

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

基本

系统

上传

开发

数据库

新增

启用

禁用

删除

不限

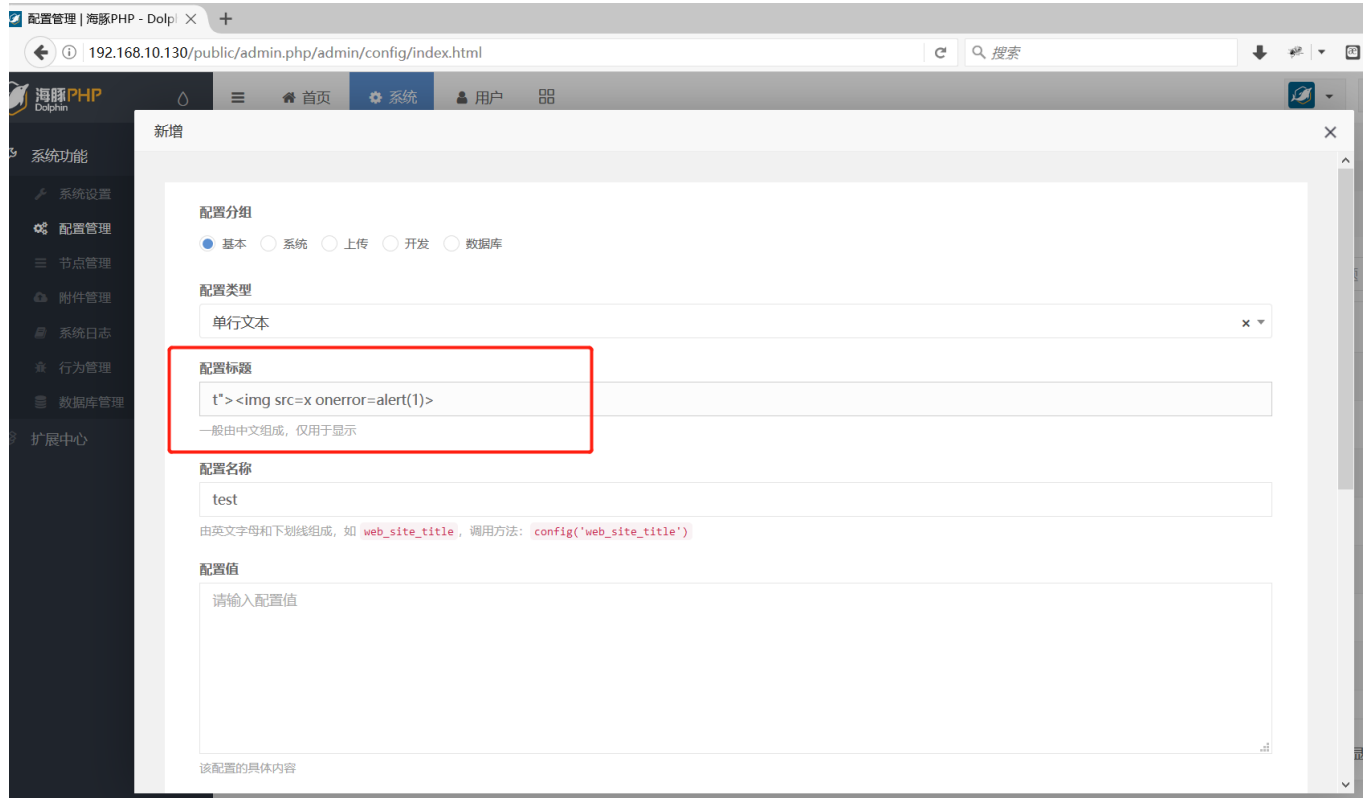
请输入名称/标题

	名称	标题	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	编辑 删除
<input type="checkbox"/>	web site title	站点标题	单行文本	<input checked="" type="checkbox"/>	2	编辑 删除
<input type="checkbox"/>	web site slogan	站点标语	单行文本	<input checked="" type="checkbox"/>	3	编辑 删除
<input type="checkbox"/>	web site logo	站点LOGO	单张图片	<input checked="" type="checkbox"/>	4	编辑 删除
<input type="checkbox"/>	web site logo.text	站点LOGO文字	单张图片	<input checked="" type="checkbox"/>	5	编辑 删除
<input type="checkbox"/>	web site description	站点描述	多行文本	<input checked="" type="checkbox"/>	6	编辑 删除
<input type="checkbox"/>	web site keywords	站点关键词	单行文本	<input checked="" type="checkbox"/>	7	编辑 删除
<input type="checkbox"/>	web site coovriahrt	版权信息	单行文本	<input checked="" type="checkbox"/>	8	编辑 删除

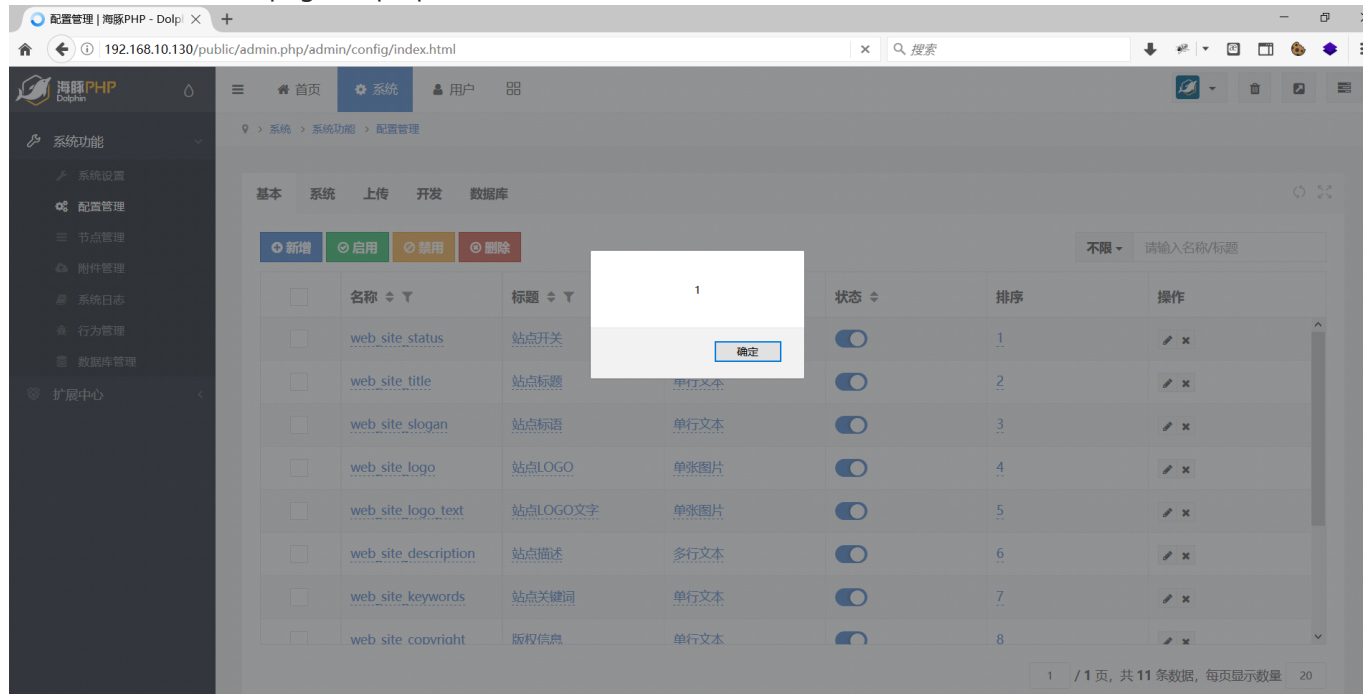
1 / 1 页, 共 10 条数据, 每页显示数量 20

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

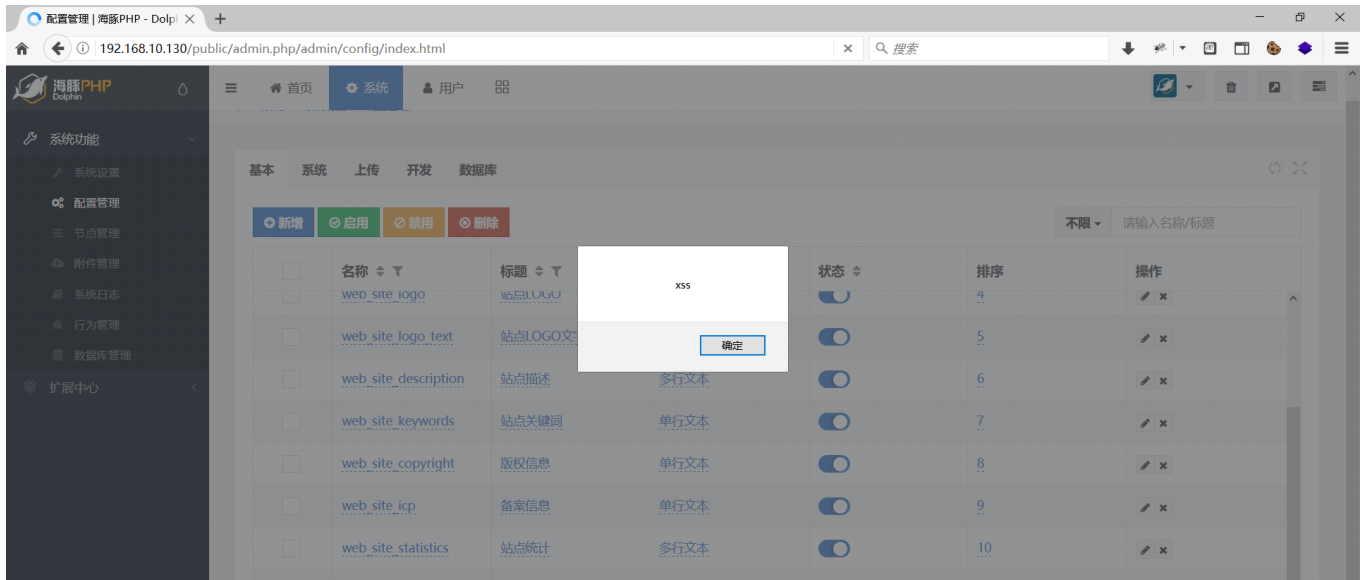
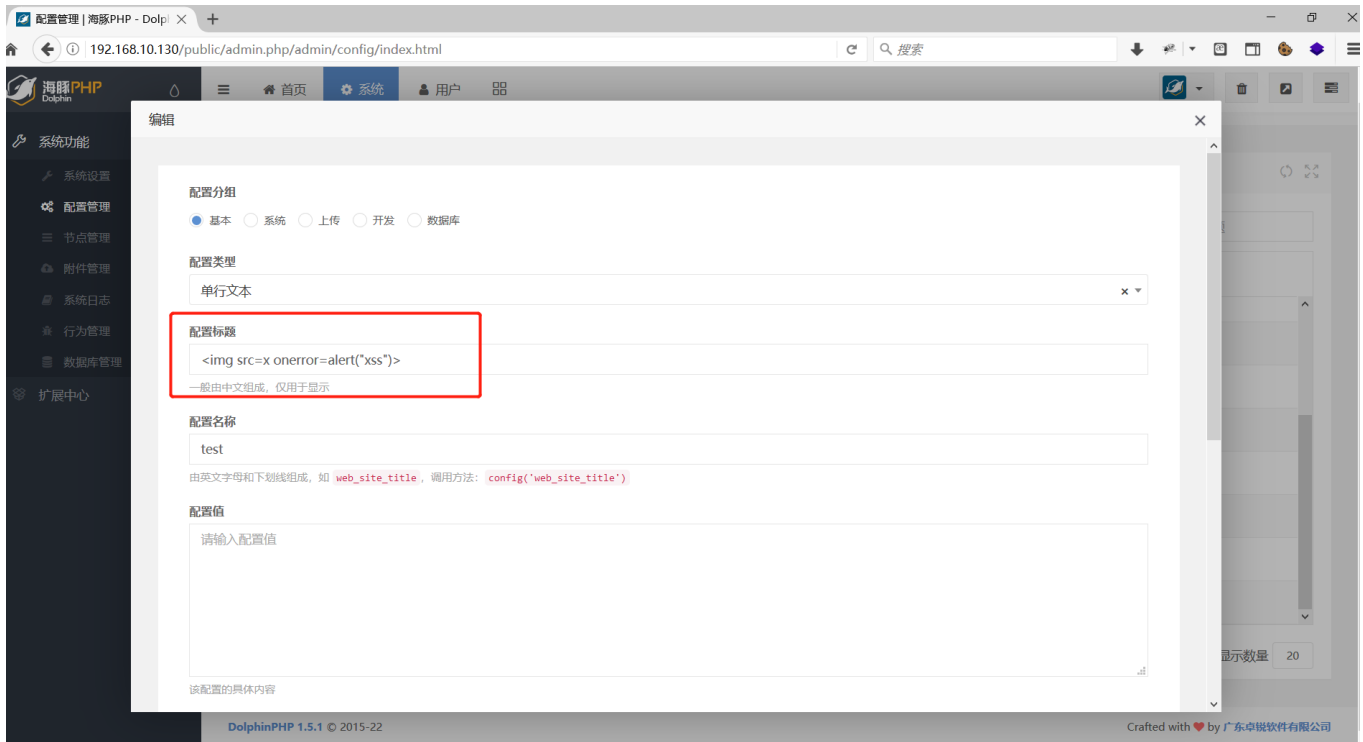
payload: `t">`



Save and refresh the page. Pop up window.



payload: ``



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

