http://www.bit.edu.cn/images/2013zzgb/logo.jpg

测试方案

项目组 ： FishTouchers

小组成员： 刘 硕 1120161950

张嘉熙 1120161966

何祎君 1120161942

张 歆 1120161967

彭清峰 1120161957

潘恋军 1120161955

Professor：单纯

瞿凤业 1120161944

2019年8月30日 星期五

目录

[一、 文档说明 3](#_Toc18079113)

[二、 测试用例设计 3](#_Toc18079114)

[三、 测试过程方案 4](#_Toc18079115)

[3.1 功能性测试 4](#_Toc18079116)

[3.2 易用性测试 5](#_Toc18079117)

[3.2.1界面测试 5](#_Toc18079118)

[3.2.2文字测试 5](#_Toc18079119)

[3.2.3表单测试 6](#_Toc18079120)

[3.2.5 兼容性测试 6](#_Toc18079121)

[3.2.6 安全性测试 6](#_Toc18079122)

[SQL注入 6](#_Toc18079123)

[隐藏页面测试 7](#_Toc18079124)

[四、 测试报告撰写 8](#_Toc18079125)

文档修订

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **更改人** | **描述（注明修改的条款或页）** |
| 1.0 | 2019/8/30 | 张嘉熙 | 编辑测试过程方案 |
|  |  |  |  |

# 文档说明

本文档具体描述了对“高校科研实验室网站”进行系统测试的具体实施方案，包含测试用例设计，功能性测试、易用性测试、兼容性测试、安全性测试的具体步骤。

# 测试用例设计

根据需求规格说明书，列出主要功能列表，完成系统功能结构图如下：

* 管理员功能结构图：

****

* 用户功能结构图：

****

根据功能结构图，设计测试用例，实现对系统功能点的全覆盖，同时包含多种非法操作，以测试系统的安全性和健壮性。

本测试计划中设计了测试用例的编写模板，如下图：



通过统一所有组员的测试用例，可以更方便得统计出各项测试数据，整合分析各类bug，给出分析报告

# 测试过程方案

## 3.1 功能性测试

为确保网站功能的完整与正确，我们需要在业务逻辑测试阶段对系统流程中各个业务进行逐一测试，判断各个业务能否得到正确的执行，以及出现错误能否得到及时的反馈。

逐个运行测试用例集中与系统功能相关的全部测试用例，记录测试用例的通过情况，整合失败的测试用例进行分析，确定出现缺陷的功能点。

## 3.2 易用性测试

### 3.2.1界面测试

对于一个网站的系统，无论其功能如何，最终面向用户进行交互的，还是前端界面。用户界面测试就是为了保证用户界面能为用户提供相应的访问或浏览功能。此外，保证用户有良好的使用体验也是很重要的，比如功能模块的布局是否合理，整体风格是否一致，各个控件的放置位置是否符合客户使用习惯，操作是否便捷，导航是否简单易懂，界面中文字是否正确，命名是否统一，页面是否美观，文字、图片组合是否完美等等。

对所有的用户界面测试来说，都需要有外部人员（与Web应用系统开发没有联系或联系很少的人员）的参与，最好是最终用户的参与。

界面测试本身范围过大，可拆分为单个界面测试，整体界面测试，文字测试和表单测试：

#### 单个界面测试

1. **测试目的**
   1. 测试每个页面的美观程度，分析所有控件的设计是否合理；
   2. 分析每个页面中是否有多余或缺失的元素；
2. **测试方法**
   1. 需要靠测试人员浏览测试页面，通过自我的感官来对页面进行评价，找到对页面美感有所破坏的组件；
   2. 需要测试人员结合系统的功能，分析每个页面中是否有多余或缺失的元素；

#### 整体界面测试

1. **测试目的：**
   1. 测试整个系统的页面结构设计是否能给用户一种整体感，风格是否符合系统的功能；
   2. 页面之间的切换是否合理，正确，导航栏是否方便使用
2. **测试方法：**

要靠测试人员浏览所有的网页，分析记录系统中不符合整体风格的页面，并对系统的整体风格做出评价

### 3.2.2文字测试

1. **测试目的**
   1. 发现系统中是否有错别字或描述不当的地方，标点符号是否有误；
   2. 分析系统中所有文字的字体、字号等格式是否美观，是否统一；
2. **测试方法**
   1. 需要靠测试人员浏览所有包含文字的页面，分析其中的文字是否有错；
   2. 需要靠测试人员浏览所有包含文字的页面，观察其格式是否美观，并横向对比，分析页面之间的文字是否格式统一；

### 3.2.3表单测试

1. **测试目的**
   1. 测试所有的浏览数据表单是否会在异常的数据下产生问题（比如数据过长无法显示等）；
   2. 测试所有的填写数据表单是否会在异常的数据下产生问题；
2. **测试方法**
   1. 在系统功能允许的范围内设计测试用例，测试每个浏览数据的表单是否会有显示异常；
   2. 测试所有可能的输入数据（包含合法和非法），是否会在填写数据的表单处出现显示异常；

## 3.2.5 兼容性测试

兼容性测试保证网页在多种浏览器下运行正常

主要测试的浏览器如下：

* IE浏览器：IE8-IE11
* 360浏览器
* 火狐、chrome浏览器
* QQ、搜狗浏览器

测试工具：IETester，SpoonBrowserSandBox

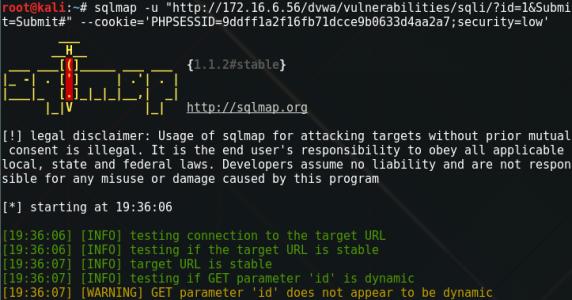
## 3.2.6 安全性测试

### SQL注入

**简介：**sql注入，即通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。个人开发的网站在上传表单、通过url传递参数的过程中非常容易出现对sql语句处理不规范导致的sql注入漏洞。sql注入漏洞是利用难度低且危害性极大的一种漏洞，极易导致任意sql语句执行，从而实现非授权访问甚至拖库、删库等对数据库产生巨大危害的恶意行为，甚至能够通过注入恶意语句获得服务器的shell，实现远程控制。

**测试计划：**在环境搭建、进行试用的过程中，已经发现了用户登录处存在sql注入漏洞，能够实现无密码登入任意账户并执行任意sql语句。所以推测软件中对sql执行的限定极为宽松，大概率存在更多对sql注入漏洞点，为了对注入漏洞进行全面的检测，我们使用针对sql注入的自动化检测工具sqlmap对站点进行注入漏洞扫描，能够获得大部分容易出现注入的Vulnerability， 然后对所有需要进行表单提交、数据库操作的代码部分进行审计，严格把控所有注入漏洞，并尝试对注入漏洞进行更多种方式的利用。

**工具介绍：**sqlmap是一个自动化的SQL注入工具，其主要功能是扫描，发现并利用给定的URL的SQL注入漏洞，SQLMAP采用四种独特的SQL注入技术，分别是盲推理SQL注入，UNION查询SQL注入，堆查询和基于时间的SQL盲注入。能够高效的对目标网站进行注入漏洞测试，其实际使用图片如下：

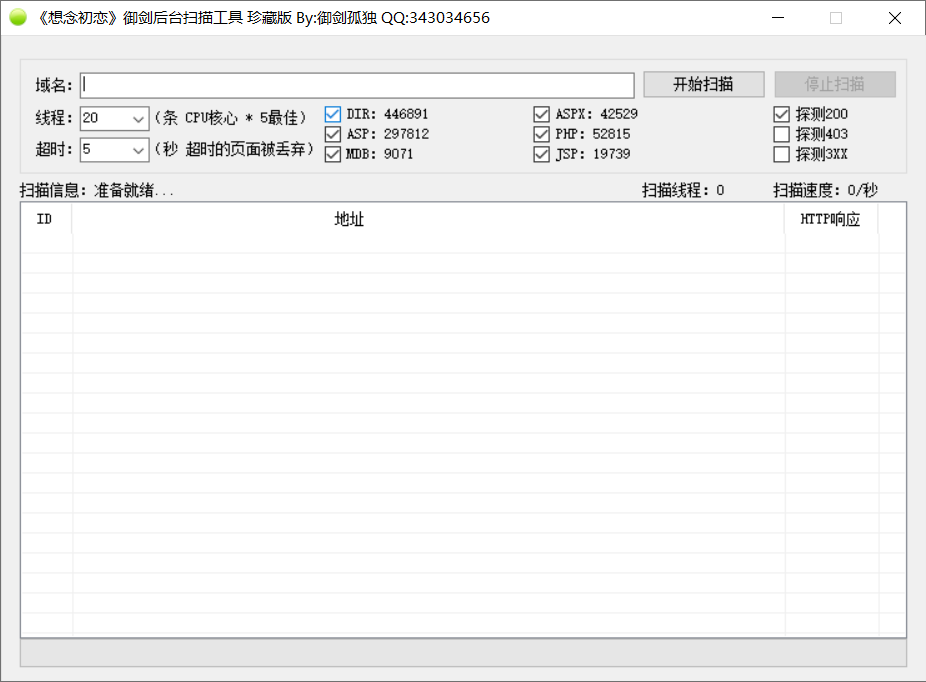


### 隐藏页面测试

**简介：**网站中的一些敏感文件通常在网页层面不可达，但是未对访问权限进行限制，如admin页面等。一旦攻击者知悉敏感文件页面的url，则能够进行非法访问，造成信息泄露或越权访问。

**测试计划：**图书管理系统除了普通用户页面外，必然存在管理员页面。理论上，管理员页面是普通用户无权访问的，但是不排除部分网站认为普通用户不能获得管理员页面的url，而没有采取相应的限制措施。使用御剑后台扫描工具对网站后台目录进行扫描，主要针对admin页面。如果存在普通用户可以访问的admin页面尝试对admin页面进行爆破，如果管理员使用弱密码则非常容易通过字典爆破获得管理员权限

**测试工具：**御剑后台扫描工具：软件能够对整个网站的页面进行扫描，使用强大的字典，支持对多种网页类型的页面进行扫描，获得隐藏页面目录。同时能够对扫描到的漏洞进行简单的分析。实际使用图片如下：



# 测试报告撰写

测试报告应包含以下内容：

* 系统功能测试中正确的功能点和出现缺陷的功能点
* 系统安全测试中发现的安全漏洞。
* 回归测试中已修复的缺陷和漏洞
* 回归测试中是否引入新的缺陷或漏洞
* 性能测试结果。
* 兼容性测试结果
* 系统安全风险报告