功能测试：

1. 注册：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 输入条件 | 有效等价类 | 有效数据 | 无效等价类 | 无效数据 |
| 用户名 | 字符串 | A,.s | 空 |  |
| 空格 |  |
| 用户密码 | 字符串 | 1234 | 空 |  |
| 空格 |  |
| 联系电话 | 11位数字串 | 13611111111 | 0-10位数字 | 00000 |
| 超过11位数字 | 136111111112 |
| 字母 | Aaaa |
| 半角字符 | A%% |
| 全角字符 | 1 2 3 4 |
| 空 |  |
| 空格 |  |
| OICQ | 字母串 | aa | 空 |  |
| 数字串 | 123 | 半角字符 | %% |
| 字母+数字 | 123aa | 全角字符 | 1 2 3 |
| 空格 |  |
| E-mail | 字母和数字组合+’@’+字母和数字组合+’.’+字母和数字组合 | Abc@aa.com | 不含‘@’和’.’的字母数字串 | Abcecm |
| 不含’.’或‘@’的字符串 | abc@aa |
| ‘@’或‘.’在结尾的字符串 | abc@. |
| ‘@’在‘.’之后的字符串 | Abc.an@cm |
| 半角字符 | a%%@a.com |
| 空 |  |
| 来自 | 字符串 | 西安 | 空 |  |
| 空格 |  |

测试用例：

1. 输入已注册过的用户名输入对应的密码进行注册；
2. 不输入用户名和密码进行注册；
3. 用户名输入空格，正确格式的密码点击注册；
4. 用户名和密码都为空格点击注册；
5. 输入正确格式的用户名和不输入密码点击注册；
6. 正确格式的用户名，密码输入空格点击注册；
7. 密码正确，不输入确认密码点击注册；
8. 不输入联系电话点击注册；
9. 输入0-10位数字联系电话点击注册；
10. 输入超过11位数字联系电话点击注册；
11. 联系电话输入字母点击注册；
12. 联系电话输入半角符号点击注册；
13. 联系电话输入全角字符点击注册；
14. 联系电话输入空格点击注册；
15. 不输入OICQ点击注册；
16. OICQ输入半角字符点击注册；
17. OICQ输入全角字符点击注册；
18. OICQ输入空格点击注册；
19. 不输入E-mail点击注册；
20. E-mail输入不含‘@’和’.’的字符串点击注册；
21. E-mail输入不含’.’或‘@’的字符串点击注册；
22. E-mail输入‘@’或‘.’在结尾的字符串点击注册；
23. E-mail输入‘@’在‘.’之后的字符串点击注册；
24. E-mail半角字符点击注册；
25. 不输入来自城市点击注册；
26. 来自城市输入空格点击注册；

测试结果：





















1. 登录：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 输入条件 | 有效等价类 | 有效数据 | 无效等价类 | 无效数据 |
| 用户名 | 正确的用户名 | koko | 空 |  |
| 不存在的用户名 | Abcd |
| 用户密码 | 正确的密码 | 1234 | 空 |  |
| 错误密码 | 123 |

1. 功能测试用例：
2. 不输入用户名和密码点击登录；
3. 输入不存在的用户名点击登录；
4. 输入正确的用户名，不输入密码点击登录；
5. 输入正确的用户名和错误的密码点击登录；
6. 安全测试用例：

1）输入错误网页刷新后密码是否保留；

1. 发帖

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 输入条件 | 有效等价类 | 有效数据 | 无效等价类 | 无效数据 |
| 帖子标题 | 字符串 | Aa | 空 |  |
| 空格 |  |
| 帖子内容 | 字符串 | Aa | 空 |  |
| 空格 |  |

1. 不输入帖子标题和帖子内容点击发布帖子；
2. 输入帖子标题，不输入帖子内容点击发布帖子；
3. 不输入帖子标题，输入帖子内容点击发布帖子；
4. 帖子标题输入空格，输入帖子内容点击发布帖子；
5. 输入帖子标题，帖子内容输入空格点击发布帖子；

测试结果：







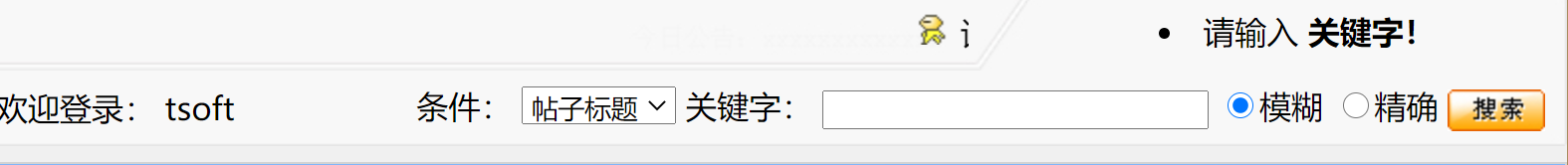
1. 搜索

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 输入条件 | 有效等价类 | 有效数据 | 无效等价类 | 无效数据 |
| 关键字 | 字符串 | Aa | 空 |  |
| 空格 |  |

测试用例：

1. 不输入关键字点击搜索；
2. 输入空格点击搜索；

测试结果：



1. 回复：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 输入条件 | 有效等价类 | 有效数据 | 无效等价类 | 无效数据 |
| 回复标题 | 字符串 | Aa | 空 |  |
| 空格 |  |
| 回复内容 | 字符串 | Aa | 空 |  |
| 空格 |  |

测试用例：

1. 不输入帖子标题和帖子内容点击回复帖子；
2. 输入帖子标题，不输入帖子内容点击回复帖子；
3. 不输入帖子标题，输入帖子内容点击回复帖子；
4. 帖子标题输入空格，输入帖子内容点击回复帖子；
5. 输入帖子标题，帖子内容输入空格点击回复帖子；

测试结果：







性能测试：

使用工具LoadRunner

能力测试：（最大吞吐率）

策略：使用LoadRunner工具添加虚拟用户登录，找到系统运行性能达标的最大用户数。

指标：系统响应时间<1s

压力测试：

策略：使用LoadRunner工具添加虚拟用户登录，找到系统崩溃时的用户数。

指标：系统运行状态

可用性测试：

填写下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **问题** | **答案** | | |
| **Yes** | **No** | **N/A** |
| 浏览 | 1．对浏览者所处网页有清晰的标记？ |  |  |  |
| 2．有清楚指向主页的链接？ |  |  |  |
| 3．网站各主要部分都可以由主页进入？ |  |  |  |
| 4．有网站索引，已备需要？ |  |  |  |
| 5．网站架构简单，没有不必要的分级？ |  |  |  |
| 6．有易用的搜索功能，已备需要？ |  |  |  |
|  | | | | |
| 功能 | 1．所有功能都有清晰的标签？ |  |  |  |
| 2．不需要离开网站，即可运用各必需的功能？ |  |  |  |
| 3．没有使用不必要的外挂工具？ |  |  |  |
|  | | | | |
| 控制 | 1．用户可将所操作程序取消？ |  |  |  |
| 2．每一页都有一个清晰的出口？ |  |  |  |
| 3．每个图形链接都有相应的文字链接？ |  |  |  |
| 4．网站可配合用户的应用流程？ |  |  |  |
| 5．支持所有常用的浏览器？ |  |  |  |
|  | | | | |
| 响应 | 1．网站内所发生的事情都很清楚? |  |  |  |
| 2．需要时，用户可以得到Email回复？ |  |  |  |
| 3．很快便可以得到响应？ |  |  |  |
| 4．需要外挂程序或特定浏览器版本时，用户会得到相应指示？ |  |  |  |
| 5．用户可依据Email或表单提供意见? |  |  |  |
| 6．有在线帮助信息，已备需要？ |  |  |  |
|  | | | | |
| 避免及更正错误 | 1．避免不必要的错误？ |  |  |  |
| 2．错误信息以普通文字形式出现？ |  |  |  |
| 3．错误信息出现的同时，有描述所需的相应动作？ |  |  |  |
| 4．错误信息中有清晰的出口？ |  |  |  |
| 5．错误信息上附有支持服务联络人的详细资料？ |  |  |  |
|  | | | | |
| 视觉清晰度 | 1．编排清楚？ |  |  |  |
|  | 2．有足够的空白地方？ |  |  |  |
|  | 3．所有图像都加上“ALT”标记？ |  |  |  |
|  | 4．避免出现不必要的动画？ |  |  |  |

安全性测试：

1）身份验证：测试有效和无效的用户名和密码

2）web系统超时限制。

3）错误处理：相关信息是否写进了日志文件、是否可追踪。

4）上传文件：

1.上传文件是否有格式限制,是否可以上传exe文件；

2.上传文件是否有大小限制,上传太大的文件是否导致异常错误,上传0K的文件是否会导致异常错误,上传并不存在的文件是否会导致异常错误；

3.通过修改扩展名的方式是否可以绕过格式限制，是否可以通过压包方式绕过格式限制；

4.是否有上传空间的限制,是否可以超过空间所限制的大小,如将超过空间的大文件拆分上传是否会出现异常错误。

5.上传文件大小大于本地剩余空间大小，是否会出现异常错误。

6.关于上传是否成功的判断。上传过程中，中断。程序是否判断上传是否成功。

7.对于文件名中带有中文字符，特殊字符等的文件上传。

5）下载文件

6）URL：

1.某些需登录后或特殊用户才能进入的页面,是否可以通过直接输入网址的方式进入；

2.对于带参数的网址,恶意修改其参数,(若为数字,则输入字母,或很大的数字,或输入特殊字符等)后打开网址是否出错,是否可以非法进入某些页面；

3.搜索页面等url中含有关键字的,输入html代码或JavaScript看是否在页面中显示或执行。

4.输入善意字符。

7）数据库安全：防止SQL注入