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

高校实验室网站

安全性测试报告

项目组 ： FishTouchers

小组成员： 张 歆 1120161967

刘 硕 1120161950

张嘉熙 1120161966

何祎君 1120161942

彭青峰 1120161957

潘恋军 1120161955

庞治宇 1120161956

张嘉诚 1120161965

瞿凤业 1120161944

2019年9月12日 星期四

目录

[一、文档简介 4](#_Toc19473500)

[1.1. 编写目的 4](#_Toc19473501)

[1.2. 系统简介 4](#_Toc19473502)

[测试概要 5](#_Toc19473503)

[2.1测试范围 5](#_Toc19473504)

[2.2测试方法和测试结果 6](#_Toc19473505)

[2.2.1. 测试工具介绍： 6](#_Toc19473506)

[2.2.2. 验证输入安全 6](#_Toc19473507)

[2.2.3. 隐藏页面安全 6](#_Toc19473508)

[2.2.4. 会话管理 6](#_Toc19473509)

[2.2.5. 权限控制 7](#_Toc19473510)

[2.2.6. 注入式漏洞 7](#_Toc19473511)

[2.3测试环境要求 7](#_Toc19473512)

[三、测试结论 7](#_Toc19473513)

# 一、文档简介

## 编写目的

本文档的主要内容是记录高校实验室网站开发项目安全性测试的测试过程、记录和分析经过测试暴露出的系统安全漏洞， 并在文末给出针对本系统的测试结论和测试建议。

## 系统简介

本网站分为游客、教师/学生、管理员三个视图，其功能结构图如下：

****

教师/学生功能结构图

****

管理员功能结构图

# 测试概要

## 2.1测试范围

对系统的安全测试范围包括

* 全部的功能操作，验证其操作中是否会出现安全威胁
* 测试覆盖的漏洞点包括：SQL注入、访问控制缺陷、输入安全、隐藏页面、会话管理、注入式漏洞、跨站脚本(XSS)

主要测试手段有：

1. 使用常见的攻击手段尝试对系统进行攻击
2. 使用自动化检测工具对网站进行扫描
3. 进行多种非预期的操作验证系统响应是否满足安全要求。

## 2.2测试方法和测试结果

### 2.2.1. 测试工具介绍：

|  |  |  |  |
| --- | --- | --- | --- |
| **工具名称** | **用途** | **生产厂商** | **版本** |
| 御剑后台扫描 | 扫描后台隐藏目录 | 御剑独孤(个体) | 1.0 |
| Acunetix Web Vulnerability Scanner | 对网站安全威胁进行全面的扫描 | Acunetix | 10.5 |

### 2.2.2. 验证输入安全

输入安全主要包括验证数据类型（字符串，整型，实数，等）、允许的字符集、最小和最大的长度、是否允许空输入、重复是否允许。

在系统输入位置输入：非法数据类型、超长字符串、空输入等。

**测试结果**：表单页面限制了必填项的输入；超长数据不会产生崩溃。

### 2.2.3. 隐藏页面安全

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。

使用御剑网站后台扫描工具对站点进行扫描。

**测试结果**：经过扫描，没有出现隐藏页面

### 2.2.4. 会话管理

会话管理安全主要体现在用户不同登录状态下页面的显示。用户结束会话后，用户页面不能继续显示。

在用户个人页面选择退出后再次从浏览器中输入用户页面URL

**测试结果** : 用户退出账户后，输入用户页面URL不会进入用户页面，显示未登录状态

### 2.2.5. 权限控制

权限控制分为水平访问控制和垂直访问控制，用户只能访问自己的页面，而不应该能够欧访问其他用户的页面和上级的页面。

1. 在其他用户个人页面选择退出后再次从浏览器中输入用户页面URL，尝试访问其他用户的页面。
2. 普通用户登陆后在浏览器中输入2.2.3中扫描得到的管理员页面url，尝试登陆管理员页面。

**测试结果** :未登录状态下访问下载专区和管理员页面都直接跳转到登录页面，有较好的权限控制。

### 2.2.6. 注入式漏洞

实验室网站使用vue路由搭建页面，不存在通过url进行注入的威胁，sql注入漏洞只能存在于用户输入。

在用户登录页面用户名处输入“123; #”,任意密码尝试进行登录；在用户注册页面用户名处输入“456 ; drop database books; # ”尝试进行删库攻击。

**测试结果**：没有实现对sql的绕过，可以认为本网站不存在sql注入漏洞。

## 2.3测试环境要求

* 测试结果及缺陷分析 软件环境：
  + Windows 10
  + Mysql 8.0
  + Tomcat 7.0.94
* 硬件环境：
  + Intel core i5及以上
  + 内存4G以上
  + 硬盘容量：100G以上

# 三、测试结论

1. 本次测试覆盖全面，测试数据基础合理，测试有效。
2. 数据输入部分有较好的数据管理和过滤功能，输入安全测试通过
3. SQL注入测试，sql注入测试通过
4. 用户权限控制和会话管理安全测试，网站具有较好的权限控制和会话管理机制，通过测试。

综合以上结论得出本次安全测试通过。