

master

...

maccms\_userinfo\_xss / maccms\_xss.md

I7o-0 Update maccms\_xss.md

History

1 contributor

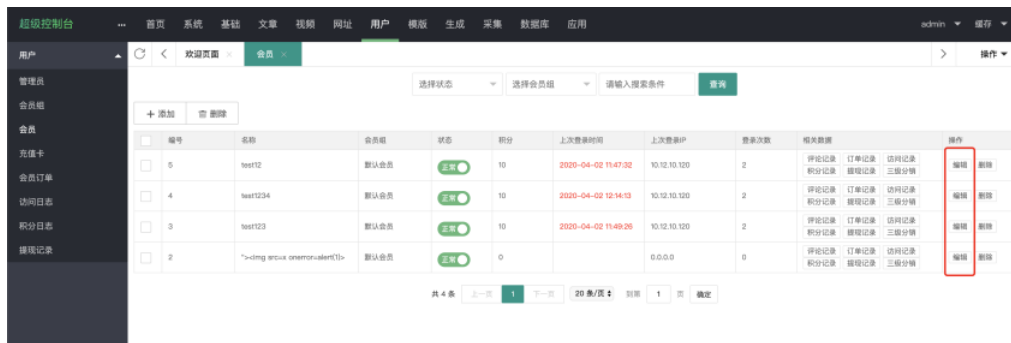
37 lines (19 sloc) 1.28 KB

maccms Background member information exists xss

version: v10

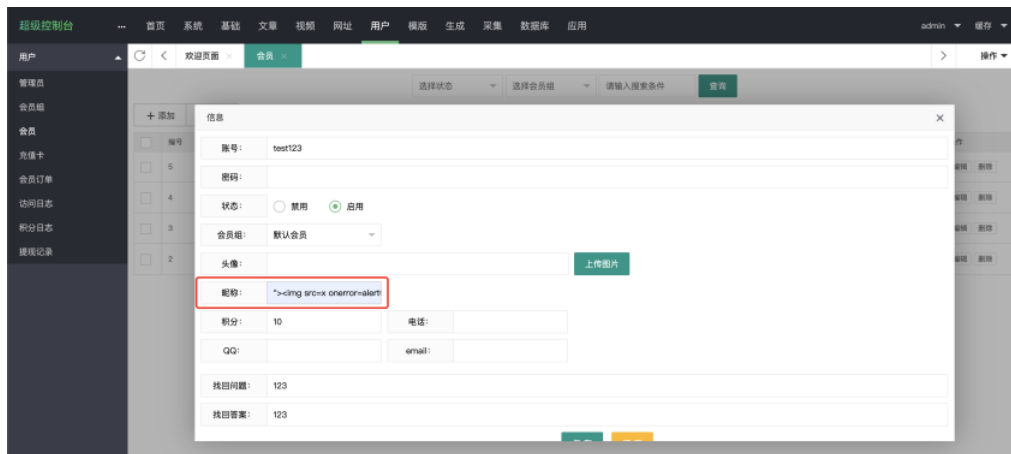
Software download address: <http://www.maccms.com>

Login to the background to enter the user-> member module -> editing function



管理	编号	名称	会员组	状态	积分	上次登录时间	上次登录IP	登录次数	相关数据	操作
<input type="checkbox"/>	5	test12	默认会员	正常	10	2020-04-02 11:47:02	10.12.10.120	2	评论记录 订单记录 访问记录 积分记录 编辑记录 三级分类	编辑 删除
<input type="checkbox"/>	4	test1234	默认会员	正常	10	2020-04-02 12:14:13	10.12.10.120	2	评论记录 订单记录 访问记录 积分记录 编辑记录 三级分类	编辑 删除
<input type="checkbox"/>	3	test123	默认会员	正常	10	2020-04-02 11:49:26	10.12.10.120	2	评论记录 订单记录 访问记录 积分记录 编辑记录 三级分类	编辑 删除
<input type="checkbox"/>	2	<img src=x onerror=alert(1)>	默认会员	正常	0		0.0.0.0	0	评论记录 订单记录 访问记录 积分记录 编辑记录 三级分类	编辑 删除

Write payload to the nickname in the edit window ( "<img src=x onerror=alert(1)>" )



信息

账号: test123

密码:

状态: ☐ 禁用 ☒ 启用

会员组: 默认会员

头像:  上传图片

昵称: <img src=x onerror=alert(1)>

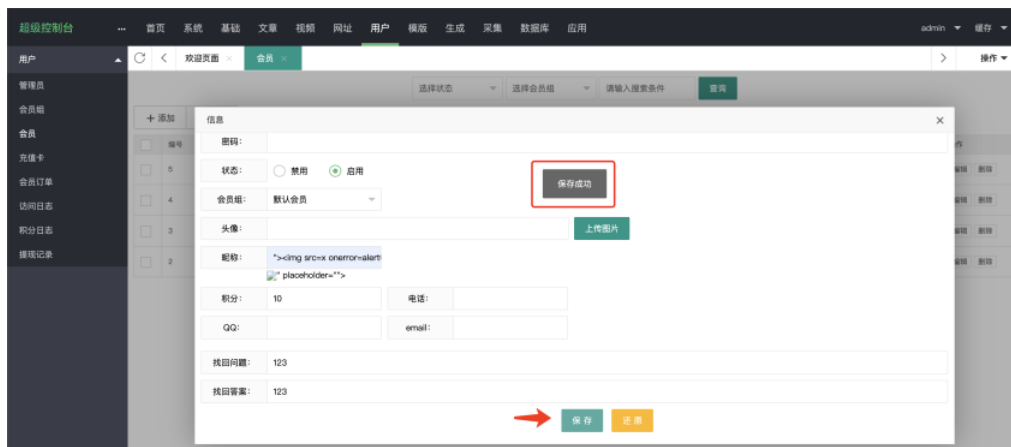
积分: 10 电话:

QQ: 邮箱:

找回密码: 123

找回密码: 123

Click save. Save successfully



信息

密码:

状态: ☐ 禁用 ☒ 启用

会员组: 默认会员

头像:  上传图片

昵称: <img src=x onerror=alert(1)>

积分: 10 电话:

QQ: 邮箱:

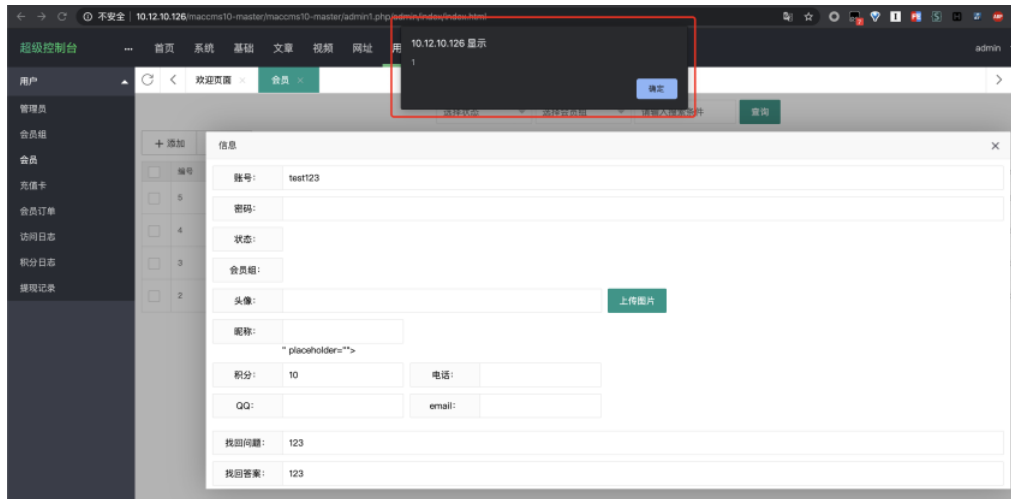
找回密码: 123

找回密码: 123

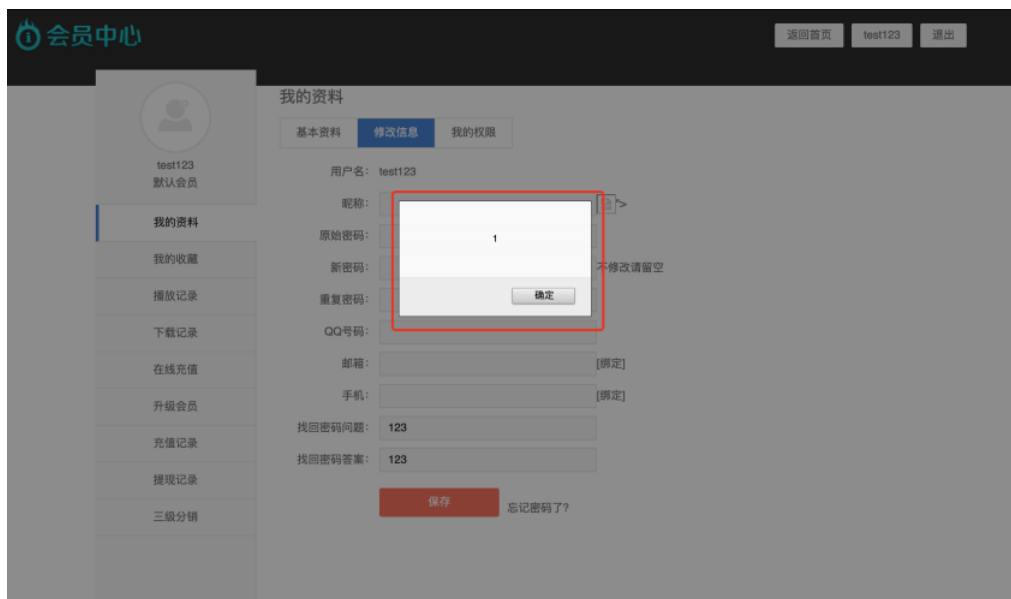
保存成功

保存 取消

The XSS attack is triggered when the administrator edits the user again



An XSS attack is also triggered when the user logs in



in /application/admin/controller/User.php

```

public function info()
{
    if (Request()->isPost()) {
        $param = input('post. ');
        $res = model('User')->saveData($param);
        if($res['code']>1){
            return $this->error($res['msg']);
        }
        return $this->success($res['msg']);
    }

    $id = input('id');
    $where=[];
    $where['user_id'] = ['eq',$id];
    $res = model('User')->infoData($where);

    $this->assign('info',$res['info']);

    $order='group_id asc';
    $where=[];
    $res = model('Group')->listData($where,$order);
    $this->assign('group_list',$res['list']);

    $this->assign('title','会员信息');
    return $this->fetch('admin@user/info');
}

```

XSS occurs when the data is not filtered while accepting the post data at the time of the saved information

in /application/admin/view/user/info.html

```

<div class="layui-form-item" >
    <label class="layui-form-label">昵称: </label>
    <div class="layui-input-inline">
        <input type="text" class="layui-input" name="user_nick_name" value="{{$info.user_nick_name}}" placeholder="">
    </div>
</div>

```

Data is also not filtered when user nicknames are returned