# 游戏测试笔试题

请根据题目内容，设计相应的测试用例。

1、a、b、c分别为三角形的三条边，请设计测试该三角形的测试用例。

1. 等价类划分、边界值分析：

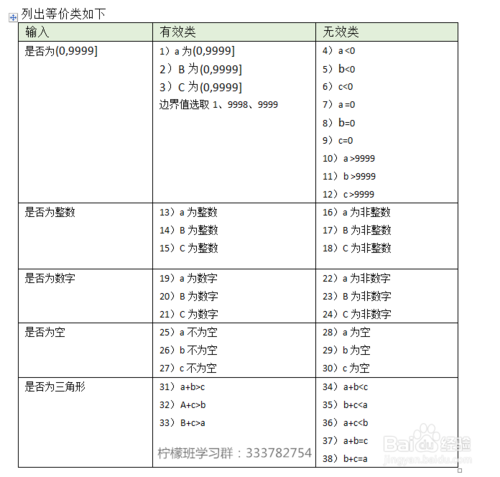
1.这道题的输入为a、b、c的值，值的要求数据类型满足正整数、长度满足(0,9999]；

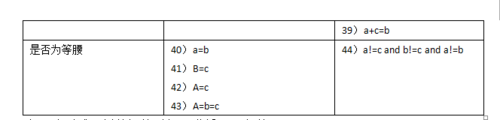
细分正整数、长度，得出输入值的要求(1)(0,9999] (2)整数 (3)数字 (4)3个数

2.三角形的要求，(5)任意2边之和大于第3边

3.等腰三角形的要求，(6)任意2边相等

满足以上要求，则正确输出等腰三角形

[](http://jingyan.baidu.com/album/2d5afd69d3c29b85a3e28e7b.html?picindex=2)

[](http://jingyan.baidu.com/album/2d5afd69d3c29b85a3e28e7b.html?picindex=3)

1. 在设计测试用例数据的时候，遵循下面条件

先新增一条测试用例覆盖尽量多的有效类，再逐步补充用例，确保所有有效类覆盖完全

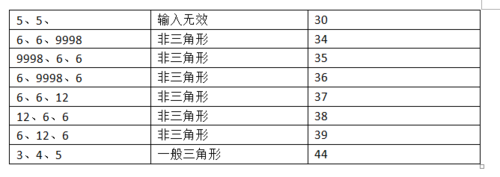
新增一条测试用例只覆盖一个无效类，继续新增，确保所有的无效类覆盖完全

1. ——》 覆盖有效等价类的测试用例

[](http://jingyan.baidu.com/album/2d5afd69d3c29b85a3e28e7b.html?picindex=4)

1. ——》覆盖无效类的测试用例

[](http://jingyan.baidu.com/album/2d5afd69d3c29b85a3e28e7b.html?picindex=5)

[](http://jingyan.baidu.com/album/2d5afd69d3c29b85a3e28e7b.html?picindex=6)

2、请设计出下面这个登录框的测试用例。



功能性用例设计点：

1.  输入已注册的用户名和正确的密码，验证是否成功登录

2.  输入已注册的用户名和不正确的密码，验证是否成功失败，且提示信息正确

3.  输入未注册的用户名和任意密码，验证是否登录失败，且提示信息正确

4.  使用未激活账户登录，验证是否登录失败

5.  使用被停用用户登录，验证是否登录失败

6.  用户名和密码两者都为空，验证是否登录失败，且提示信息正确

7.  用户名和密码两者之一为空，验证是否登录失败，并且提示信息正确

8.  如果登录功能启用了验证码功能，在用户名和密码正确的情况下，输入正确的验证码，验证是否登录成功

9.  如果登录功能启用了验证码功能，在用户名和密码正确的情况下，输入错误的验证码，验证是否登录失败，且提示信息正确

10.用户名和密码是否大小写敏感

11.页面上的密码框是否加密显示、或者是否需要有明暗码切换按钮

12.后台系统创建的用户第一次登录成功时，是否提示修改密码

13.忘记用户名和忘记密码的功能是否可用

14.前端页面是否根据设计需求限制用户名和密码长度

15.如果登录功能需要验证码，点击验证码图片或者点击换一张是否可以更换验证码，更换后的验证码是否可用

16.刷新页面是否会刷新验证码

17.如果验证码有时效性，需要分别时效性内和时效性外验证码的有效性

18.用户登录成功但是会话超时后，继续操作是否会重定向到用户登录界面

19.不同级别的用户，比如管理员和普通用户，登录系统后权限是否正确

20.页面默认焦点是否定位在用户输入框中

21.快捷键Tab和Enter等，是否可以正常使用

22.为空和输入空格字符串的校验是否一致

23.使用中文键盘输入字母和使用英文键盘输入字母传入后端的字符长度是否一致

24.成功登录后的session的时效设置

25.输入栏是否设置快速删除按钮

26.用户名和密码是否支持特殊字符和中文

27.浏览器的前进后退按钮，是否有效

28.成功登出后，点击浏览器回退按钮，是否可以继续操作系统

29.需求中是否有登录时间限制，如果有验证时间限制是否有效

30.验证不同登录方式的正确性：扫码、账号密码、第三方……

31.若支持手机号+验证码登录，验证码是否有时间限制，移动设备是否可以直接获取验证码

32.操作错误提示信息是否简单明了

兼容性测试用例设计点：

1.  不同浏览器下，验证登录页面的显示以及功能正确性

2.  相同浏览器的不同版本下验证登录页面的显示以及功能正确性

3.  不同移动设备终端的不同浏览器下，验证登录页面显示以及功能的正确性

4.  不同分辨率的界面下，验证登录页面的显示以及功能正确性

安全性测试用例设计点：

1.  用户密码后台存储是否加密

2.  用户密码在网络传输过程中是否加密

3.  密码是否具有有效期，密码有效期到期后，是否提示需要修改密码

4.  不登录的情况下，在浏览器中直接输入登录后的URL地址,验证是否会重新定向到用户登录界面

5.  密码输入框是否不支持复制粘贴

6.  密码输入框内输入的密码是否都可以在页面源码模式下被查看

7.  用户名和密码输入框分别输入典型的“SQL注入攻击”字符串，验证系统的返回页面

8.  用户名和密码输入框分别输入典型的“XSS跨站脚本攻击”字符串，验证系统行为是否被篡改

9.  连续多次登录失败的情况下，系统是否会阻止后续的尝试以应对暴力破解

10.同一用户在同一终端的多种浏览器上登录，验证登录功能的互斥性是否符合设计预期

11.同一用户先后在多台终端的浏览器上登录，验证登录是否具有互斥性

12.是否可以记住密码，记住的密码保存是否加密，记住的密码是否有有效期，过了有效期后是否清空密码

13.是否支持第三方登录

14.密码的强弱性，复杂度校验

15.异地登录校验、更换设备登录校验、登陆信息异常是否考虑账户冻结停用、是否允许第三方平台存储密码

16.是否可以使用登录的api发送登录请求，并绕开验证码校验

17.是否可以用抓包工具抓到的请求包直接登录

18.截取到的token等信息，是否可以在其他终端上直接使用，绕开登录，token过期时间校验

19.登录错误后的提示是否存在安全隐患

注：这里还有自动登录的用例需要补充

3、有一个输入框只能输入0~100的整数，请设计测试该输入框的测试用例。

一、共性

默认值（仅在输入框第一次出现时）

1.1 输入框有默认值：输入框信息为默认值。

1.2 输入框无默认值：输入框为空。

预期值（仅在输入框为空时）

2.1 输入框有预期值：输入框显示预期值，焦点在输入框/输入框输入信息时，预期值消失。

2.2 输入框无预期值：输入框不显示内容。

必填项

3.1 输入框是必填项：输入框为空，消息提醒且无法提交当前页面。

3.2 输入框非必填项：输入框为空，可以提交当前页面。

唯一性

4.1 输入框字段唯一：输入该字段已存在的值，消息提醒且无法提交当前页面。

4.2 输入框字段不唯一：输入该字段已存在的值，可以提交当前页面。

读写性

5.1 输入框为只读：输入框无法输入信息。

5.2 输入框为读写：输入框可以输入信息。

特殊键

6.1 Tab键：焦点在输入框时，点击Tab键，是否在输入框间切换。

6.2 Enter键：焦点在输入框时，点击Enter键，是否提交当前页面。

空格和制表符

7.1 输入框中是否会自动去掉空格和制表符，不自动去掉时空格和制表符是否会对输入框产生影响。

数值类型

1.1 数字：数字框中输入数字信息（如：123），输入数值不变，可以提交当前页面。

1.2 非数字：数字框中输入非数字信息（如：测试数字框TestNumber-0123.4560αβγさしすⅠⅡⅢ＋－×÷），消息提醒且无法提交当前页面。

数值大小

2.1 数值大小有限制：数字框中输入超过数值大小范围的数字，消息提醒且无法提交当前页面；或数字框中无法输入超过数值大小范围的数字。

2.2 数值大小无限制：数字框中输入足够大的数字（如999999999999999），输入数值不变，可以提交当前页面。

数值正负

3.1 允许负值：数字框中输入负数（如：-123），输入数值不变，可以提交当前页面。

3.2 不允许负值：数字框中输入负数（如：-123），消息提醒且无法提交当前页面。

小数数值

4.1 允许小数：数字框中输入小数（如：1.23），输入数值不变，可以提交当前页面。

4.2 允许小数（保留位数）：按照其规则，依次在数字框中输入小数（如：规定保留3位小数，依次在数字框中输入1.23456，1.2），输入数值按照规则改变（如：1.23456变为1.234，1.2变为1.200），可以提交当前页面。

4.3 不允许小数：数字框中输入小数（如：1.23），消息提醒且无法提交当前页面。

自动去0

5.1 有自动去0：数字框中输入首位含0的数值（如0，01，000123），输入数值自动去0（如：0变为空，01变为1，000123变为123），可以提交当前页面。

5.2 无自动去0：数字框中输入首位含0的数值（如0，01，000123），输入数值保留0不变（如0变为0，01变为01，000123变为000123），可以提交当前页面。

4、请列举下你玩过的游戏清单，并简要说明下你对每个游戏的体会。如果是网游，请说明下你在这个游戏中职业、等级等基本信息（如有人民币付出，请务必说明数额）。

5、我们创业公司996的上班时间，公司会提供业内相对好的项目奖金机制，基于以上内容，请您提出自己要求的相应待遇？