功能测试：

测试用例表：

系统模块	功能点	用例编号	前置条件	测试内容	预期结果	测试结果	失败原因
1 输入框	2.1 字符型输入框	1.1.1	页面成功加载	英文全角、英文半角、数字、空或者空格、特殊字符“~！@#￥%……&*？[]{}”特别要注意单引号和&符号。禁止直接输入特殊字符时，使用“粘贴、拷贝”功能尝试输入。	不允许有非法字符存在	符合	
		1.1.2	页面成功加载	长度检查，小于最小长度、超过最大长度	输入失败	符合	
		1.1.3	页面成功加载	输入的字符间有空格、字符前有空格、字符后有空格、字符前后有空格	不允许有空格存在	符合	
		1.1.4	页面成功加载	多行文本输入，允许回车换行	不允许多行文本输入	符合	
	1.2 信息重复	1.2.1	页面成功加载	在一些需要命名,且名字应该唯一的信息输入重复的名字或ID,看系统有没有处理,会否报错,重名包括是否区分大小写,以及在输入内容的前后输入空格,系统是否作出正确处理	用户名无法重复	符合	
2 注册登录模块	2.1 注册	2.1.1	用户名密码均已输入	点击注册按钮	应该跳转到登录界面	符合	
	2.2 登录	2.2.1	用户已注册	输入正确的用户名和正确的密码	以登录状态跳转到首页	符合	
		2.2.2	用户已注册	输入正确的用户名和错误的密码	登陆失败	符合	
		2.2.3	用户已注册	输入错误的用户名和正确的密码	登陆失败	符合	
		2.2.4	用户已注册	输入错误的用户名和错误的密码	登陆失败	符合	
		2.2.5	用户已注册	不输入用户名和密码（均为空格）	登陆失败	符合	
		2.2.6	用户已注册	只输入用户名，密码为空	登陆失败	符合	
		2.2.7	用户已注册	用户名为空，只输入密码	登陆失败	符合	
		2.2.8	用户已注册	输入正确的用户名和密码，但是不区分大小写	登陆失败	符合	
		2.2.9	无	用户名和密码包括特殊字符	登陆失败	符合	
		2.2.10	无	用户名和密码输入超长值	登陆失败	符合	
		2.2.11	用户已删除	已删除的用户名和密码	登陆失败	符合	

系统模块	功能点	用例编号	前置条件	测试内容	预期结果	测试结果	失败原因
3 留言与点赞模块	3.1 留言	3.1.1	以登录状态跳转到首页	编辑留言内容后点击提交	提交成功，留言出现在主页	符合	
		3.1.2	以登录状态跳转到首页	长度检查，超过最大长度	提交失败	符合	
		3.1.3	留言出现在主页上	点击删除按钮	留言从主页移除	符合	
	3.2 点赞	3.1.1	留言出现在主页上	点击点赞按钮	点赞成功	符合	
		3.1.2	留言已经被赞过	该用户继续点击点赞按钮	取消点赞	符合	
4 个人主页模块	4.1 个人主页	4.1.1	用户发布过留言	点击该用户用户名	跳转到个人主页	符合	
		4.1.2	进入个人主页	返回主页	返回成功	不符合	没有返回主页的链接

性能测试：

1 连接速度测试

用户连接到 Web 应用系统的速度根据上网方式的变化而变化，他们或许是电话拨号，或是宽带上网。当下载一个程序时，用户可以等较长的时间，但如果仅仅访问一个页面就不会这样。如果 Web 系统响应时间太长(例如超过 5 秒),用户就会因没有耐心等待而离开。

另外，有些页面有超时的限制，如果响应速度太慢，用户可能还没来得及浏览内容，就需要重新登陆了。而且，连接速度太慢，还可能引起数据丢失，使用户得不到真实的页面。

西电新鲜事，由于体量较小并不存在连接速度太慢的问题。

2 负载测试

负载测试是为了测量 Web 系统在某一负载级别上的性能，以保证 Web 系统在需求范围内能正常工作。负载级别可以是某个时刻同时访问 Web 系统的用户数量，也可以是在线数据处理的数量。例如：Web 应用系统能允许多少个用户同时在线？如果超过了这个数量，会出现什么现象？Web 应用系统能否处理大量用户对同一个页面的请求？

西电新鲜事，由于体量较小，就 Tomcat 的访问量来讲，250 人的同时访问时应用运行状态正常，但是如果超过 600 人同时访问 Tomcat 则会崩溃。

3 压力测试

负载测试应该安排在 Web 系统发布以后，在实际的网络环境中进行测试。因为一个企业内部员工，特别是项目组人员总是有限的，而一个 Web 系统能同时处理的请求数量将远远超出这个限度，所以，只有放在 Internet 上，接受负载测试，其结果才是正确可信的。

进行压力测试是指实际破坏一个 Web 应用系统，测试系统的反映。压力测试是测试系统的限制和故障恢复能力，也就是测试 Web 应用系统会不会崩溃，在什么情况下会崩溃。黑客常常提供错误的数据负载，直到 Web 应用系统崩溃，接着当系统重新启动时获得存取权。压力测试的区域包括表单、登陆和其他信息传输页面等。

西电新鲜事由于体量较小，不考虑故障恢复问题，保证访问量不超过 600 即可。

安全性测试：

（1）SQL 注入（比如登陆页面）

（2）XSS 跨网站脚本攻击：程序或数据库没有对一些特殊字符进行过滤或处理，导致用户所输入的一些破坏性的脚本语句能够直接写进数据库中，浏览器会直接执行这些脚本语句，破坏网站的正常显示，或网站用户的信息被盗,构造脚本语句时，要保证脚本的完整性。

document.write("abc")

<script>alter("abc")</script>

（3）URL 地址后面随便输入一些符号，并尽量是动态参数靠后

（4）验证码更新问题

（5）现在的 Web 应用系统基本采用先注册，后登陆的方式。因此，必须测试有效和无效的用户名和密码，要注意到是否大小写敏感，可以试多少次的限制，是否可以不登陆而直接浏览某个页面等。

（6）Web 应用系统是否有超时的限制，也就是说，用户登陆后在一定时间内（例如 15 分钟）没有点击任何页面，是否需要重新登陆才能正常使用。

（7）为了保证 Web 应用系统的安全性，日志文件是至关重要的。需要测试相关信息是否写进了日志文件、是否可追踪。

（8）当使用了安全套接字时，还要测试加密是否正确，检查信息的完整性。

（9）服务器端的脚本常常构成安全漏洞，这些漏洞又常常被黑客利用。所以，还要测试没有经过授权，就不能在服务器端放置和编辑脚本的问题。

（10）考虑到西电新鲜事性质，安全性不做过多考虑。只需要达到普通水平即可。

webUI 测试：

1、风格、样式、颜色是否协调

是

2、界面布局是否整齐、协调（保证全部显示出来的，尽量不要使用滚动条

是

3、界面操作、标题描述是否恰当（描述有歧义、注意是否有错别字）

是

4、操作是否符合人们的常规习惯（有没有把相似的功能的控件放在一起，方便操作）

是

5、提示界面是否符合规范（不应该显示英文的 cancel、ok，应该显示中文的确定等）

是

6、界面中各个控件是否对齐

是

7、日期控件是否可编辑

无

8、日期控件的长度是否合理，以修改时可以把时间全部显示出来为准

无

9、查询结果列表列宽是否合理、标签描述是否合理

无

10、查询结果列表太宽没有横向滚动提示

无

11、对于信息比较长的文本，文本框有没有提供自动竖直滚动条

无

12、数据录入控件是否方便

是

13、有没有支持 Tab 键，键的顺序要有条理，不乱跳

支持

14、有没有提供相关的热键

无

15、控件的提示语描述是否正确

是

16、模块调用是否统一，相同的模块是否调用同一个界面

是

17、用滚动条移动页面时，页面的控件是否显示正常

无

18、日期的正确格式应该是 XXXX-XX-XX 或 XXXX-XX-XX XX:XX:XX

无

19、页面是否有多余按钮或标签

无

20、窗口标题或图标是否与菜单栏的统一

是

21、窗口的最大化、最小化是否能正确切换

是

22、对于正常的功能，用户可以不必阅读用户手册就能使用

是

23、执行风险操作时，有确认、删除等提示吗

无

24、操作顺序是否合理

是

25、正确性检查 :检查页面上的 form, button, table, header, footer, 提示信息，还有其他文字拼写，句子的语法等是否正确。

是

26、系统应该在用户执行错误的操作之前提出警告，提示信息.

无

27、页面分辨率检查，在各种分辨率浏览系统检查系统界面友好性。

兼容

28、合理性检查：做 delete, update, add, cancel, back 等操作后，查看信息回到的页面是否合理。

合理

29、检查本地化是否通过 :英文版不应该有中文信息 ,英文翻译准确，专业。

无英文版