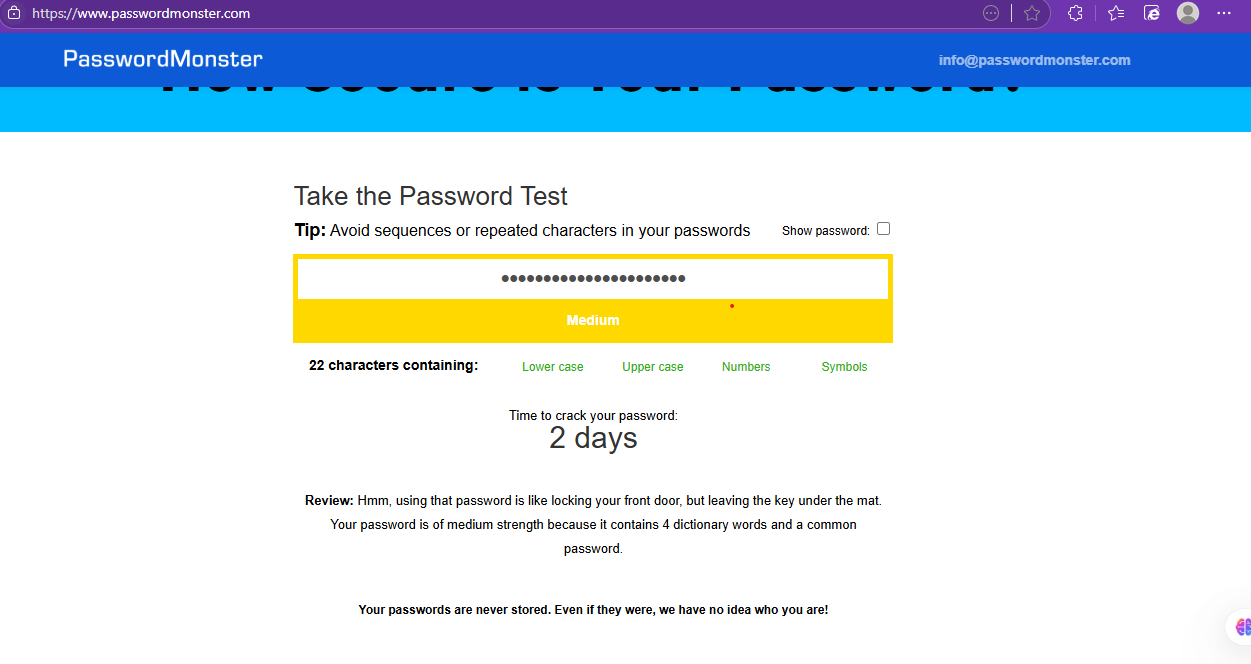
Task 6 ELEVATE LABS: Harshitha M

Creating strong passwords and analysing its strength



**🔐 Password Details**

* **Length**: 22 characters
* **Character Types Used**:
  + ✅ Lowercase letters
  + ✅ Uppercase letters
  + ✅ Numbers
  + ❌ **Symbols** (not used)

**📊 Password Strength Rating**

* **Rating**: **Medium**
* **Estimated Time to Crack**: **2 days**
* **Reason Given**:
  + Contains **4 dictionary words**
  + Includes a **common password**

**📋 Review Summary**

"Using that password is like locking your front door, but leaving the key under the mat."

This means:

* Even though the password is **long**, its **predictability** (due to dictionary words and common patterns) weakens it.
* Attackers using **dictionary attacks** or **brute-force tools** with pre-built wordlists could still crack it fairly quickly.

**✅ Tips to Improve the Password**

To raise the strength from **Medium** to **Strong**:

1. **Add special symbols** (like !, @, #, ^, etc.)
2. **Avoid common dictionary words** or break them up with symbols or numbers.
3. **Use passphrases that are unique or nonsensical** (e.g., Blu3!Cr0w@D@wn2025)
4. Consider a **random password generator** or a **password manager** to create & store complex passwords.