<u>Project Details:</u>

- **<u>Hash identifier</u>**
  - User inputs in textbox -> processed on backend (getHashId()) -> message reflected on frontend
- **<u>Email breach checker</u>**
  - User inputs an email and click check -> processed on backend (isEmailBreach()) -> sent to rapidapi -> response come to backend in json -> purified json data is reflected in frontend
- **<u>Password breach</u>**
  - User inputs an password and click check-> processed on backend (ispasslBreached()) -> sent to pwnedpassword APIv2-> response come to backend in json -> some calculations to get exact number of leakage -> Is leak? And number of leakages is reflected in frontend
- **<u>Message encryption and decryption (A DB is required to store the keys)</u>**
  - 2 input fields
    1. **Encryption ➔** user inputs a plain text on text box -> message in encoded in client end for extra safety -> encoded text is encrypted in backend (encrypt()) -> private key, cipher text and N is stored in the DB with encoding -> cipher text is reflected in frontend with a copy button
    2. **Decryption ➔** user inputs a cipher text -> sent to backend for decryption -> checks if the cipher text is even present in the DB or not, if present -> decrypt the message -> get encoded message -> encoded message is sent to the frontend and decoded in client side and data is reflected in frontend with a copy button