

# Web 应用测试

## Web 应用测试

Web 应用测试的目标是对系统的质量维度进行检查，找出其中隐藏的错误或缺陷，主要针对 Web 应用的内容、功能、结构、可用性、导航性、性能、兼容性、互操作性和安全属性，进行的主要步骤是单元测试，功能测试，性能测试，安全性测试，WebUI 测试。

### 一. 单元测试

单元测试即是评测内容的语法和语义错误、评审内容的许可性、测试接口机制的正确操作、测试组件确保正确的功能。

我们利用 NUnit 对系统进行了单元测试，通过将 NUnit 引用到项目中再进行测试，通过一步一步的来进行测试：第一步，应该对所有程序集中的公开类以及公开类里面的公开方法添加单元测试；第二步，对于构造函数和公共属性进行单元测试；第三步，添加全面单元测试。

通过不断的测试，修改了一部分代码段中的 BUG 并且及时修正了代码，使程序变得更加健壮。

### 二. 功能测试

功能测试分为链接测试，交互测试，数据校验，cookies 测试，数据库测试，特定功能需求测试。

1. 链接测试：（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。经测试，我们的系统不存在孤立的页面。
2. 交互测试：（1）对表单元素中的标识域给出正确标记，并且为用户显示的标识出强制域；（2）对每一项用户输入进行正确性和合法性检查；（3）对用户输入错误时的异常处理机制进行检查；（4）当用户没有从下拉菜单或按钮组中进行选择时使用合适的默认下；（5）浏览器后退等功能没有破坏输入的表单中的数据。我们对系统进行了交互测试，如购买商品，发出求购信息等，然后查看各个模块是否功能正常，再根据事件的优先级查看这几个时间的工

作顺序，发现该系统的事件处理上有一定的不足，经过我们对其不断地修改，最终能够较好地进行交互。

3. cookies 测试:cookies 是突然通常用来存储用户信息和用户在 web 应用的操作。当一个用户使用 cookies 访问了某一个 web 应用时,web 服务器将发送关于这一用户的信息并把该信息的形式存储在客户端计算机上，测试的内容包括 cookie 是否起作用。是否按预定的时间进行保存刷新了页面的 cookie 是否有影响以及有什么影响等等。如果在 cookie 中保存注册信息请确认该 cookie 能够正常工作，而且对这些信息加密。如果使用 cookie 来统计次数需要验证次数累积正确。经过对系统的 cookies 测试，发现系统 cookies 性能良好。
4. 数据库测试：数据库采用 MySQL 关系型数据库，我们测试了数据一致性错误及输出错误两方面，数据一致性错误主要是用户提交的表单信息不正确导致的，输出错误主要是网络错误或程序设计问题引起的，针对这种情况，经测试发现，本系统涉及到的用户即买卖双方提交的表单信息不正确时会发生数据不一致。在输出方面，程序设计中每个变量都有自己的类型，如果用户输入的类型不符合，或者由高精度值转向低精度值数据输出会出现异常。
5. 特定功能需求测试：本系统的特定功能即用户能够互相发布求购、购买信息并且买卖商品，经过对系统的测试，发现本系统达到了该需求的一切功能，能够完美实现所要求。

### 三. 性能测试

目的是为了评估系统的性能，确定系统的瓶颈，系统调优和检测 Web 应用中潜在的问题。内容是速度测试，负载测试，压力测试，并发测试，大数据测试，配置测试，可访问性，可靠性测试。

使用了 jmeter 进行性能测试，通过产生 Web 请求来测试系统的性能，一个 web 请求的处理包括以下步骤：1、客户发送请求；2、web server 接受到请求,进行处理;3、web server 向 DB 获取数据；4、web server 生成用户请求的页面，返回给用户。从客户发送请求开始到客户接收到最后一个字节的时间成为响应时间。进行速度、压力及负载测试，如瞬间达到访问压力高峰或每个用户传送大量数据或是长时间的使用时，系统的响应时间等指标。但测试结果并不尽如人意，

表示系统的速度、负载以及压力承担能力不强。

并发测试：并发数是指同时进行请求的客户数量，并发数用于模拟用户的真实负载情况。本系统的并发能力可行，有处理适量并发事件的能力。

大数据测试：无。

配置测试：能够适应大部分操作系统及浏览器，系统的配置设置的较为完善。

可访问性及可靠性测试：其进行测试，在系统上进行各种操作，记录实时数据以及期望结果及实际结果是否与期望结果一致并分析其原因，最终结果为，系统大部分操作的实际结果与期望结果一致。

#### 四. 安全性测试

对系统进行数据加密测试，用户身份验证测试，日志文件测试，Session 测试，备份与恢复测试，访问控制策略测试，安全漏洞测试，TCP 端口测试，服务器脚本漏洞检查，防火墙测试。

##### 1. 对用户登录身份验证的测试

由于本二手物品交易平台登录时需要先注册后登录，且登录类型分为用户登录和管理员登录。因此我们从有效用户名和无效用户名、用户名及密码大小写、登录时输入密码错误次数、是否可以通过用户登录进入管理员界面、游客登录是否会出现与其游客权限不符的状况等方面进行测试。其结果为无效用户名无法进行登录，只有有效用户名且正确输入密码后才能进行登录；账户名和密码均对大小写敏感，大小写不同视为不同输入；用户或管理员在登录时没有输入次数的限制，直达输入正确的密码为止。用户登录和管理员登录权限不同，用户无法获得管理员相关的权限。

##### 2. 日志文件测试

日志文件记录了所有事务处理，记录用户名且每个用户、管理员的每一次有效操作都会被记录并进行保存。无效操作不会被记录，游客注册失败也不会被记录；记录 IP 地址。

##### 3. Session 测试

当使用用户名和密码登录网站，系统会首先验证当前登陆用户是否合法，当合法后将用户名等相关信息保存在 Session 中。

登陆后点击进入某功能页面时，系统也会去判断当前你是否拥有访问权限，判断的方式是验证 Session 中的内容是否正确。由于本平台未设置时间限制，所以用户在登录到退出系统的整个过程中没有超时限制，无论等待多长时间仍能进行有效操作。

#### 4. 备份与恢复测试

没有设置备份与恢复策略，因此在数据丢失后只能通过日志查看丢失原因而无法对已丢失的数据进行恢复。

#### 5. 访问控制策略测试

游客、用户、管理员拥有不同的权限，仅能够使用与其权限所对应的功能，例如游客只能进行浏览而无法进行其他操作，用户也无法进行公告栏管理等操作。测试表明本平台有完善的访问控制策略文档，其准确的定义了不同登录类型的用户可以访问的内容、使用的功能。

#### 6. 安全漏洞测试

没有设置防火墙，对 SQL 注入没有防范，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。容易遇到在未经授权状况下篡改数据库中的数据，恶意修改网页内容，私自添加管理员账户等问题。

容易受到 XSS 攻击，恶意攻击者往 Web 页面里插入恶意 html 代码，当用户浏览该页之时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意攻击用户的特殊目的。

#### 7. TCP 端口测试

通过 telnet 命令语句来对 TCP 端口进行测试，测试表明所以端口都处于联通状态

#### 8. 服务器脚本漏洞测试

通过动态的向 web 页面编辑、改变或添加，对由 HTML 表单提交的用户请求或数据进行响应，访问数据或数据库并向浏览器返回等行为，对服务器进行使用测试，结果表明服务器行为运作良好未出现漏洞。

#### 9. 防火墙测试

未设置防火墙，容错能力低、服务器兼容较差，服务器性能有限，无法同时处理大量数据，同时处理大量数据是会发生连接速度变慢、响应时间增长的问题；对多种媒体格式的支持较好，

对于不同操作系统上不同浏览器都能够很好的支持，未出现明显兼容性问题；数据完整性强。总体而言安全性能较差。

## 五. WebUI 测试

进行导航测试，图形测试，内容测试，表格测试，整体界面测试。

### 1. 导航测试

导航描述了用户在一个界面内的操作，起着链接站点或者各个页面的作用。本平台页面设计易于导航且导航十分直观，web系统的主要部分都可以通过主页存取，系统导航帮助准确无误，不需要站点地图的帮助，有搜索功能。Web 页面结构、导航、菜单、交接风格一致。

### 2. 图形测试

每个图片都有自己存在的明确用途，所有页面的字的风格、颜色、格式相同。背景颜色与字体颜色和前景颜色搭配良好，图片采用 JPG 格式，大小适中、清晰度良好。图片与文字指向对应关系正确无误。

### 3. 内容测试

商品信息正确性高，不会产生误导。信息的准确性高，无拼写错误或是语法错误，断句措辞等不会产生歧义。信息的相关性强，可以在当前页面可以找到与当前浏览信息相关的信息列表或入口。

### 4. 表格测试

商品界面表格布局、颜色、风格统一，存在筛选条件、搜索控件且位于页面上方。对应多个搜索条件的场景，未采用高级搜索按钮并将其打包起来、未配置重置按钮便于一键清空搜索条件。当字段数量过多，需要横向滚动表格，且需要对比数据时，采用固定属性列字段

### 5. 整体界面测试

整体界面风格良好，界面清晰明了具有一定的引导性，功能明确让用户知道自己的目标。通过配色、字体以及布局排版使得界面规范而不失特色。