FortifyGuard: Enhancing Password Resilience Through Strength Analysis

By Jayden R Garcia

WHAT IS FortifyGuard?

- "FortifyGuard" is a password strength checker program designed using Github & Vagrant with the primary intention of enhancing password security and mitigating the risk of hacking. By analyzing the strength of passwords, the program aims to empower users with the knowledge needed to create robust and resilient passwords that are less susceptible to unauthorized access. Utilizing advanced algorithms and techniques, FortfiyGuard assesses the complexity of passwords, considering factors such as length, character variety, and unpredictability to address the vulnerability of weak passwords that are susceptible to exploitation by malicious actors.

Password Resilience Through Strength Analysis

- The ultimate goal of FortifyGuard is to contribute to a safer online environment by encouraging individuals to adopt strong password practices, thereby reducing the likelihood of successful hacking attempts and unauthorized breaches of personal and sensitive information.

Languages

- JavaScript 52.2%   CSS 24.2%
- HTML 23.6%

- This password strength checker program provides a basic way to assess the strength of passwords entered by users. It evaluates passwords based on length and provides feedback on their strength. Implemented using HTML, CSS, and JavaScript. It provides real-time feedback on the strength of a password as it is being typed. When the submit button is clicked, it displays alerts indicating the strength of the password and provides suggestions for improvement.

Visualization

Installing and Using Github & Vagrant

- Github & Vagrant are two different softwares so by default, the following command should be run if you have vagrant but don't already have github:

```
sudo apt-get update
sudo apt-get install git
```

- Navigating to you desired directory inside your VM. Decide where you want to clone your repository using cd to navigate to the appropriate directory.

```
cd /path/to/your/desired/directory
```

```
sysadmin@UbuntuDesktop:~$ ls
Cybersecurity-Lesson-Plans    Documents  Music     Public    Templates
Desktop                       Downloads  Pictures  python    Videos
sysadmin@UbuntuDesktop:~$ cd python
sysadmin@UbuntuDesktop:~/python$ ls
1  2  3  FortifyGuard  password-strength-checker1
sysadmin@UbuntuDesktop:~/python$ cd FortifyGuard
sysadmin@UbuntuDesktop:~/python/FortifyGuard$ ls
FortifyGuard                          index.html  README.md  styles.css
FortifyGuard-Password-Strength-Checker  LICENSE     script.js  Vagrantfile
sysadmin@UbuntuDesktop:~/python/FortifyGuard$
```

FortifyGuard: Password Strength Checker Demo

https://github.com/Jayden94Garcia/
password-strength-checker

Live Demo Website
https://jayden94garcia.github.io/password
-strength-checker/

Mitigating Password Threats

- In essence, the combination of GitHub and Vagrant streamlines the development and deployment of FortifyGuard. It enables effective collaboration, version control, and the creation of a reliable, reproducible environment for developing and testing the password strength checker program. This cohesive approach will contribute to the successful realization of the project's goal to enhance password security and mitigate vulnerabilities.
- Mitigating password threats is achieved through the use of a password strength checker program. This tool assesses the quality of passwords by identifying weak passwords, users are prompted to enhance their security with stronger alternatives. This proactive approach reduces the vulnerability to unauthorized access, data breaches, and cyberattacks.

The End Goal: Vulnerability being exploited in creating FortifyGuard

- The end goal of creating FortifyGuard, is to address the vulnerability of weak passwords that are susceptible to exploitation. The program aims to analyze and identify the shortcomings of passwords, such as lack of complexity, common patterns, and inadequate length. By highlighting these vulnerabilities, FortifyGuard empowers users to take proactive measures in strengthening their passwords. Through education and actionable insights, the program strives to create a more secure digital landscape, mitigating the potential for unauthorized access.