## 页面描述

web登录页面：有两个文本框，一个提交按钮(注册、忘记密码等按钮)

## 用例设计

### 【功能测试(Function test)

0.什么都不输入，点击提交按钮，看提示信息。（非空检查）

1.输入正确的用户名和密码，点击提交按钮，验证是否能正确登录。（正常输入）

2.输入错误的用户名或者密码, 验证登录会失败，并且提示相应的错误信息。（错误校验）

3.登录成功后能否能否跳转到正确的页面（低）

4.用户名和密码，如果太短或者太长，应该怎么处理（安全性，密码太短时是否有提示）

5.用户名和密码，中有特殊字符（比如空格），和其他非英文的情况（是否做了过滤）

6.记住用户名的功能

7.登陆失败后，不能记录密码，用户名可以保存

8.用户名和密码前后有空格的处理

9.密码是否加密显示（星号圆点等）

10.登录需要验证码的，输入完用户名和密码后，验证码为必填项

11.牵扯到验证码的，还要考虑文字是否扭曲过度导致辨认难度大，考虑颜色（色盲使用者），"刷新"或"换一个"按钮是否好用

12.登录页面中的注册、忘记密码，登出用另一帐号登陆等链接是否正确

13.输入密码的时候，大写键盘开启的时候要有提示信息。

14.输入错指定次数后，账号锁定，需要做解锁处理

15.登录失败的提示信息需要高亮处理

16.登录失败有次数限制的，每失败一次，提示剩余可以登录次数和处理建议

### 【界面测试(UI Test)

1.布局是否合理，输入框和按钮是否对齐

2.输入框和按钮的长度，高度是否复合要求

3.界面的设计风格是否与UI的设计风格统一

4.界面中的文字简洁易懂，没有错别字。

### 【性能测试(performance test)

1.打开登录页面，需要几秒

2.输入正确的用户名和密码后，登录成功跳转到新页面，不超过5秒

3.多用户登录是否达到设计要求

4.登录达到需求上限，系统稳定工作时间达到要求

### 【安全性测试(Security test)

1.登录成功后生成的Cookie，是否是httponly (否则容易被脚本盗取)

2.用户名和密码是否通过加密的方式，发送给Web服务器

3.用户名和密码的验证，应该是用服务器端验证， 而不能单单是在客户端用javascript验证

4.用户名和密码的输入框，应该屏蔽SQL注入攻击

5.用户名和密码的的输入框，应该禁止输入脚本 （防止XSS攻击）

6.错误登陆的次数限制（防止暴力破解）

7.考虑是否支持多用户在同一机器上登录；

8.考虑一用户在多台机器上登录

9.cookie有效时间验证

### 【可用性测试(Usability Test)

1.是否可以全用键盘操作，是否有快捷键

2.输入用户名，密码后按回车，是否可以登陆

3.输入框能否可以以Tab键切换

### 【兼容性测试（Compatibility Test）

1.主流的浏览器下能否显示正常已经功能正常（IE,6,7,8,9, 10，Firefox, Chrome, Safari,等）

2.不同的平台是否能正常工作，比如Windows, Mac

3.移动设备上是否正常工作，比如Iphone, Andriod

4.不同的分辨率

### 【本地化测试 （Localization test）

1.不同语言环境下，页面的显示是否正确。

### 【软件辅助性测试 （Accessibility test）

软件辅助功能测试是指测试软件是否向残疾用户提供足够的辅助功能

1. 高对比度下能否显示正常 （视力不好的人使用）

**注册要求：**

1.注册账号可以是手机号或邮箱。

2.手机号码：中国地区手机号长度11位，以13/14/15/17/18开头

3.邮箱：  “@”前面的部分、“@”和最后一个“.”之间部分、最后一个“.”后面的部分和一些其他的情况

4.密码：英文或英文数字组合，8-20位，区分大小写 （数字：0,1,2,3,4,5,6,7,8,9 字母：a-z，A-Z）

针对此注册功能的页面，测试用例（效率高+覆盖全+逻辑明确）

 选择正确的输入值，可注册成功：

（1）符合格式的手机号、新密码为符合要求的非最多和最少的字符（数字+英文）、确认密码一致、正确验证码  （冒烟测试）

（2）符合格式的邮箱、新密码为符合要求的非最多和最少的字符（纯英文）、确认密码一致、正确验证码（冒烟测试）

一、账号输入框：

1.手机号：

A、有效等价类：13\14\15\17\18开头的11位纯数字

B、无效等价类：

         （1）位数不等于11（大于或小于）

（2）全角数字

         （3）号码包含非数字（中文、英文/大小写、特殊字符）

         （4）号码中包含空格（前/中/后、中英文/全半角空格）前后的空格能不能自除，一般要求自除，另外全角和半角的空格长度是不一致的，全角空格，定义上是2个半角空格的大小，在网页中却大约相当于3~4个半角空格的大小（中文全半角和英文全半角是一致的）

         （5）不以13\14\15\17\18开头。如10、12、63开头

2.邮箱：

     邮箱的验证要根据需求来，因为邮箱众多，涉及的会比较复杂（不一一描述）

     但归根揭底是要验证 “@”前面的部分、“@”和最后一个“.”之间部分、最后一个“.”后面的部分和一些其他的情况

二、密码和确认密码

1.正常输入，无提示异常:

（1）密码为符合要求的非最多和最少的字符（数字+英文），确认密码一致

（2）密码为符合要求的最少字符（数字+英文），确认密码一致

（3）密码为符合要求的最多字符（英文），确认密码一致

（4）可选：密码为符合要求的最多字符-1（数字+英文），确认密码一致

（5）可选：密码为符合要求的最少字符+1（英文），确认密码一致

 （6）注册成功后用密码登录 ，登录成功

 （7）注册成功后，用密码更换大小写（大写变小写、小写变大写），登录失败【用于中英文大小写，如没要求，忽略此条】

2.注册失败，提示异常信息：

（1）密码为符合要求的最少字符 -1，提示

（2）密码为符合要求的最多字符 +1，提示

 （3）密码为符合要求的非最多和最少的字符，且密码为非允许字符或允许字符加上非允许字符，提示

            【特殊字符（如@、#、-、+等）、汉字等】

1. 密码和确认密码包含空格，提示

 （5）密码和确认密码不一致，提示

 （6）新密码中英文小写，确认密码中英文大写（或相反）【中英文大小写，如没要求，忽略此条】

3.密码是否以 \* 或 · 之类的加密符号

4.密码是否可以复制、粘贴（可从外面黏贴进来，不能出密码输入框复制出去）

三、验证码

可分为3个：

1.对手机号格式和邮箱格式的验证，这个上面已经有提过了，这里略过不提

2.对验证码获取功能的验证

3.对验证码是否正确也要进行验证

具体可分为以下几小点：

（1）手机号或邮箱格式不正确的，无法点击发送验证码

（2）先输入符合的的手机号或邮箱，再删除一些手机号删除1位，邮箱删除@，变成格式不正确的手机号和邮箱，验证是否可以点击发送验证码（不能发送）

（3）手机号或邮箱格式正确，且已注册过的，不可发送

（4）手机号或邮箱格式正确，且未注册过的，可发送（分别验证手机号和邮箱）

（5）输入正确验证码6位，不提示错误

（6）输入正确验证码6-1位，提示错误

（7）输入正确验证码6+1位，提示错误

（8）输入错误验证码6位（非数字，字母、符号、中文或数字字母符号中文混合）

（9）明确验证码的失效时长后，在时长之后输入输入码，提示该验证码已失效，请重新获取验证码（提示：对不起，验证码不存在或者已经超时！）

（10）倒计时是否有异常，倒计时最好长一些（60秒），倒计时期间，发送验证码按钮不能再被点击

（11）发送验证码次数过多，是否有提示（主要针对手机，邮箱无此限制，参考百度，如果发送验证过多，会提示24小时之后再发送）

四、服务协议和隐私政策

1.服务协议和隐私政策内容无错别字、排版整齐

2.勾选协议，正常注册

3.不勾选协议，提示要勾选

4.先勾选，在勾除，提示要勾选

五、其他

1.看是否支持tap和enter键等；

2.各输入框非空校验

3.各链接正确

4.既然是web系统，那么进行兼容性测试要涉及到：

（1）浏览器：IE6-11，谷歌浏览器、火狐浏览器这几个是主要的，还有根据需求其他的浏览器

（2）分辨率：一般是1360\*768以上、包括1080P、2K（比较少）。一般1360\*768和1080P是主流

（3）CPU（一般用于手机app测试，web较少）

（4）屏幕尺寸（一般用于手机app测试，web较少）

（5）各个PC品牌（一般用于手机app测试，web较少）

边界值分析

闭区间：                范围为[1-10]，上点为1和10，离点为0和11，内点为域内得任意点

闭区间和开区间：范围为（1-10]，上点为1和10，离点为2和11，内点为域内得任意点

开区间：                范围为（1-10），上点为1和10，离点为2和9，内点为域内得任意点

**考虑的常见场景：**

**登录：**

1、用例是否考虑A的用户名+B的密码？（后端）

2、用例是否考虑母账号被禁用，子账号是否能登录？

3、用例中是否考虑，一个用户多地登陆的场景？

4、用例是否考虑登录时，密码是否明文显示？

5、用例是否考虑登录按钮只能在用户名或者密码文本框都符合格式下点击才能发送请求？（前端）

6、用例是否考虑未注册用户名的登录？

7、用例是否考虑用户名输入格式（特殊字符，中英文字符，字符长度，为空）？

8、用例是否考虑密码文本框格式（特殊字符，中英文字符，字符长度，为空）？

9、用例是否考虑登录错误次数太多，极验是否弹出？

10、用例是否考虑记住用户名的情况下，直接关闭页面，再次打开登录页面，是否直接登录成功？

11、用例是否考虑记住用户名的情况下，点击退出，再次打开登录页面，是否直接登录成功？

12、用例是否考虑没记住用户名的情况下，直接关闭页面，再次打开登录页面，是否直接登录成功？

13、用例是否考虑没记住用户名的情况下，点击退出，再次打开登录页面，是否直接登录成功？

14、用例是否考虑，多个用户在一个地点登录的场景？

**注册：**

考虑的常见场景：

1、用例是否考虑用户名输入格式（特殊字符，中英文字符，字符长度，为空）？

2、用例是否考虑密码文本框格式（特殊字符，中英文字符，字符长度，为空）？

3、用例是否考虑手机文本框格式（特殊字符，中英文字符，字符长度，为空）？

4、用例是否考虑验证码文本框格式（特殊字符，中英文字符，字符长度，为空）？

5、用例是否考虑密码可否明文显示？

6、用例是否考虑极验弹出的情况和频率？

7、用例是否验证手机号码唯一性？

8、用例是否考虑每天发送短信的次数？

9、用例是否考虑注册按钮只能在用户名或者密码文本或者验证码都符合格式下才能点击注册请求？

**忘记密码**

正常类测试

点击忘记密码       ———1.页面成功跳转到重置密码页面 2.页面显示当前绑定的手机，需输入验证码和重置密码

点击获取验证码     ——该手机成功收到验证码

输入一致的新密码>提交   ——提交成功密码重置成功，点击【返回首页】，回到首页

异常类测试

填写错误的验证码      ——提示验证码错误

查看提交按钮          ——所有内容未填写完整，提交按钮置灰

输入格式错误的新密码       ——格式错误

输入不一样的重复密码    ——两次密码不一致

记住密码

正常类测试

点击勾选记住我   ——记住账号密码，再次登陆不需要再次填写

注册界面测试流程：

正常类测试

点击注册  ——跳转到注册界面

进入注册面，查看必填项  ——XX，XXX，XXX……为必填项

输入正确的有效的手机号，点击获取验证码   ——获取验证码成功，提示验证码已发送，重新获取为60s

输入所有有效的信息，正确的手机号和验证码          ——注册成功，跳转到XX页

异常类测试

输入不存在的手机号，点击获取验证码 ——提示手机号不存在

输入正确的手机号，填写错误的验证码  点击注册  ——注册失败

**快速注册**

正常类测试

点击快速注册 ---跳转到快速注册页面

进入快速注册页面，输入有效手机号，点击：发送验证码

获取验证码成功，提示验证码已发送，显示：XXs

输入正确的验证码点击注册----注册成功，跳转到首页

异常输入测试

输入不存在的手机号，点击获取验证码 ——提示手机号不存在

输入正确的手机号，填写错误的验证码  点击注册  ——注册失败