

Требования по созданию пароля:

- Не менее 6 символов

- Обязательно должно быть как минимум:

Одна Заглавная буква, одна строчная буква, одна цифра, один спецсимвол

1) Найти классы эквивалентности

2) Найти граничные значения

3) Напишите тесты

Перед тем как проводить разделение на классы и писать тесты, проанализируем требования, зададим вопросы и попробуем найти на них предполагаемые ответы в рамках ДЗ.

1. По требования длина пароля 6 и более символов. Более это сколько? 20? 50? 100? Почему?

Как правило, длина пароля зависит от алгоритма хэширования. Рекомендуется использовать SHA-256, длина поля ввода есть только теоретически…

Можно предположить, что пароль будет хранится, как тип CHAR (который хранит 256 символов) или VARCHAR(а какая длина?) или как BINARY(32). Но это только мои предположения, а хотелось бы знать, что бы таки не сломать… Допустим у нас 256…

То есть тут вопрос!

2. Символы какого алфавита допустимы? Только латиница, кириллица, греческие буквы и т.д.??? Логика подсказывает, что только латиница. Но я, например, на своей работа работаю с базой, где существуют логины, и пароли и латиницей и кириллицей.

То же вопрос!

Сначала выделим классы эквивалентности по длине вводимого значения

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
| 1 5 | 7 | |  |
| 6 | |  |  |

Класс 1. 0 / NULL – то есть поле пустое

Класс 2. 1-5

Класс 3. 6 – 255

Мне кажется, что класс «NULL» необходимо выделить отдельно. Тогда же следующий будет начинаться не с 0, а с 1, т.к. это количество введенных символов, а не их значение.

При проведении тестов с первым классом и вторым классом должно быть сообщение об ошибке. Тут, по-моему, не надо проводить проверку отвечает ли пароль ниже приведенным требованиям или нет.

Негативные сценарии

Тест-кейс ПВ1. Проверка поля «Password» с длиной данных менее 6 символов

1. Ввести пароль с количеством символов согласно таблицы 1.

2. Нажать кнопку «Submit»

Таблица 1.

|  |  |
| --- | --- |
| Введенное значения | Ожидаемый результат |
| Оставить поле пустым | Сообщение об ошибке |
| Ввести пароль из 1 символа «А» | Сообщение об ошибке |
| Ввести пароль из 5 символов «12345» | Сообщение об ошибке |

Все введенные значения по условиям класса эквивалентности 3 будут 6 и более символов, но менее 256.

При исследовании третьего класса необходимо производить проверку по следующим требованиям, предъявляемым в условии к паролю: «*должно быть как минимум: Одна Заглавная буква, одна строчная буква, одна цифра, один спецсимвол*»

Проверим сначала класс эквивалентности 3 на граничные значения по длине с условием валидности самого значения.

Тест-кейс ПВ2. Проверка поля «Password» с длиной данных от 6 до 256 символов с валидным значением

1. Ввести пароль согласно таблицы 2.

2. Нажать кнопку «Submit»

Таблица 2.

|  |  |  |
| --- | --- | --- |
| Введенное значения | Ожидаемый результат |  |
| Ввести пароль из 6 символа «Pass-123» | Переходим на следующую страницу |  |
| Ввести пароль из 256 символов «PASword$123456….256» | Переходим на следующую страницу | Тут я понимаю, что перебор…. |
| Ввести пароль из 257 символов «PASword$123456….257» | Сообщение об ошибке | Опять перебор ? |

В рамках класса эквивалентности 3, выделим следующие классы, с условием, что буквы будут только латиницей:

1. только заглавные буквы
2. только прописные буквы
3. прописные и заглавные буквы
4. только цифры
5. только спецсимволы
6. цифры и спецсимволы
7. заглавные буквы и цифры
8. заглавные буквы и спецсимволы
9. прописные буквы и цифры
10. прописные буквы и спецсимволы
11. заглавные буквы, цифры и спецсимволы
12. прописные буквы, цифры и спецсимволы
13. заглавные буквы, прописные буквы, цифры и спецсимволы

Тут хочется составить таблицу с возможными вариантами, примерами и ожидаемым результатом

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | заглавные буквы | прописные буквы | цифры | спецсимволы | пример | ожидаемый результат |
| 1 | + | - | - | - | PASSWORD | error |
| 2 | - | + | - | - | password | error |
| 3 | + | + | - | - | PASSword | error |
| 4 | - | - | + | - | 1234567 | error |
| 5 | - | - | - | + | @#$#!$^% | error |
| 6 | - | - | + | + | 123@#$@ | error |
| 7 | + | - | + | - | PASS1234 | error |
| 8 | + | - | - | + | PASS@#@ | error |
| 9 | - | + | + | - | pass9874 | error |
| 10 | - | + | - | + | pass#$%^ | error |
| 11 | + | - | + | + | PASS-123 | error |
| 12 | - | + | + | + | pass\*123 | error |
| 13(1) | + | + | + | + | Pass-123 | OK |
| 13(2) | + | + | + | + | 123»PASw | OK |

То есть классы с 1 до 12 будут негативными, а 13 класс будет позитивный

Тест-кейс ПВ3. Проверка поля «Password» значением, содержащим буквы латиницы (заглавные, прописные), цифры, спецсимволы, с валидной длиной

1. Ввести пароль согласно таблицы 3.

2. Нажать кнопку «Submit»

Таблица 3.

|  |  |
| --- | --- |
| Введенное значения | Ожидаемый результат |
| PASSWORD | Сообщение об ошибке |
| password | Сообщение об ошибке |
| PASSword | Сообщение об ошибке |
| 1234567 | Сообщение об ошибке |
| @#$#!$^% | Сообщение об ошибке |
| 123@#$@ | Сообщение об ошибке |
| PASS1234 | Сообщение об ошибке |
| PASS@#@ | Сообщение об ошибке |
| pass9874 | Сообщение об ошибке |
| pass#$%^ | Сообщение об ошибке |
| PASS-123 | Сообщение об ошибке |
| pass\*123 | Сообщение об ошибке |
| Pass-123 | Переходим на следующую страницу |
| 123»PASw | Переходим на следующую страницу |

При данной постановке задачи, у меня возник еще вопрос. А если мы введем в поле пароля JavaScript, например,

<script>alert(‘Hello!’)</script>

Или же тег html, например

<hr style="border-color: red;"> (тут тоже возникает вопрос, написанный ниже)

Тут же все условия пароля выполняются.

Не совсем понятно как будут обрабатываться «белые пробелы».

То есть понятно, что при введении 6 пробелов не будет выполняться условие для пароля и должно выводиться сообщение об ошибке.

А вот если перед или после валидного пароля будут стоять пробелы?

А если внутри пароля будет стоять пробел?

Я так понимаю, это тоже будет зависеть от типа данных, в котором будет храниться пароль…

Это тоже надо как-то учитывать в классах эквивалентности?

Так же необходимо выделит отдельно класс, в котором будем использовать и/или кириллицу. Но мне кажется, перебор всех вариантов проводить нет смысла, т.к. при введении в поле хотя бы одного символа кириллицы должна появляться ошибка.

Тест-кейс ПВ5. Проверка поля «Password» с длиной данных от 6 до 256 символов использованием кириллицы

1. Ввести пароль, содержащий кириллицу, цифры, спецсимволы: Пароль№123

2. Нажать кнопку «Submit»

Ожидаемый результат: Сообщение об ошибке