New issue

Jump to bottom

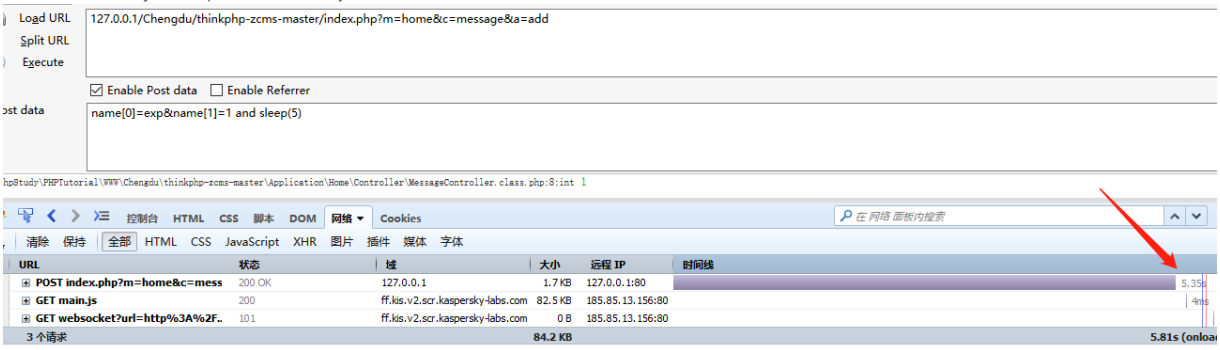
There is a sql injection vulnerability via index.php?m=home&c=message&a=add #2

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

Echox1 commented on Jul 15, 2019

```php
<?php
namespace Home\Controller;

class MessageController extends HomeController{

    public function add()
    {
        var_dump(1);
        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');
            }
```

use time-based bind injection to prove the vulnerability



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant