KATA: You shall not pass

Create a method to check the strength of a password passed as a parameter. There are 5 criteria which determine the strength of a password. Nordic letters are not catered for simplicity.

A password is said to be **strong** if it satisfies the following criteria:

1. It contains at least one lowercase English (non-Nordic) character.
2. It contains at least one uppercase English (non-Nordic) character.
3. It contains at least one [special character](https://owasp.org/www-community/password-special-characters). You can simply check for not alphanumeric.
4. Its length is at least 8.
5. It contains at least one digit.

If the password matches 3-4 of the above criteria it is **moderate** and if it matches only 1-2 it is **weak**.

If the password is less than 6 characters long, or contains white spaces, return **invalid**.

The examples given should be written as **unit** **tests**, it is recommended to approach this from a test-driven development perspective.

**Optional upgrade:** Tell the user why their password was weak, i.e. what they still need to do to make it strong. You can break design convention for this and simply WriteLine() in the check password strength method.

**Examples:**

stonk -> “Invalid”

pass word -> “Invalid”

password -> “Weak”

11081992 -> “Weak”

mySecurePass123 -> “Moderate”

!@!pass1 -> “Moderate”

@S3cur1ty -> “Strong”