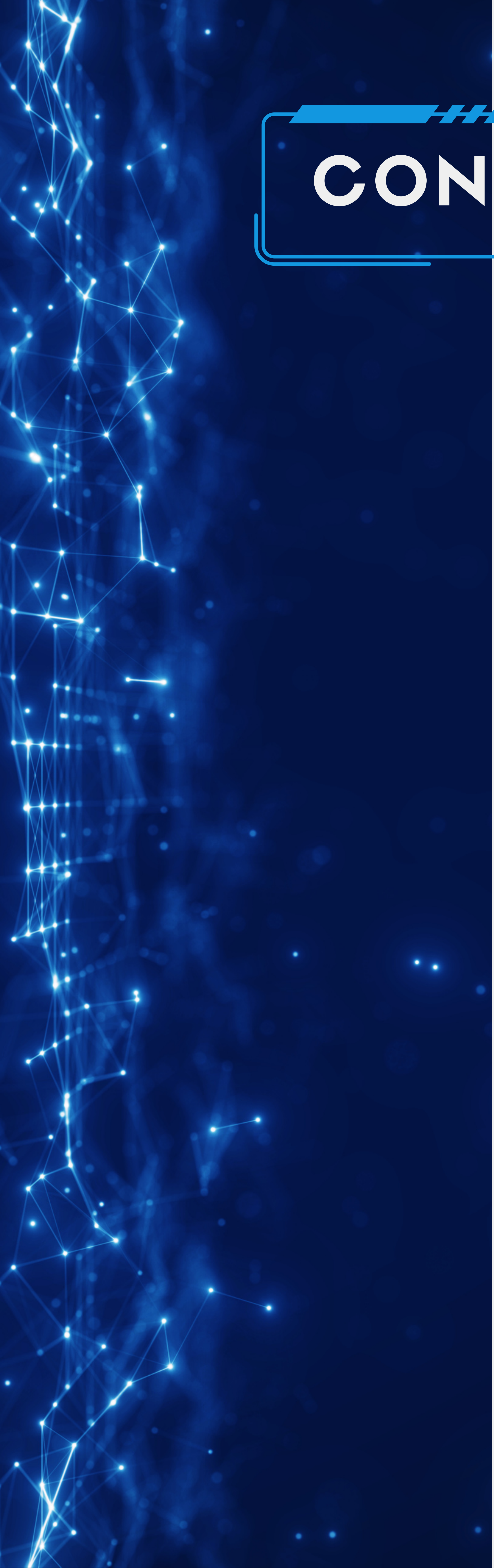
“Password Strength Tester”

BY :
FERDAWES HAOUALA
MELEK KAHLOUN
HOUDA RABIA

TUNIS BUSINESS SCHOOL
UNIVERSITY OF TUNIS

REPORT
TUNIS BUSINESS SCHOOL
2023-2024

CONTENTS



Introduction

As digital dependence grows, so do the threats to our online security. Passwords remain the frontline defense for user accounts, but weak passwords are easily compromised, leading to devastating consequences like data breaches, identity theft, and financial loss.
Thus, creating and remembering strong, unique passwords for various platforms can be a challenge. This is where password strength testers come in to analyze passwords and provide valuable insights into their security.

The Importance of Password Strength Tester:
The Password Strength Tester is a free cybersecurity tool designed to empower users to create strong, secure passwords. It measures the strength of your password using a given criteria such as complexity, length, and randomness. It estimates how much time it would take to crack a given password. To ensure that passwords protect bank accounts, other subscriptions, and internet accounts, use a password tester – it is quick and easy.
This project adheres to the best practices outlined by the Open Web Application Security Project (OWASP).

Main Concepts

1.Main Concepts

OWASP: The project of OWASP Application Security Verification Standard (ASVS) focuses on testing technical security controls of web applications as well as giving developers a checklist for safe development. The main goal of the project is to level out the scope and rigor spectrum in the marketplace in terms of Web application security verification using a commercially workable open standard.d.

Password complexity: Password entropy, also known as password strength is a measure of how hard a password can be guessed especially against brute force attacks. Often for first-time users trying to use applications or devices, password complexity relates to safety requirements that evaluate its security level. The more complex the password is the greater protection it will give against guessing and similar attacks.

Strong vs. Weak Passwords: Strong passwords are long and contain a variety of characters (which include capital letters, lowercase letters, numbers, and symbols). Weak passwords could be short, easily predicted, or composed of common words.

Main Concepts

1.Main Concepts

User Flexibility: Subject-Verb Agreement: Some flexibility has to be given to users in enforcing their password rules so that they can make strong and memorable words. Forcing overcomplicated password codes might result in consumers jotting them down or using them for more than one account, which may undermine security as a whole.

Brute-Force Attacks: This hacking technique uses all possible combinations of characters until the password is eventually guessed. However, cracking strong passwords usually takes much more time than using brute-force attacks.

Password Cracking: It encompasses brute force attacks, dictionary attacks (trying out common words and phrases), and social engineering (tricking the user into revealing the password itself); this is thus an all-inclusive term in which different hacking methods can be classified.

Main Concepts

2. Main Components:

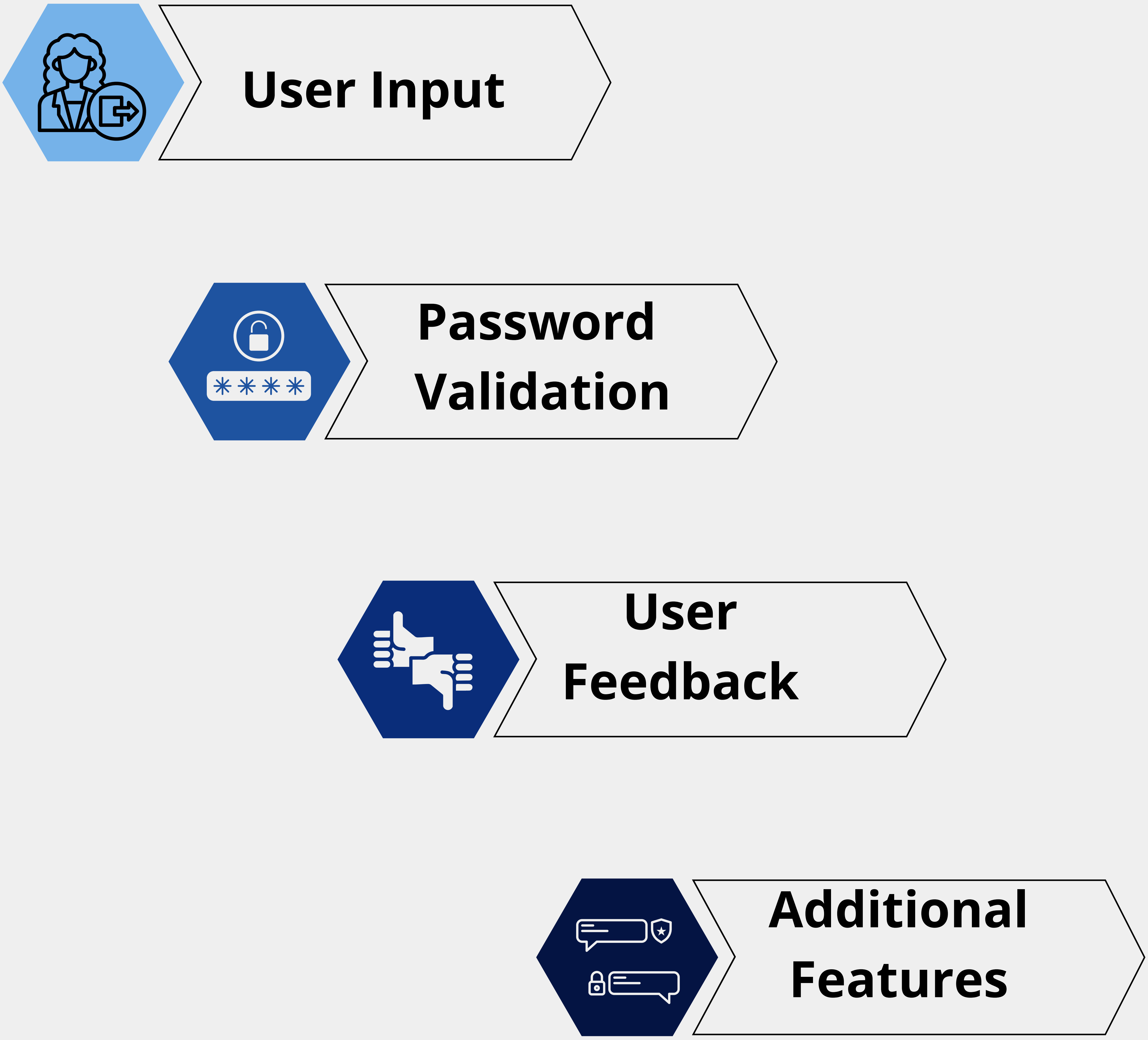
Several major components make up the password strength tester and work together to determine how strong a password is:

- **User Interface (UI):** With the UI, users type passwords or phrases and have their strengths checked. This part offers explicit directives on how to create strong passwords, checks for some basic rules such as minimum length and complexity, and provides a strength score plus feedback to the user.
- **Database:** It keeps track of frequently used passwords in one place. When a password entered by a user matches any entry in the database, irrespective of whether it satisfies current password requirements or not, the system immediately declines it.

- **A password evaluation algorithm:** The system's core component which defines the strength of a password is referred to as the password evaluation algorithm. Since it should comply with the industry's rules and best practices, this algorithm is expected. To determine how strong a given password is, various aspects ought to be put into consideration by this algorithm; these include length, diversity, and identification among others. It has to give suggestions on ways of bettering the password if required.

Main Concepts

3. Functional Flow:



User Input

Password Validation

User Feedback

Additional Features

Main Concepts

3. Functional Flow:

To evaluate the password’s strength and ensure it meets best practices, the Password Strength Tester follows the following process:

1. User Input:

- Users enter their desired password.
- The system should provide clear guidance on creating strong passwords, including length requirements and complexity (mix of uppercase, lowercase, numbers, and symbols).
- Additionally, offering tips for memorability is crucial, as complex passwords can be difficult to remember.

2. Password Validation:

- The system checks the password against essential security standards, like OWASP (Open Web Application Security Project) guidelines.
- This includes minimum length and complexity requirements.
- Furthermore, the system should verify the absence of common words, phrases, or personal information (names, birthdays) to avoid easily guessable passwords.
- Advanced password strength testers might employ techniques like dictionary word checks, common pattern recognition, and verification against known compromised password databases.

Main Concepts

3. Functional Flow:

3. User Feedback:

- The system provides clear and concise feedback on password strength.
- This can include a rating system (weak, medium, strong) or a color-coded indicator for better visual representation.

4. Additional Features (Optional):

- Some password strength testers offer:
- Password expiration and reset functionalities to enforce regular password changes.
- Multi-factor authentication (MFA) for added security beyond just password verification.
- Integration with existing systems for streamlined password management.