# 1        概述

为了能使测试人员有效的设计测试用例，对所有需要测试的产品进行全面的测试，以尽最大可能发现最隐蔽的问题，当前的测试设计以此文档作为参考标准。

# 2        测试范围

## 2.1      产品安装测试

（1）安装主画面上的软件名称及版本信息是否正确

（2）更改安装程序提供的缺省安装进行安装，程序是否能正确运行

（3）记录用户姓名及组织机构名称操作是否正确

（4）程序安装结束语是否正确

（5）程序组的建立是否正确

（6）程序项的建立是否正确

（7）在所有能中途退出安装的位置是否能正确退出安装程序。

（8）异常情况时是否会提示磁盘空间不足、缺少目录创建权限

（9）软件安装 后是否能够立即运行

（10）是否有帮助文档、操作手册、ReadMe等

## 2.2      产品功能测试

功能测试，是根据产品特征、操作描述和用户方案，测试一个产品的特性和可操作行为以确定它们满足设计需求。

### 2.2.1      链接测试

链接是Web应用系统的一个主要特征，它是在页面之间切换和指导用户去一些不知道地址的页面的主要手段。<可用测试工具Xenu来执行>

（1）测试所有链接是否按指示的那样确实链接到了该链接的页面

（2）测试所链接的页面是否存在

（3）保证Web应用系统上没有孤立的页面，所谓孤立页面是指没有链接指向该页面，只有知道正确的URL地址才能访问

### 2.2.2      表单测试

通常在web应用系统中，前台与后台的数据信息交互都是通过表单来完成，所以表单是web应用中的主要功能测试点。

1、表单新增功能测试

（1）文本为空

（2）空格文本

（3）输入特殊字符或符号

（4）输入数字

（5）输入超出文本长途的字符

（6）输入汉字

（7）输入汉字、字母和数字混合

（8）输入用户名如：ad，min

（9）是否有提交成功提示信息

（10）是否有提交失败的详细信息

（11）根据具体的输入规则设计测试，如密码的格式、mail的格式、电话号码的格式和出生年月的格式等

（12）验证信息是否提交到数据库中，查看数据库信息

2、表单删除功能测试

（1）是否证实数据信息被删除，对应到数据中查看

（2）对删除的动作是否逻辑提示

（3）删除成功，是否有提示

（4）删除失败，是否有提示

3、表单查询功能测试

（1）文本为空

（2）空格文本

（3）查询失败，是否有提示

（4）精确查询

（5）模糊查询

（6）组合查询

4、表单修改功能测试

（1）是否可以修改主键，如：ID、用户名等

（2）修改后的信息是否确认保存到数据库中，查看数据库

注：其他项跟新增测试用例一致

5、表单登录功能测试

（1）文本为空

（2）空格文本

（3）输入长度超过文本框

（4）输入长度为1位

（5）输入用户名、密码相同

（6）将用户名和密码颠倒输入

（7）是否有相关提示信息

（8）是否有取消登录功能

## 2.3      产品集成测试

集成测试，也叫组装测试或联合测试。在单元测试的基础上，将所有模块按照设计要求组装成为子系统或系统，进行集成测试。实践表明，一些模块虽然能够单独地工作，但并不能保证连接起来也能正常的工作。程序在某些局部反映不出来的问题，在全局上很可能暴露出来，影响功能的实现。

集成测试应该考虑以下几点：

（1）在把各个模块连接起来的时候，穿越模块接口的数据是否会丢失

（2）各个子功能组合起来，能否达到预期要求的父功能

（3）一个模块的功能是否会对另一个模块的功能产生不利的影响

（4）全局数据结构是否有问题

（5）单个模块的误差积累起来，是否会放大，从而达到不可接受的程度

## 2.4      产品界面测试

### 2.4.1      导航栏

（1）导航是否直观

（2）系统的主要部分是否可通过主页到达

（3）系统是否有站点地图、搜索引擎或其它的导航帮助

（4）系统是否有搜索引擎或其它的导航帮助

（5）用户是否能在3次导航之后到达目的地

### 2.4.2      窗口

（1）窗口在屏幕上的显示位置是否正确、美观

（2）窗口标题是否正确

（3）窗口中各对象位置是否正确、美观

（4）窗口的系统菜单及按钮操作是否正常

（5）窗口在各种不同分辨率下是否能全部显示

<1024x768 | 800x600 | 600x400 | 1280x1024>

（6）通过在点击浏览器上的后退和前进按钮来观察窗口的状态

### 2.4.3      菜单

（1）菜单是否显示正确

（2）菜单项文字意义是否明确

（3）主菜单条上各项是否均有快捷方式

（4）主菜单条上各项的快捷方式是否有效

（5）下拉式菜单中各菜单项显示是否正确

（6）下拉式菜单中各菜单项文字意义是否明确

（7）有快捷方式的下拉式菜单项的快捷方式是否有效

### 2.4.4      工具条

（1）工具条显示的位置是否正确

（2）工具条中各项必须均有浮动说明

（3）工具条中各按钮必须有按下和抬起两种状态

（4）可移动工具条在窗口边际位置其形状及位置的相应变化是否正确

（5）工具条中开关按钮、按钮组及List Box对象必须有缺省值

### 2.4.5      状态条

（1）状态条显示位置是否正确、美观

（2）状态条内状态信息显示是否根据操作而变化

（3）状态条内状态信息是否正确

（4）状态条内状态信息文字是否正确、意义是否明确

### 2.4.6      对话框

（1）对话框弹出时机及位置是否正确

（2）对话框内各对象位置是否正确

（3）对话框内各对象的文字标题意义是否明确

（4）模式对话框和非模式对话框的属性是否正确

### 2.4.7      消息框

（1）弹出时机及位置是否正确

（2）信息意义是否正确、意义是否明确

（3）弹出时必须锁住Mouse消息和键盘输入

（4）必须有正确的对象用于退出Message Box

### 2.4.8      列表框

（1）列表框显示及位置必须正确、美观

（2）列表框应有缺省值

（3）列表框内可选内容必须全面

### 2.4.9      单选复选按钮

（1）显示位置要正确

（2）文字意义要明确

（3）单选复选按钮的默认值是否正确

（4）单选按钮的组成关系要正确且选择必须互斥

（5）复选按钮是否支持复选功能

（6）单选复选按钮是否正确触发了事件

### 2.4.10 文字Label

（1）显示位置要美观

（2）文字意义要明确

（3）同一界面上字体及字体大小应统一、美观

### 2.4.11 文字或图像Button

（1）显示位置要美观

（2）Button上的文字意义要明确

（3）同一界面上字体及字体大小应统一、美观

（4）相应的文字说明或意义明确

（5）应有按下和抬起两种状态

（6）检查在未选择项目情况下点击后的警告信息

（7）检查在执行按钮操作后的页面显示状态

（8）新增 更新按钮与删除按钮应保持一定距离,避免用户误操作

（9）是否可以通过TAB键进行按钮的之间切换

（10）按钮是否响应Enter键

### 2.4.12 文本输入域

1、字符输入域

（1）输入为空

（2）输入为空格字符

（3）任意字符串<中英文>

（4）功能键或者符号键

（5）超越字符串的处理

（6）检查焦点是否在第一个可输入域

（7）检查TAB键的次序

2、时间输入域

（1）    输入字符串

（2）    输入字符?和/等特殊字符

（3）    输入数字字符

（2）各种时间表示格式的输入(美国方式及中国方式等)

3、整型数字输入域

（1）输入字符串

（2）输入浮点数

（3）超界值处理

（4）输入正负和零值

（5）输入特殊字符加数字

（6）输入字母加数字

（7）输入ASCII值

（8）输入重复值

（5）输入空值

4、浮点型数字输入域

（1）整型数字输入域中的测试用例

（2）超长浮点数输入

### 2.4.13 显示域

（1）显示域中各对象显示位置正确、美观

（2）显示域中文字Label信息正确

（3）显示域中文字Label字体及字体大小应统一且美观

（4）显示域中显示信息应与输入的信息一致

（5）在屏幕显示不下时，是否增加滚动条以确保信息显示的完整

## 2.5      产品兼容性测试

### 2.5.1      操作系统

（1）Windows 2003

（2）Windows xp

（3）Windows 7

（4）Windows Vista

### 2.5.2      浏览器

（1）IE5.0

（2）IE6.0

（3）IE7.0

（4）IE8.0

（5）火狐浏览器

## 2.6      产品安全性测试

### 2.6.1      目录测试

Web 安全的第一步就是正确设置目录。每个目录下应该有 index.html 或 main.html 页面，这样就不会显示该目录下的所有内容。

### 2.6.2      SSL测试

很多站点使用 SSL 进行安全传送。你知道你进入一个 SSL 站点是因为浏览器出现了警告消息，而且在地址栏中的 HTTP 变成 HTTPS。如果开发部门使用了SSL，测试人员需要确定是否有相应的替代页面(适用于3.0 以下版本的浏览器，这些浏览器不支持SSL。当用户进入或离开安全站点的时候，请确认有相应的提示信息。是否有连接时间限制？超过限制时间后出现什么情况？

### 2.6.3      登录测试

有些站点需要用户进行登录，以验证他们的身份。这样对用户是方便的，他们不需要每次都输入个人资料。你需要验证系统阻止非法的用户名/口令登录，而能够通过有效登录。用户登录是否有次数限制? 是否限制从某些 IP 地址登录? 如果允许登录失败的次数为3，你在第三次登录的时候输入正确的用户名和口令，能通过验证吗? 口令选择有规则限制吗? 是否可以不登陆而直接浏览某个页面？

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。

### 2.6.4      日志文件测试

在后台，要注意验证服务器日志工作正常。日志是否记所有的事务处理? 是否记录失败的注册企图?是否在每次事务完成的时候都进行保存并记录IP 地址和用户名等信息?

### 2.6.5      脚本语言测试

脚本语言是常见的安全隐患。每种语言的细节有所不同。有些脚本允许访问根目录。其他只允许访问邮件服务器，但是经验丰富的黑客可以将服务器用户名和口令发送给他们自己。找出站点使用了哪些脚本语言，并研究该语言的缺陷。还要需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。