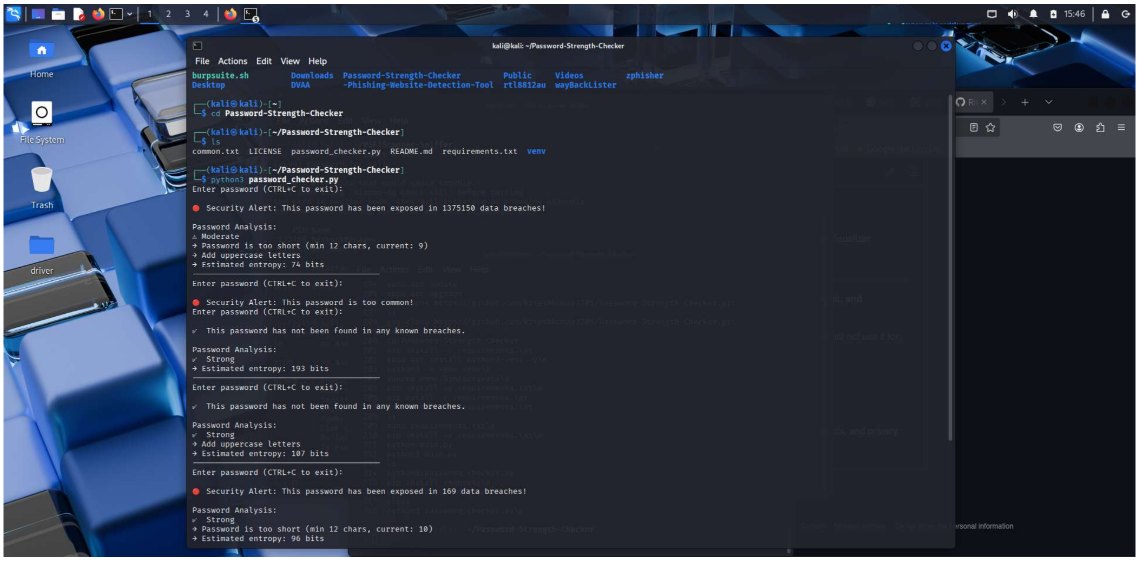
SAMPLE OUTPUT:-

The Password Strength Checker evaluates the entered password based on its presence in known data breaches, entropy-based strength, and compliance with recommended security practices. Below is an example of the output generated during program execution:



kali@kali: ~/Password-Strength-Checker
File Actions Edit View Help
Home
File System
Trash
driver
15:46

```
burpsuite.sh          Downloads  Password-Strength-Checker          Public     Videos         zphisher
Desktop               DVAA       -Phishing-Website-Detection-Tool   rtl8812au  wayBackLister

┌──(kali㉿kali)-[~]
└─$ cd Password-Strength-Checker

┌──(kali㉿kali)-[~/Password-Strength-Checker]
└─$ ls
common.txt  LICENSE  password_checker.py  README.md  requirements.txt  venv

┌──(kali㉿kali)-[~/Password-Strength-Checker]
└─$ python3 password_checker.py
Enter password (CTRL+C to exit):

● Security Alert: This password has been exposed in 1375150 data breaches!

Password Analysis:
⚠ Moderate
→ Password is too short (min 12 chars, current: 9)
→ Add uppercase letters
→ Estimated entropy: 74 bits
────────────────────────────────────────
Enter password (CTRL+C to exit):

● Security Alert: This password is too common!
Enter password (CTRL+C to exit):

✓ This password has not been found in any known breaches.

Password Analysis:
✓ Strong
→ Estimated entropy: 193 bits
────────────────────────────────────────
Enter password (CTRL+C to exit):

✓ This password has not been found in any known breaches.

Password Analysis:
✓ Strong
→ Add uppercase letters
→ Estimated entropy: 107 bits
────────────────────────────────────────
Enter password (CTRL+C to exit):

● Security Alert: This password has been exposed in 169 data breaches!

Password Analysis:
✓ Strong
→ Password is too short (min 12 chars, current: 10)
→ Estimated entropy: 96 bits
```