上海交通大学致远学院官方网站

测试结果报告

版本 1.0

修订历史记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 07/06/2020 | 1.0 | Web GUI测试报告 | 林江浩 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

1. 简介 4

1.1 目的 4

1.2 范围 4

1.3 定义、首字母缩写词和缩略语 4

1.4 参考资料 4

1.5 概述 4

2. 测试过程明细 5

2.1 功能性测试 5

2.1.1 按钮 5

2.1.2 输入框 6

2.1.3 下拉框 6

2.1.4 轮播盘 7

2.1.5 PDF文件查阅 7

2.1.6 文件下载 8

2.1.7 日历组件 9

2.2 可用性测试 10

2.2.1 导航测试 10

2.2.2 图形测试 11

2.2.3 整体界面测试 11

2.3 安全性测试 11

2.3.1 登录验证测试 11

2.3.2 数据加密测试 11

2.3.3 超时限制测试 12

2.3.4 渗透测试 12

2.4 兼容性测试 12

3. 测试结果概述 13

3.1 功能性测试 13

3.2 可用性测试 13

3.2.1 导航测试 13

3.2.2 图形测试 13

3.2.3 **.** 整体界面测试 14

3.3 安全性测试 14

3.3.1 登录验证测试 14

3.3.2 数据加密测试 14

3.3.3 超时限制测试 14

3.3.4 渗透测试 15

3.4 兼容性测试 15

3.5 小结 15

4. 措施建议 16

4.1 图形测试 16

4.2 超时限制测试 16

4.3 渗透测试 16

测试结果报告

# 简介

本测试报告是针对上海交通大学致远学院官方网站的测试文档。上海交通大学致远学院官方网站于四月份完成界面重构，面向广大师生开放学院概况介绍、学生事务通知等多类教学服务。本次测试为Web GUI测试，共分为功能性测试、可用性测试、安全性测试、兼容性测试四部分进行。本次测试采用selenium python作为测试框架，用pytest的断言工具以及requests的网络请求作为辅助测试工具，使用VsCode编写和运行测试用例。

## 目的

本测试报告展示了针对上海交通大学致远学院官方网站的Web GUI测试过程明细与结果概述，在测试内容上，我们的测试涵盖了功能性测试、可用性测试、安全性测试和 兼容性测试四大部分；测试方法上，我们结合测试框架selenium中的多种元素定位方法，进行综合测试。

## 范围

本次测试分为四大部分，分别是功能性测试、可用性测试、安全性测试、兼容性测试。

1. 功能性测试

在功能性测试中，我们选取了网站中的七大主要元素：按钮、输入框、下拉框、轮播盘、PDF文件查阅、文件下载、日历组件。而数据以及Cookies测试，我们将之合并至安全性测试中。

1. 可用性测试

在可用性测试中，我们进行了导航测试、图形测试和整体界面测试。而内容测试因为涉及网站内容正确性的测试，因此在本次测试中略去。而对于导航测试和整体界面测试的内容，往往涉及到最终用户的整体感受，因此我们邀请第三方用户进行调研测试。

1. 安全性测试

在安全性测试中，我们将结合了功能性测试中的Cookies测试，进行了四项测试内容：登录验证测试、数据加密测试、超时限制测试和渗透测试。

1. 兼容性测试

在兼容性测试中，我们通过更换不同的终端设备、浏览器驱动、显示分辨率、连接速率进行测试，考查致远官网在不同环境下的兼容能力。

## 定义、首字母缩写词和缩略语

|  |  |
| --- | --- |
| 缩写词 | 含义 |
| 致远官网 | 上海交通大学致远学院官方网站，测试网站名称 |
| Web GUI测试 | 针对基于浏览器的网页网站测试 |
| Selenium | 本次测试使用python语言的测试框架 |

## 参考资料

《Software Testing - A Craftsman’s Approach》

## 概述

本次测试报告包含针对测试用例设计的说明，测试结果和覆盖率展示，以及对被测试软件改进的建议

# 测试过程明细

## 功能性测试

在功能性测试中，我们选取了网站中的七大主要元素：按钮、输入框、下拉框、轮播盘、PDF文件查阅、文件下载、日历组件。

### 按钮

按钮是致远官网最常见的元素之一，数量巨大，因此我们根据按钮的种类、功能等将按钮元素进行大致分类，并对每一个类别进行测试。同时，测试框架selenium具有多种定位html元素的方法，我们针对不同种类的按钮类，采用不同的定位方法进行测试。具体分类和测试情况如表2.1.1.1所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **按钮类别** | **种类描述** | **例图** | **定位方法** |
| 图标按钮 | 带有明确含义的图标无需其他文字说明 |  | css\_selector |
| 导航按钮 | 位于网页上部，点击后可以跳转到具有相应功能或信息的分页 |  | link\_text |
| 条目按钮 | 在“最新动态”等分页下出现，往往一个分页会批次出现 |  | class\_name |
| 页码跳转按钮 | 位于网页下部，点击后可跳转至对应页码的分页 |  | tag\_name |
| 其他按钮 | 普通的按钮，具有明确的矩形边框界限、底色、文字等要素 |  | xpath |

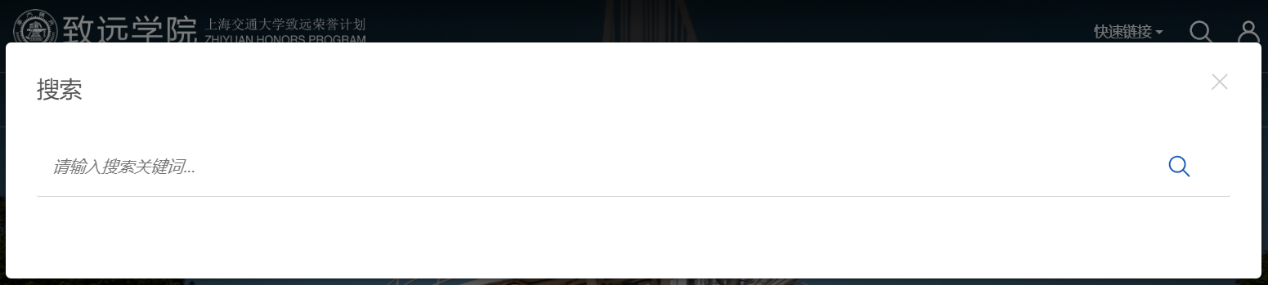
**表2.1.1.1 按钮元素的分类**

在测试检验方法上，当且仅当一个按钮可以被点击、并且能够成功跳转到对应页面，我们才认为该按钮元素通过检验。同时我们可以通过读取来获取当前页面类别信息，以用于检验跳转是否正确。

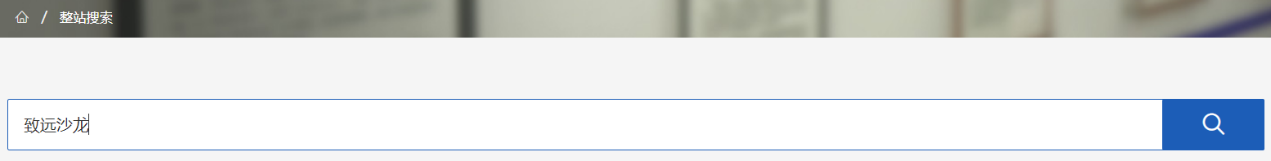


### 输入框

在致远官网内，只有两处地方用到了输入框元素，且都是用于整站搜索功能的。第一处是在网页上部点击“搜索”图标按钮后，会跳出输入框；第二处则是位于整站搜索页面。具体情况可见下图所示，同样的，我们采用了三种不同的定位方法对输入框元素进行测试。



**图2.1.2.1 第一个输入框元素**



**.图2.1.2.2 第二个输入框元素**

在检验方法上，测试代码在获取输入框焦点后，会输入关键字，在检验输入框文本和输入关键字一致后，模拟键盘回车进行检索，当且仅当输入框可以正确输入文本并且检索内容不为空时，我们认为该输入框元素通过测试。

### 下拉框

下拉框在html中常常使用select元素实现，在selenium中为该元素提供了一系列方法可以获取其所有可选项、已选项，以及选择，反选等操作。然而在致远官网中采用了更为优美的下拉框样式，这种下拉框是由其自定义的列表和JavaScript代码实现，因此在测试中针对这种实现方式进行特殊测试。



**图2.1.3.1 下拉框元素**

具体测试步骤如下：

1. 进入致远官网下课程信息页面
2. 找到学年下拉框元素，点击，弹出可选菜单，测试可选项是否符合
3. 找到2018-2019学年选项，点击，测试是否选中
4. 按照上面的方法同样测试并依此选择秋季、计算机科学、2017级
5. 点击筛选，并等待结果返回
6. 检查筛选结果是否正确，包括筛选出课程的数量，以及课程的分类是否正确

### 轮播盘

轮播图位于致远官网首页最显眼的位置，也是网页加载过程中相当费时费力的一部分（四张分辨率很高的图片浪费了很多的带宽传输）。轮播图具有两个特点：一是无需用户任何操作就会每隔一段时间切换图片；二是用户也可以手动干预轮播图的播放，选择想看的图片。因此，我们的测试过程也分为两个部分：自动播放的测试与手动选择的测试。具体测试过程如下：



**图2.1.4.1 轮播盘元素**

1. 进入致远官网首页，等待页面（漫长的）加载过程。
2. 自动播放的测试：估算每次切换图片大约7秒，因此等待30秒，期间每隔1秒检查当前激活的图片元素，获取其图片url，并把它加入图片集合。最终图片集合中应当有四种不同的url，通过验证集合元素个数来检验测试的正确性。
3. 手动控制的测试：依此点击图片下方的四个按钮，点击后立即检查当前激活的图片是否正确。

### PDF文件查阅

在致远官网中，存在需要浏览pdf文件的场景。我们选取的pdf预览功能，位于致远官网-教学服务-培养方案下，选择专业和年级后便会加载出相应的pdf文件供预览使用。Pdf预览的功能是通过内嵌页面iframe的embed模块实现的。由于pdf预览的功能并不同于通常的html中的DOM元素，所以不能直接通过selenium定位和测试。我们采用了发送Key指令和win32gui、win32con模块来完成这部分测试。



**图2.1.5.1 pdf预览功能**

具体测试步骤如下：

1. 进入致远官网-教学服务-培养方案，并等待加载完成
2. 选择学科和年级，并点击筛选，等待pdf加载完成
3. 查找内嵌页面iframe元素，检查其src属性是否为pdf文件
4. 点击iframe设置焦点
5. 发送两次TAB键信号，使焦点落在旋转按钮上
6. 发送四次ENTER键信号，按下旋转按钮，使得pdf版式旋转90度四次。
7. 再次发送TAB键信号，使焦点落在下载按钮上
8. 再次发送ENTER键信号，触发下载，弹出另存为对话框
9. 通过win32gui模块定位到另存为对话框，并发送信号按下确定，下载完成，返回网页。
10. 通过switch\_to.frame切换到内嵌页面
11. 获取pdf元素并检查类型是否正确
12. 测试完成

### 文件下载

上海交通大学致远学院官方网站在特定分页会提供文件下载功能，此处我们挑选查阅并下载培养计划作为测试用例，将使用iframe展示培养计划pdf，并且提供下载功能，最后测试文件下载功能。

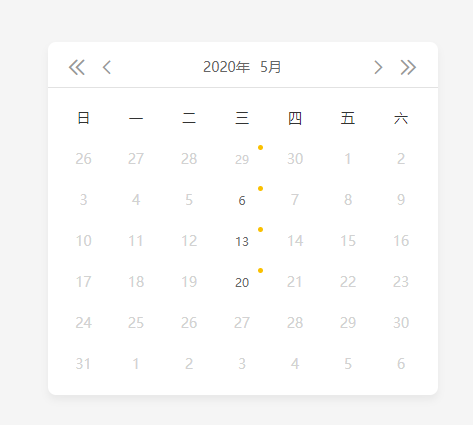


**.图2.1.6.1 iframe元素**

在检验方法上，测试代码在进入相应页面后，通过下拉框选择学科和年级，并点击的筛选按钮，等待iframe加载PDF，此时控制selenium switch into iframe，选择到iframe中的下载按钮，将文件存储与测试代码相同的文件夹中，如果下载文件不为空，则通过测试。

### 日历组件

日历是致远官网首页的一个重要元素，能够更加方便的让同学了解到某一天是否存在相关的活动（例如致远沙龙）。在有活动安排的日期中，右上角会存在一个光点，日期可以点击进入到选择日期的活动列表，没有活动安排的日期则不可以点击。



**图2.1.7.1 日历元素**



**图2.1.7.2 点击有效日期后的页面**

在检验方法上，我们将首先点击月份，选择月份为5月，进一步的，分别点击无效日期和有效日期，分别检查点击无效日期时页面没有发生跳转，在点击有效日期时页面将跳转到重要活动的列表。

## 可用性测试

在可用性测试中，我们进行了导航测试、图形测试和整体界面测试。而内容测试因为涉及网站内容正确性的测试，因此在本次测试中略去。而对于导航测试和整体界面测试的内容，往往涉及到最终用户的整体感受，因此我们邀请第三方用户进行调研测试。

### 导航测试

导航测试的测试内容主要包括对Web系统页面结构的测试，导航条、菜单、链接风格是否一致，以及用户凭直觉是否可以知道对应内容的位置等。这一系列测试的代码自动化测试已经被3.1.1的按钮测试所覆盖，而除此之外，还要有最终用户参与到测试过程中，以第三方用户的视角对网站进行测试。

因此，我们邀请了其他测试人员进行第三方测试，给他们一些致远官网的浏览任务，并最终通过问卷调查的形式进行测试结果汇总。本次的调研测试，一共邀请测试人员48名，其中上海交通大学本科生18人，其他高校在读本科生30人，每个人被给予以下的浏览和观察任务（为了保证调研测试的友好型，我们在问卷调查中将“二级页面”等专业名词隐去，且问卷中的2分钟仅为个人预估时间）：

1. 之前是否使用过上海交通大学致远学院官网
2. 是否能在2分钟内进入“学生服务”二级页面
3. 是否能在2分钟内进入“培养方案”二级页面
4. 是否能够通过整站搜索功能查找自己想要的内容
5. 网站整体的导航栏、字体、按钮等元素是否风格一致
6. 给网站浏览的整体感受打分（0-10分）

### 图形测试

致远官网首页使用轮播盘来循环展示图片，因为在轮播的过程中，组件的高度和宽度是固定，不同的分辨率会导致原始图片的长宽比拉伸变化、清晰度难以统一等问题。从用户可用性角度来思考，轮播盘中使用的图片应该使用相同的分辨率，如此用户才不会觉得有的图片相对不清晰，整体不统一，因此我们将对轮播盘图片的分辨率进行图形测试。

在检验方法上，测试代码首先进入到致远官网首页，并通过xpath获取到轮播盘的所有图片，使用python PIL library获取到图片的分辨率，所有图片分辨率相同则通过测试。

除此之外，我们还对导航栏下的所有二级页面进行筛查，着重检查二级叶念的字体风格是否一致、排版风格是否一致，以及非轮播盘的图片是否也能够做到分辨率一致、清晰度统一。

### 整体界面测试

整体界面测试是对整个Web系统的页面结构设计的测试，着重考察第三方用户对系统的一个整体感受。因此我们将这部分的测试合并到导航测试的问卷调查中，在问卷最后让每一个测试用户对网站的整体风格设计进行打分（0-10分）

## 安全性测试

在安全性测试中，我们结合了功能性测试中的Cookies测试，进行了四项测试内容：登录验证测试、数据加密测试、超时限制测试和渗透测试。

### 登录验证测试

上海交通大学致远学院官网通过Jaccount接口，提供了用户登录功能。



**图2.3.1.1 致远官网的用户登录入口**

我们结合功能性测试中的Cookies测试，进行登录验证测试，而因为Jaccount接口层的原因，关于输入的密码是否对大小写敏感、是否有长度和条件限制等等因素都无需考虑，这些都已经交给Jaccount解决。具体的测试步骤如下：

1. 打开致远学院官网，检验标题和登录入口是否存在
2. 验证 已经设置了两条Cookies
3. 点击登录入口按钮，验证跳转至Jaccount登录页面

### 数据加密测试

致远学院官网通过HTTPS协议进行传输加密和身份认证，保证了传输过程的安全性。因此在数据加密测试中，我们通过获取并检验网网站证书的有效性来测试数据加密。

### 超时限制测试

我们通过在登录后在主页驻留2小时不操作，来测试致远官网是否存在超时限制，即当用户长时间不做任何操作的时候，需要进行重新登录才能继续操作。

### 渗透测试

渗透测试包含了对致远官网的一系列目录测试、提权攻击等等，灵活性较高，我们将在下文的测试结果概述中进行详细阐述

## 兼容性测试

在兼容性测试中，我们通过更换不同的终端设备、浏览器驱动、显示分辨率进行测试（因为条件限制，不对连接速率进行调整和测试），考查致远官网在不同环境下的兼容能力。

从终端设备上，测试环境分为PC端与移动端两种。在PC端，我们先后使用Chrome和Firefox驱动进行测试，并且通过调整窗口大小来改变显示分辨率。在移动端，我们使用Chrome驱动去模拟移动端设备的访问，不同的手机终端则代表不同的显示分辨率。具体的测试环境分类情况可见表2.4.1。

|  |  |  |  |
| --- | --- | --- | --- |
| 测试环境编号 | 终端设备 | 浏览器驱动 | 显示分辨率 |
| 1 | PC端 | Chrome | 1920 \* 1080 |
| 2 | PC端 | Chrome | 1440 \* 900 |
| 3 | PC端 | Firefox | 1920 \* 1080 |
| 4 | PC端 | Firefox | 1440 \* 900 |
| 5 | 移动端 | Chrome | iPhone 6 |
| 6 | 移动端 | Chrome | iPhone X |
| 7 | 移动端 | Chrome | Galaxy S5 |
| 8 | 移动端 | Chrome | Pixel 2 |

**表2.4.1 兼容性测试环境概览**

针对以上测试环境，我们仅进行功能性测试，因为此部分测试均可以完全复用之前PC端功能性测试的代码，只需要调用selenium的相应接口去修改模拟设备、浏览器驱动和窗口分辨率即可。除了复用之前的代码进行功能性测试，我们同样对不同测试环境下的元素排版等进行人工测试，具体测试项目如下：

1. 轮播盘功能是否正常工作
2. 导航栏的显示是否正常
3. 二级页面下的条目元素是否显示正常

# 测试结果概述

## 功能性测试

在2.1中描述的针对网站七大元素的功能性测试全部通过，因此可以认为上海交通大学致远学院官方网站能够符合用户的基本使用需求。

## 可用性测试

### 导航测试

调研测试的统计结果可见表3.2.1.1：

|  |  |  |
| --- | --- | --- |
| 问卷问题 | 回答“是”的人数 | 回答“否”的人数 |
| 之前是否使用过上海交通大学致远学院官网 | 13（27%） | 35（73%） |
| 是否能在2分钟内进入“学生服务”二级页面 | 48（100%） | 0 |
| 是否能在2分钟内进入“培养方案”二级页面 | 47（98%） | 1（2%） |
| 是否能够通过整站搜索功能查找自己想要的内容 | 48（100%） | 0 |
| 网站整体的导航栏、字体、按钮等元素是否风格一致 | 48（100%） | 0 |

**表3.2.1.1 导航测试问卷调研的统计结果**

在调研测试的48名第三方测试人员中，有13名人员（27%）曾经浏览过致远学院官网，35名人员（73%）是第一次浏览该网站。比例合适。其他结果中，绝大多数测试人员均可以在短时间内从主页导航栏找到对应的二级页面入口，都能找到对应的整站搜索功能（即按钮测试中的一个带有放大镜图标的图形按钮），且所有人都认为在浏览过程都认为网站整体元素风格保持高度一致。由此，可以认为致远官网可以通过导航测试。

### 图形测试

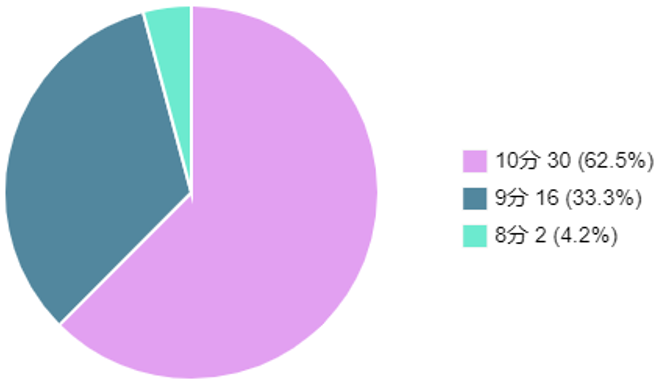
对于图片分辨率一致性的测试中，轮播盘的所有图片分辨率全部保持一致，通过测试。但是在二级页面下的条目图片却存在分辨率不一致的情况，导致某些条目的展示图片存在拉伸、失真的情况，测试不通过。具体情况可见图3.2.2.1所示。而字体、按钮等其他元素的风格也全部能够在二级页面下保持一致，通过测试。



**图3.2.2.1 原图与条目图片的前后对比**

### **.** 整体界面测试

问卷调研显示，48名第三方测试用户为网站的整体感受打分打出了9.58的平均分（满分10分），因此可以认为致远官网的网站整体设计符合大众审美，具备足够的美观性和可用性，通过整体界面测试。打分的分数分布可见表3.2.3.1所示。



**图3.2.3.1 整体界面测试的整体感受分数分布**

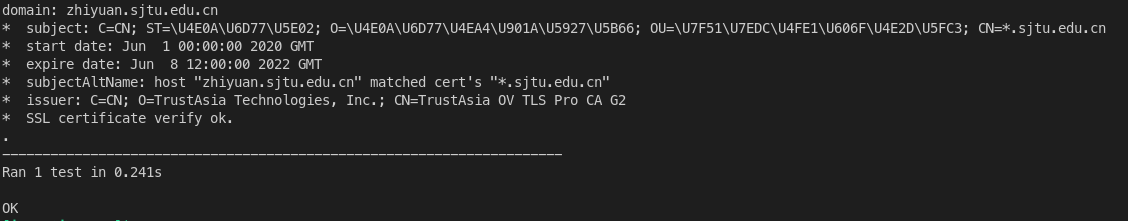
## 安全性测试

### 登录验证测试

测试结果显示，能够正确跳转至Jaccount登录界面，因此通过登录验证测试。

### 数据加密测试

HTTPS证书有效性得到检验，数据加密测试通过，证书的关键信息打印如下：



**图3.3.2.1 HTTPS证书的部分信息**

### 超时限制测试

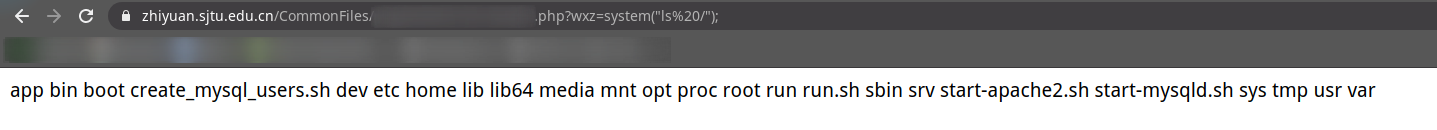
测试发现，从最终用户的角度，网站本身不存在超时限制功能，即登录后用户在某一界面停驻2小时依然不用重新登录。但是这一现象与本身网站的设计冲突，因为网站开发人员是对网站Cookies设置了120分钟超时限制的。

进一步研究后，我们发现，这是因为用户登录使用的是JACCOUNT认证，而Jaccount授权有效期为浏览器会话级，同时采用了SSO单点登陆技术，因此在网站登陆失效后会跳至Jaccount认证自动再次登陆，因此在浏览器不关闭的情况下站点Cookies实际上没有超时限制。

### 渗透测试

网站前台内容大部分为静态，搜索框处使用了ORM技术避免了SQL注入，浏览PDF处也限制了目录，无法读取其他文件，较为安全，因此可以认为致远网站通过了目录测试。

但是在取得低权限账户后，拥有上传权限，在上传校验处存在校验不当，可以上传任意php文件，通过CommonFiles路由访问造成任意命令执行。如图3.3.4.1所示，低权限用户可以在根目录下执行了ls命令。因此致远官网未能很好的通过渗透测试。



**图3.3.4.1 渗透攻击结果展示**

## 兼容性测试

针对八种不同的测试环境进行了功能性测试（复用2.1中功能性测试的代码）和人工排版测试，具体测试结果可见表3.4.1。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试环境编号 | 是否通过所有功能性测试 | 轮播盘功能是否正常工作 | 导航栏的显示是否正常 | 二级页面下的条目元素是否显示正常 |
| 1 | √ | √ | √ | √ |
| 2 | √ | √ | √ | √ |
| 3 | √ | √ | √ | √ |
| 4 | √ | √ | √ | √ |
| 5 | √ | √ | √ | √ |
| 6 | √ | √ | √ | √ |
| 7 | √ | √ | √ | √ |
| 8 | √ | √ | √ | √ |

**表3.4.1 兼容性测试结果**

由上述测试结果可见，在不同的测试环境下，致远官网均可通过了功能性测试，且在不同终端设备、浏览器驱动、显示分辨率下都能够正常显示元素排版。因此可以认为上海交通大学致远官方网站通过兼容性测试。

## 小结

综上，上海交通大学致远学院官网，通过了全部功能性测试与兼容性测试。可用性测试中，导航测试和整体界面测试通过，图形测试未通过。安全性测试中，登录验证测试、数据加密测试和目录测试通过，超时限制测试和渗透测试未通过。

# 措施建议

针对上述的Web GUI测试结果，致远官网未通过的测试项目分别为图形测试、超时限制测试和渗透测试，针对这些测试项目，我们提出一些改进措施和建议。

## 图形测试

图形测试中，我们发现二级页面上的条目照片存在拉伸、失真的现象。可以通过将图片格式、分辨率等进行统一规范的分类，比如分为大、中、小三类，分别对应不同的图片大小，并用于不同的场景，如大图用于轮播盘播放，中图用于条目照片展示等等，并以此来规范用户的上传过程。

## 超时限制测试

超时限制测试未通过的根本原因在于Jaccount的设计问题，因此在网站开发层面难以解决，无法提出措施和建议。

## 渗透测试

渗透测试的结果表明，一个低权限的登录用户可以达到提权的目的，造成任意命令执行的结果，对此我们有以下几点修复建议：

1. 限制上传文件类型
2. 取消上传目录php文件执行权限
3. 增加php disabled\_function，不允许危险函数执行