Assignment for Application Developer Applicants :

You are writing authentication module for your first website. In order to ensure your users are not vulnerable to brute force attacks on weak passwords you want to help them create better passwords. Write a program to check the validity of password input by users with respect to following rules:

1. Minimum length: 6
2. Maximum length: 12
3. At least 1 letter in [a-z], [0-9], [A-Z] and [*$_#=@] each.
4. It should not contain any letter from [%!)(]

Your program should accept a sequence of comma separated passwords and will check them according to the above criteria. Print out each password with resulting 'Success' or 'Failure'. In case of 'Failure' also print the reason for failure in the same line.

Example
If the following passwords are given as input to the program:
12sdA@83,a F1#,2w3E*%dg,2We3345, 1234567
Then, the output of the program should be:
12sdA@83 Success
a F1# Failure Password must be at least 6 characters long.
2w3E*%dg Failure Password cannot contain %!)(.
2We3345 Failure Password must contain at least one letter from *$_#=@.
1234567 Failure Password must contain at least one letter from a-z.

Hint: Error messages for each check:

1. Password must be at least 6 characters long.
2. Password must be at max 12 characters long.
3. Password must contain at least one letter from <set_that_failed>.
4. Password cannot contain %!)(.