New issue

Jump to bottom

There is a stored xss vulnerability here: /index.php?m=home&c=message&a=add #5

Open **zhendezuile** opened this issue on Mar 30 · 0 comments

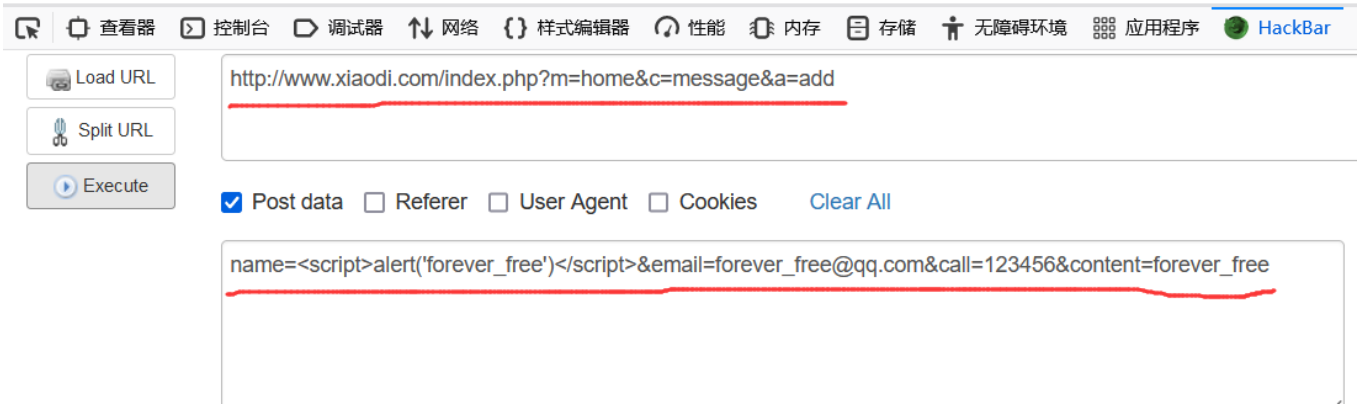
zhendezuile commented on Mar 30 • edited

Vulnerability file：\Application\Home\Controller\MessageController.class.php
You can see that the xss vulnerability is not filtered here

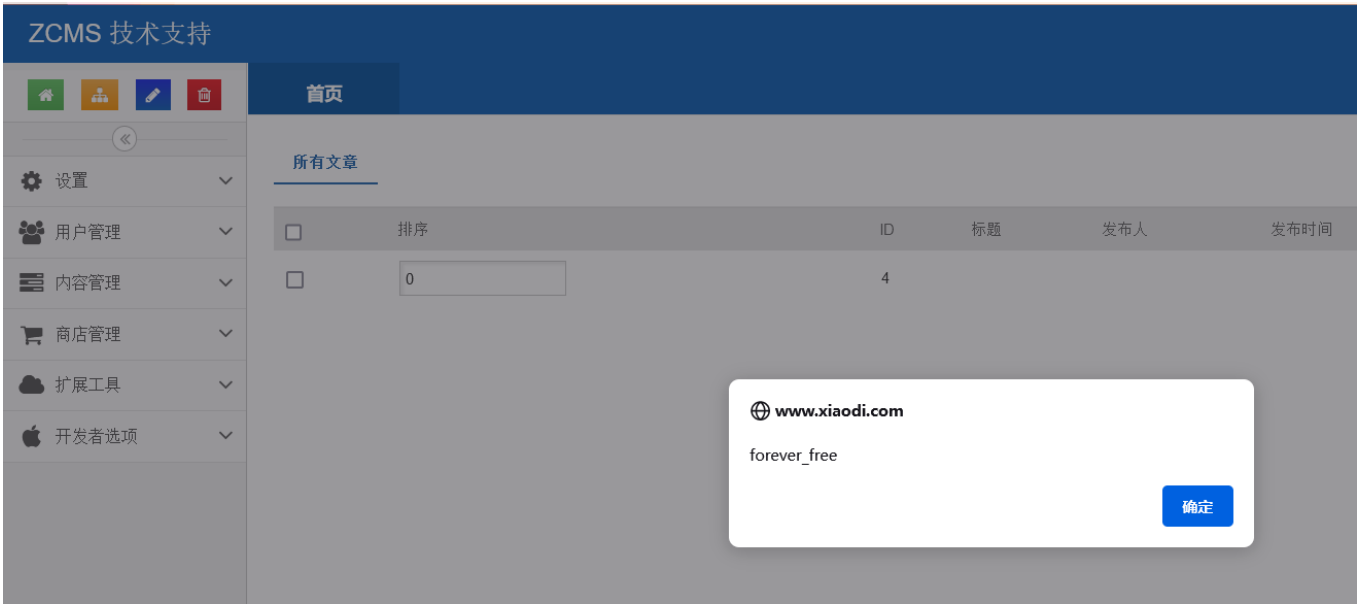
```
public function add()
{
    if(IS_POST){
        $msg=$_POST;
        $data['name']=$msg['name'];
        $data['email']=$msg['email'];
        $data['phone']=$msg['call'];
        $data['ip'] = get_client_ip();
        $data['content']=$msg['content'];
        $data['listorder']='0';
        $data['date']=date('Y-m-d h:m:s',time());


        $mssage = M("message");
        $msg_collection=$mssage->add($data);

        if($msg_collection){
            $this->success('留言成功');
        }else{
            $this->error('留言失败，请重试');
        }
    }
}
```

Vulnerability to reproduce:

1、Visit url: http://www.xxx.com/index.php?m=home&c=message&a=add ， use the post method to pass in parameter values，the specific operation screenshots are as follows:

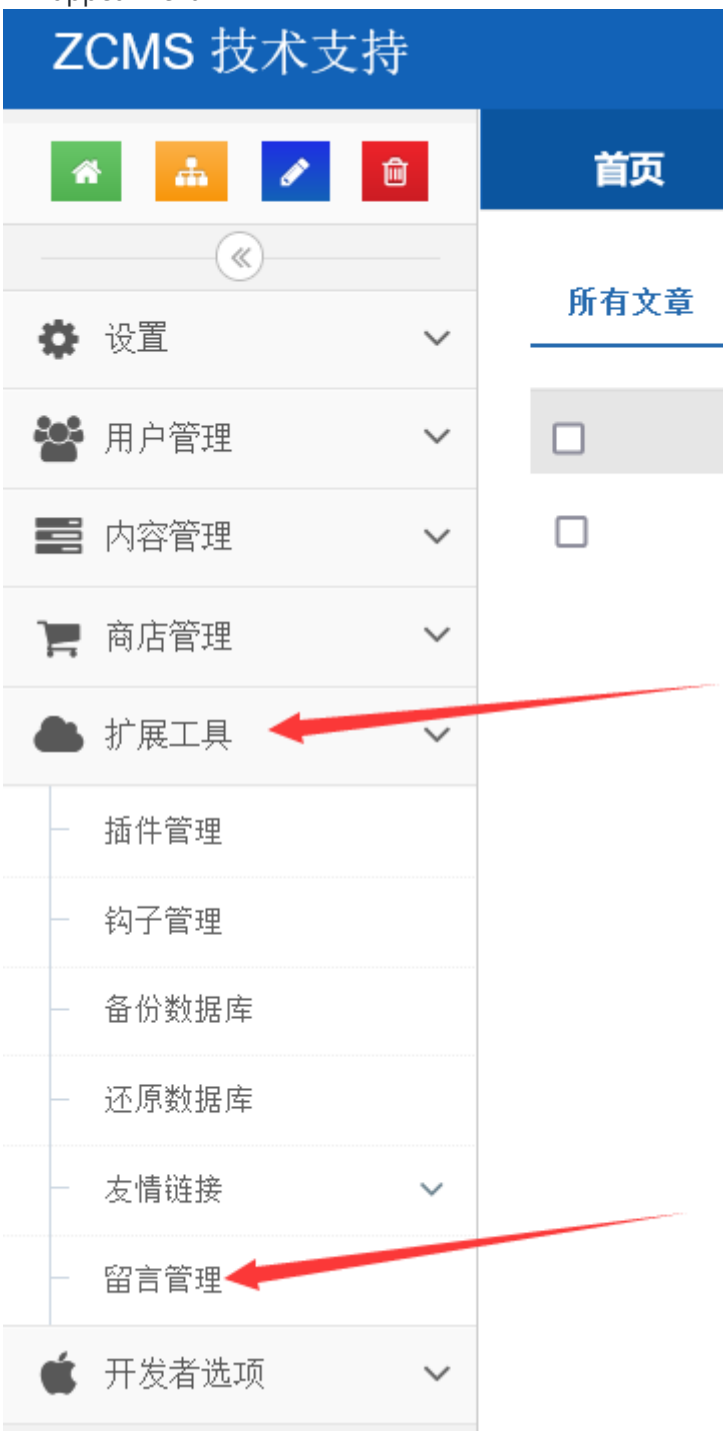


2、Access background address: http://www.xxx.com/Admin/Message/index/menuId/132 ， you can see the success popup



Or you can log in to the background, click Extension Tools, and then click Message Management， a popup

will appear next



Repair suggestion:
Use php built-in functions such as htmlspecialchars to filter xss vulnerabilities

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant