**Project Title:** Password Creator and Evaluator
**Author:** James Imbuido

**Project Overview:**

- In the digital age, data breaches are a constant threat, and weak passwords are often the first line of defense to crumble. For businesses and individuals alike, compromised credentials can lead to devastating financial losses, reputational damage, and even identity theft.
- Traditionally, password security focused on length and complexity, with a mix of uppercase, lowercase, numbers, and symbols. However, brute-force attacks and sophisticated cracking techniques have rendered these basic measures insufficient.
- By harnessing the power of Python, we can move beyond reactive data breach scenarios and proactively build a shield of robust password security. This project empowers individuals and businesses alike to take control of their digital security, one complex, brain-crafted password at a time.
- The machine learning approach used for this project was supervised as it was deemed most appropriate with the dataset.

**Data:**

- The dataset chosen for this project was sampled from ‘’Password Strength Classifier Dataset” from Kaggle (https://www.kaggle.com/datasets/bhavikbb/password-strength-classifier-dataset). This was a dataset supplied by Bhavik Bansal, which is best suited for classification applications.
- The variables involved were ‘password’ and ‘strength’.
- Upon checking in on the raw data, there was no need for further pre-processing of the dataset.

**Model Development:**

- The classification algorithms used in this project were Logistic Regression, Support Vector Machines (SVM), and Naïve Bayes.
- Grid search hyperparameter tuning was conducted on each of the algorithms to optimize their accuracies.

**Evaluation:**

- The metrics used to evaluate these models involved a classification report (accuracy, precision, recall, f1-score) and a confusion matrix.