IBM Innovation Center for Education

PHEMESOFT
Software That Matters
TRUSTED DELIVERY PARTNER for IBM ICE

RABBI ZIDNI 'ILMA
YENEPOYA
(DEEMED TO BE UNIVERSITY)

Yenepoya (Deemed To Be University)

Password Cracking Resistance Analyzer

PROJECT SYNOPSIS

BACHELOR OF COMPUTER APPLICATIONS & BACHELOR OF SCIENCE
Cyber forensics, Data analytics, Cyber security

SUBMITTED BY

Akshay R – 22BSCFDC06

Muhammed Ismail Salim –22BCACDC45

Athuljith Krishna S B – 22BSCFDC09

Akhil Shan – 22BCACDC08

Sivanand Rajesh – 22BCACDC66

GUIDED BY
Mr. Shashank Korram

Team Member Details

S no	Name	Registration No:	E-mail
1	Akshay R	22BSCFDC06	23605@yenepoya.edu.in
2	Muhammed Ismail Salim	22BCACDC45	22853@yenepoya.edu.in
3	Athuljith Krishna S B	22BSCFDC09	23722@yenepoya.edu.in
4	Akhil Shan	22BCACDC08	21570@yenepoya.edu.in
5	Sivanand Rajesh	22BCACDC66	22408@yenepoya.edu.in

Table of Contents

Introduction

In today’s digital world, passwords are the first line of defense for protecting personal and sensitive information. However, many users still rely on weak or reused passwords, making their accounts vulnerable to hacking and data breaches. With increasing cyber threats, it is crucial to create and use strong, unique passwords.
The Password Strength Checker is a web-based tool designed to help users assess the strength of their passwords quickly and easily. By analyzing factors like length, complexity, and common patterns, it provides immediate feedback to encourage the creation of secure passwords. Additionally, it integrates with the Have I Been Pwned API to check whether a password has been exposed in any known data breaches, helping users avoid compromised credentials.
This project emphasizes privacy and security by ensuring that user passwords are never stored or transmitted in plain text. It aims to educate users about good password practices and contribute to safer online experiences.

Methodology/ Planning of work

The development of the Password Strength Checker project follows a structured approach to ensure effective implementation and timely completion. The key steps involved are:

1. Requirement Analysis
   Gather and analyze the requirements for the application, focusing on password strength metrics, integration with the Have I Been Pwned API, and user privacy considerations.
2. Design
   Design the system architecture, including the frontend interface for user interaction and the backend server to handle password analysis and API communication. Plan secure and efficient data handling methods to protect user information.
3. Development
   - Frontend: Develop a responsive user interface using HTML, CSS, and JavaScript for real-time password strength feedback.
   - Backend: Build the server using Node.js and Express to process password input, perform complexity checks, and query the Have I Been Pwned API using secure hashing techniques (k-anonymity).
4. Testing
   Conduct unit testing of individual components and integration testing to ensure the frontend and backend work seamlessly. Test password checks with various input cases, including common weak passwords and known breached passwords.
5. Deployment
   Deploy the application on a local server for initial testing, followed by preparation for cloud deployment to enable wider access.
6. Documentation
   Prepare detailed documentation covering system design, usage instructions, and security practices to support users and future developers.

Facilities required for proposed work

Software Requirements:

- Node.js & npm: To develop and run the backend server and manage project dependencies.
- Code Editor: Visual Studio Code or any preferred IDE for writing and testing code.
- Web Browser: For testing and using the web-based interface.
- Have I Been Pwned API: To check if passwords have been exposed in data breaches.
- Git: For version control and project management.
- Additional Libraries:
  - Express.js for building the server
  - Axios for API requests
  - Crypto or built-in hashing libraries for secure password handling

Hardware Requirements:

- Development Machine: A computer or laptop with at least 8GB RAM and a multi-core processor (Intel i5 or equivalent) to smoothly run the development environment.
- Storage: Minimum 100 GB free disk space for software, dependencies, and project files.
- Internet Connection: Stable and high-speed internet to access APIs, download dependencies, and deploy the project.