写一下自己对ctf的了解，以便日后自己需要

原创

tik2kk 于 2021-11-07 15:49:00 发布 3268 收藏 1
文章标签： php apache nginx

11.7

本人ctf小白，参加比赛基本处于摸鱼状态，也没有系统了解过ctf以及做过相关的实践和练习，但是，对这一块比较感兴趣，所以，只能说，在学习中，就跟我当初学makefile一样，做下记录，写点自己觉得对自己有用的东西，大概这样。

ctf总共分为五部分，misc杂项,crypto解密加密,pwn攻破设备、系统,reverse逆向渗透,web网络安全。500pt的题都很难。

首先，建立在你对前后端足够了解的基础上。

web安全就是黑服务器，pwn就是黑设备黑系统，至于怎么黑，**仁者见仁智者见智，取决于你自己的思维，自己对前后端以及工具的了解程度。**这属于正确意义上的废话，就好像很多工具如果不与时俱进就越来越难找到漏洞一样，还不是得看你自己怎么想怎么整。技术好的能玩出花，技术不好的，嗯，所以，努力吧！如果可以，谁不想技术好呢对吧！而且，每个人都有她自己的想法，去验证就是了。

工具确实重要，因为你不可能手动或者意念去黑系统服务器，但是，比工具更重要的是思维，你得知道怎么去黑，怎么写代码，如果没有思路，再好的工具也是徒劳，而且现在的防御系统发展的很快，工具的更新也需要随时更上脚步，否则也是派不上用场，就，很尴尬~所以，自己学会写代码或者模块简直不要太重要。

暂时只写这么多，9月份的我真的在摸鱼打摆子啊！也不算是，学了点物理吧属于是，十月份的话，前期在摸鱼，后期在搞前端和一些乱七八糟的东西，哎，都是一个生活过程罢了，不过像我这种边学边参加比赛的人，估计也不多~

当你意识到自己不是那么强的时候，恰恰是你要前进一大步的时候。我是很喜欢这种意识的，因为它只会让我更进一步。

对了，本人对ctf的最大感受就是它是高考，你得学个三年，做很多套模拟卷，然后上考场，500pt的题就是每套卷子的最后一道大题，分高且难，其余的题，多多少少解法啊啥的，基本上平时都会学到，怎么去解用什么工具去分析去拿flag值等等，好了，不说了，实战去了，实践出真知。

ctf的题大致分为两种，一种是有固定或相似解法的，一种是没有，比如二维码比如字符串等等，在固定解法上会进行一定的题型变形，知道解法的话，题就相当于解了一半，后一种比前一种难而且分值高。想起了高中被数学支配的恐惧，一道题n种解法，或者一道题变化成数道题，换汤不换药，大概这样。**不过这个比赛以结果为导向，**所以，如果有心在这一块取得成绩，找好对的资料，多做专项练习，有针对性的训练，最起码可以保证可以拿的分能拿上，至于那些大题难题，看个人实力以及对计算机的理解程度了。实战的话，只能说实战与ctf有相同之处，但是也有不同之处，能互相给到启发当然是最好的。大概这样。

由于ctf是个比赛，而且以结果为导向，而且发展的比较成熟，所以不太可能不经过一定的了解和练习就直接上或者写代码，因为很有可能你连题目要考啥都不清楚，只能搁那儿瞎猜，然后各种还猜错。毕竟是比赛吧！有固定的模式和技巧和方法在里面，不像自己要做的项目啊啥的，学了高级语言之后，好歹能写出点东西来。如果我没猜错，因为这行打比赛收入还行，所以网上的资料要么付费要么讲的比较浅显要么就是讲的不够全面，这是肯定的，包括视频或者文字资料，如果需要拿到干货ctf资料，大概率要出钱或者报班，这个很容易想到，再看吧！做我该做的事情，尽人事听天命。

11.8

还是自己按照自己的思维来整代码或者模块比较好，虽然不一定能整出个啥东西，但是，多思考多实践总是没错的，光想着攻击了，忘了还有防火墙这码子事。

kali上的工具在靶机上应该还挺好使的，实战中就还好，仁者见仁智者见智。如果光用工具，不自己思考自己整，在实战中怕是连边都摸不到，哪怕是用工具，还得上脚本上代码上字典，还得看那代码合不合适。时间紧任务重，只能祝自己好运了。

kali很多的工具包都放在/usr/share这个目录下，包括不限于一些字典、渗透工具文件、mysql、apache2、渗透数据库等等。

11.9

不好破，真心话，可能跟我实战有关，bug比较少，有点尴尬，不过会继续，直到我自己觉得满意为止。

11.11

哎！还是自己太井底之蛙了，意识到自己在ctf这一块还是个菜狗级别，尴尬！而且跟那些个经验丰富的ctf er们写的文章比起来，真的，我这个太偏理论了，人家那都是实打实的经验，写出来的东西确实挺干的，懂得自然懂。

希望自己早日从理论转实践吧！**当我意识到自己菜的时候，恰恰是我要奋起狂追的时候！菜不可怕也不可耻，可怕可耻的是明知道自己菜还不努力！尴尬！我搁这儿大锅炖鸡汤呢！不说了~**

哦对了，那些跟我一样的ctf小白们，要想认真打ctf，先多去看看大神们或者经验丰富的ctf儿们写的文章，会收获到很多工具以及思路，然后，等熟练之后，再自己创新吧！加油共勉~

强调一下，实战和打比赛以及打靶机虽有相似，但更多不同，别问，也许以后能吃上国家公粮，别管哪儿的就行。以及，在计算机里，不管是哪个领域，思维永远比工具重要，始终坚持这一观点，永远不改~

XSS：攻击浏览器的方法，主要语言html、javascript等。

SQL注入:攻击服务器的办法，最主要的是绕过，xss也得绕过过滤机制和防火墙等防御措施，主要语言php、asp等。整个后门，想办法连接上，然后就可以让它为你服务了，至于提权、拿数据啥的，那都是后话了，先把这一步整好。

文件上传：找注入点，找到了，还是得绕防御机制，甭管什么方式，差不离吧！都得绕，你要攻，人家就要防，所以，思路转一下就知道是这么回事了。至于具体的方法，还在实践当中，你了解的越多，越详细，越得心应手，攻起来就越熟练，不敢说精通二字，因为万一人断网了，你总不能社工吧！我指的实战，还是那种比较高难度的实战。

至于抓包，就是让你知道一下自己的攻击过程和结果，大概这么个意思。

关于ctf我觉得那个攻防模式就还挺有意思的，又得攻又得守，太考验功力了，脚本小子还是大神一下子就区分开了，你得知道自己系统得漏洞，找出漏洞，还得自己去打补丁，还得去攻击别人系统的漏洞，全套操作一整，一个字，牛啊！

为什么c这么难学，因为它的函数难啊！因为它的内容多！主要还是函数难，太多道道在里面了。

11.12

在爱春秋上刷了两道题，看了一下别人写的wp，嗯，意识到了自己的垃圾，然后就是，实践大于理论，否则就是纸上谈兵了，继续努力吧！菜鸡我瑟瑟发抖不敢说话，退了，不说废话了，毕竟要写出干货，还是得靠实践靠时间也靠经验。

正在学习ctf，这让我想起了我准备法考的日子。ctf跟法考本质上也差不离吧！

首先，有正确的对应考试的资料，其次，有老师授课的视频带你入门，比你自学要好，老师知道考点在哪里，你总不能拿着本刑法典背吧！最后，做真题，做模拟题，这一步在前两步之后。

那么，对比我的ctf学习，没有正确的对应考试的资料，知道考点，不知道具体的考点，就好像不学法不考法考的人，也知道法考要考刑法民法经济法等等，有什么用？具体考点不知道啊！没有老师带入门的视频，有真题，但是前述两点不具备，直接上手真题，看到题了，不知道具体考点，除非我之前碰到过，而且，我这几天也才刚刚开始刷题，之前在做理论性的学习，看了点东西，好像不如直接看对应的具体考点再加做题，因为理论说的比较笼统，在实践中更是千变万化。至于以后的话，走一步看一步，就这样，ctfer们加油！共勉~

总感觉ctf的题做了几道，跟实战中的情况确实不一样，跟靶机中的情况也不一样，我的感觉应该没错，难度大概是靶机小于ctf小于实战（高难度的实战）。

哦明白为什么要这么执着于打ctf了，**原来是因为自己对做一名彩虹客有执念**，尽人事听天命，大概这样。

ctf和实战彩虹客和搞项目写代码，虽有相通之处，但是归根结底，是三码子事儿，连用的函数都不一样呢，本人亲测，佛了已经，靠悟也靠实践，不过会继续实践，对，实践加写代码，写代码写代码写代码，写到老子写不动那天为止，总有一天，我会成为一名彩虹客！！！

而且，计算机这个东西，简直就是为需而生的，需是需求的意思，我无数次问自己，这整半年的学习时间，我学了啥，做了啥，后面发现我是一个项目也没做，不代表我没学到东西，也不代表我就做不出东西，所以，还是自己做项目或者在实践中多历练才行，有需求了，自然就要写代码了，不写也得写，不学也得学，所以，按需学习。

对了，想打ctf，除了多做题多参加比赛，别无他法，没有任何捷径可走！这种比赛也好需要考证的考试也罢就不适合搞理论，搞理论就gg,连决赛都进不了。如果是刚入门，毕竟我也是刚入门，就多刷题，不懂的就去找别人的writeup，前期多刷多看，中后期多做多练，大概这样。

五大类题型，其实都有固定的考法和考点，然后在此基础上进行变形，比如二维码那类，比如sql那类，xss那类等，还有各种固定工具的固定用法，burpsuite、wireshark、winhex、菜刀等，各种编码解码等，以及出题人的无限脑洞，简直是酸爽！我佛了已经，ctf从入门到入土，不过我会继续努力的。

原因很简单，理想上，我喜欢玩黑客技术，想当彩虹客。现实上，ctf比赛多，钱多，当然了，你自己得有实力，再做点安全相关，温饱或者小康问题不大。

就分享到这里。

11.13

拿到一个ctf题目，先去查页面源码，肯定多多少少有点东西在里面，大部分是这样，有些是考其他的知识点，不会用到页面源码，比如路径穿越那种题。

400pt含400pt的题，基本上要自己写脚本或者模块或者代码，而且还得根据它的出题点来写，懂的自然懂。

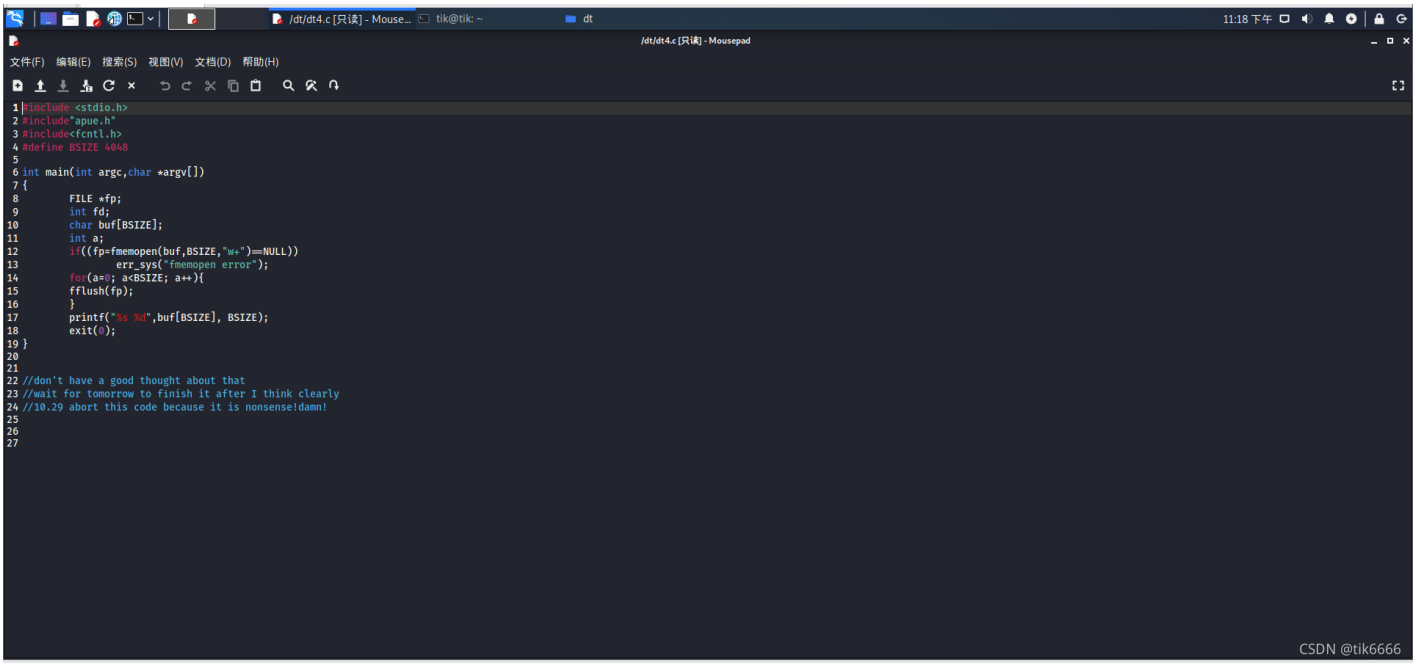
400pt、500pt的题难是难，但是真的可以get到很多有点意思的东西，能学到很多，所以，要想获得真正有价值的东西，基本上都比较难，而能轻易得到的东西，价值一般而言都不大，此处的价值衡量仅针对事物，不针对人。

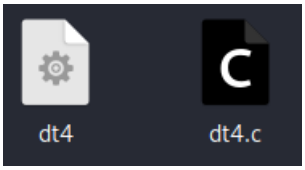
（攻防核心我给你们指出来搁这儿了，想跟我一样做黑客或者彩虹客的，黑攻基础方法也告诉你们了，至于具体做法，自己延展吧！不用谢，叫我雷锋~大道至简是真的）

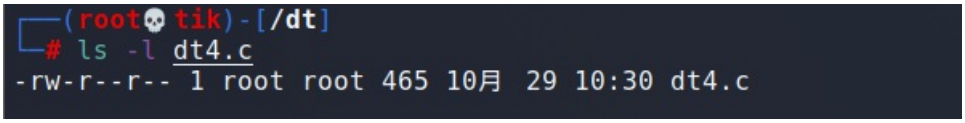
关于xss、sql、php上传、python沙盒逃逸，众所周知，**有攻有防思路**，咱们要想攻进人家系统、网站等，就得绕过人家的防御机制。原理大同小异，换汤不换药，就是把一些敏感函数过滤掉设成黑名单，一旦你提交那些含敏感信息的代码，分分钟给你kill掉。**做法无非就是绕过，用另外一些函数去代替那些敏感函数实现功能，或者换个代码书写方式，能绕过就行，**懂？至于具体怎么写，不好意思，我实战经验不足，等我多做多练多写之后，心情好了，分享一下，心情不好，我自己知道就行，干嘛要让你们知道，且！**（听说你们很强，啧，没事，总有一天，你们会成为我王富贵的手下败将，不解释,此处的你们指的是我碰到的一群反社会人格，其他人请勿对号入座）**

11.14

看了一两个pwn的题，我想说跟我的想法还是挺相似的。是这样的，我电脑里一直都有病毒文件，还被人隐藏了打都打不开，我为这事儿也想了挺久的了，当时的想法就是，找到那些文件在磁盘上存放的大致位置，然后用fflush函数去冲刷掉，大概这样，当时还写了个小小的demo，生成exe了，但是没达到我想要的效果，下面贴图。看了pwn的wp，哦原来还有专业名词叫覆盖，好吧！金丝雀这个我之前有在mit的视频课里听到过，大概是保护敏感数据的一种方式，个人理解，好吧！我懂但不代表我就一定会写出点啥，还是得多练习多实践才行，但我相信自己一定可以，多打比赛多写代码多琢磨多思考，大概这样。





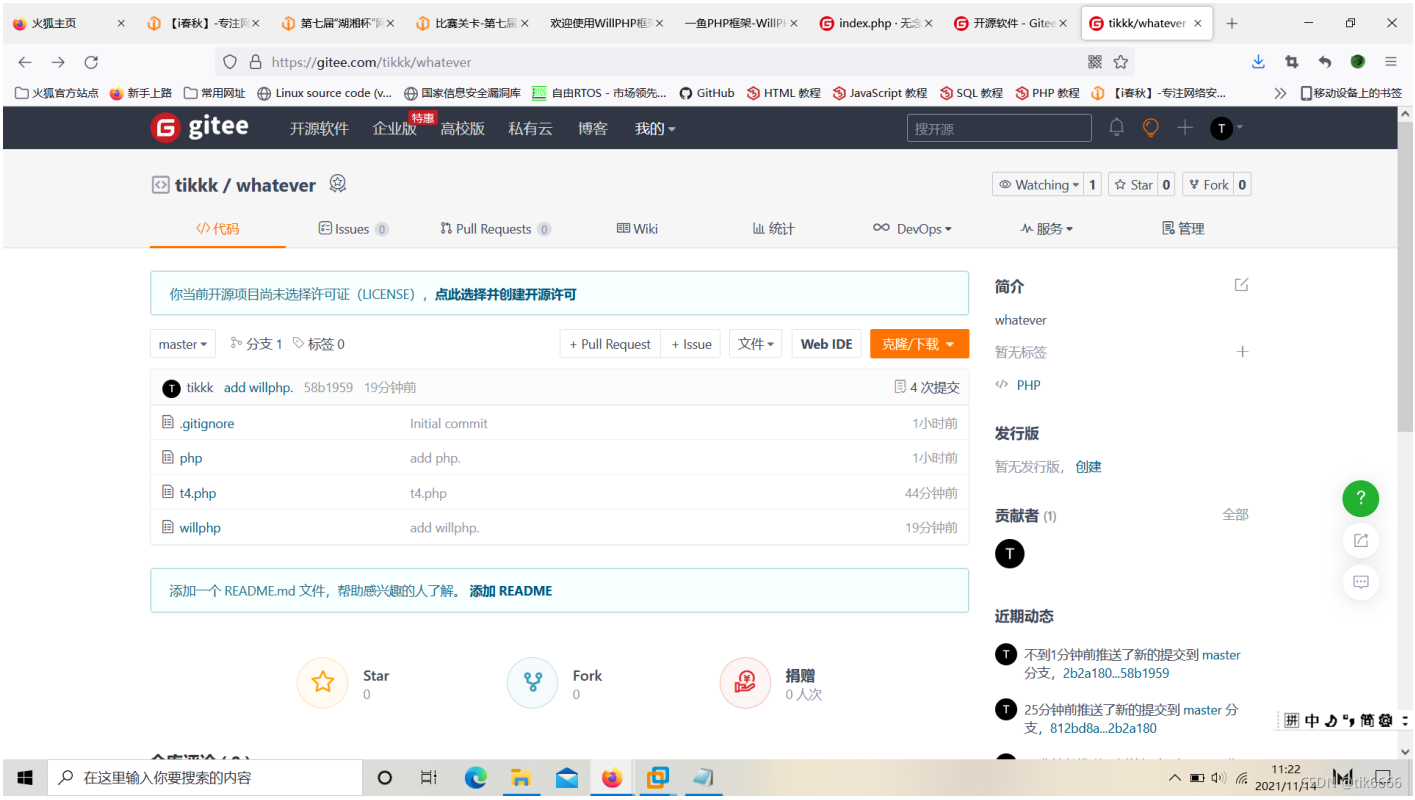


第七届湖湘杯参赛记录

观赛视角是看不到题目的，只有参赛的才可以，全部都是500pt的题目，毕竟特等奖18万奖金，比赛规模也算是很大了。我到今天才知道，原来随着一个题目解出的队伍数越多，后面解题的人分数就会越低，是一个即看结果又看速度的比赛了。

我真的佛了，全部都是要上代码的，大概是吧！加密那个也是，web那个题虽然能够上传php文件，但是我没下菜刀和中国蚁剑啊！

这是web题



这是加密题，听说算出什么p值n值可以求解，貌似是有特定的求值法。可惜我这几天就刷了十几道题，还没一道是加密解密的，尴尬~毕竟一想到md5不可逆，额，感觉学了实战中能用上的几率比较小。

task - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

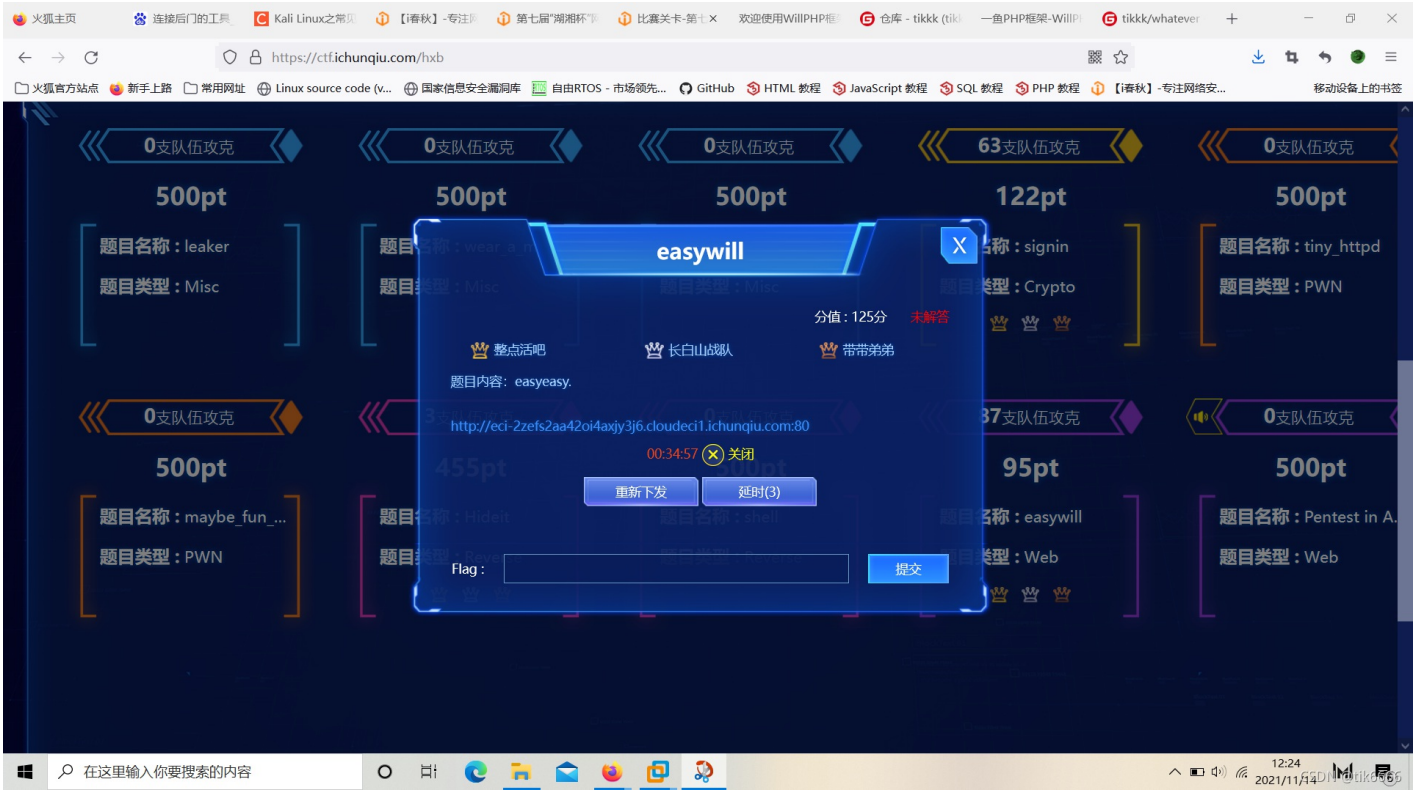
```
from Crypto.Util.number import *
from secret import flag
import random

m1 = bytes_to_long(flag[:len(flag) // 2])
m2 = bytes_to_long(flag[len(flag) // 2:])

def gen(pbits, qbits):
    p1, q1 = getPrime(pbits), getPrime(qbits)
    n1 = p1**4*q1
    q2 = getPrime(qbits)
    bound = p1 // (8*q1*q2) + 1
    p2 = random.randrange(p1, p1 + bound)
    while not isPrime(p2):
        p2 = random.randrange(p1, p1 + bound)
    n2 = p2**4*q2
    return (n1, n2), (p1, q1), (p2, q2)

e = 0x10001
pbits = int(360)
qbits = int(128)
pk, sk1, sk2 = gen(pbits, qbits)
c1 = pow(m1, e, pk[0])
c2 = pow(m2, e, pk[1])
print(f'pk = {pk}')
print(f'c1, c2 = {c1, c2}')

"""
pk =
(115039807056545949208059771862603279243555670341392348345870467529599764649324975981846832132855651007404495467661576044670825353183941703699781150622234919
430279194348919571871379732287858637954665727541926164763585998928070019144131269127428517661939153938787525213547842458068026455429417912325456679689099824390928650818982645885434682549315769720149510062821683219103590384839144770484980857731061272370031867046603507720267337395632472510835023035787937423441839323312426787370760480967800231477025141122723194974238184881935579346955837930703321787230431948234448151537438897403388706760937997288757256510360603132230962886069477081555790606288075160539819758203380284567701096401111537199032073636170993713539102434978710903348985229429340520351029028921497925709651
```

第 1 行，第 1 列 100% Unix (LF) UTF-8

在这里输入你要搜索的内容 11:26 2021/11/14

别问我为什么还有心思搁这儿记录，因为我在思考我的代码要怎么写？别问是什么代码，问就是代码。话说队伍真多啊！

真的是时间拖的越久，分值就越低，菜刀和蚁剑都下不了，因为不是正版，被人装了后门，啧~



关于这道web题，我的工具啊！不全，真不全，但是成功了又好像没成功，可能是上传的php在服务器里没跑起来。可恶啊~

```
┌──(root💀tik)-[/at]
└─# weevely http://116.55.250.136/t5.php 1234

[+] weevely 4.0.1

[+] Target:     116.55.250.136
[+] Session:    /root/.weevely/sessions/116.55.250.136/t5_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> help
The request triggers the error 400, please verify running code
Backdoor communication failed, check URL availability and password
weevely> Exiting.

┌──(root💀tik)-[/at]
└─# weevely http://116.55.250.136/t5.php 1234

[+] weevely 4.0.1

[+] Target:     116.55.250.136
[+] Session:    /root/.weevely/sessions/116.55.250.136/t5_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
The request triggers the error 400, please verify running code
Backdoor communication failed, check URL availability and password
weevely> ls
The request triggers the error 400, please verify running code
Backdoor communication failed, check URL availability and password
weevely>
```

另外，**实战和打比赛真的是两码子事（尤其是在实战难度系数比较高的情况下）**，我也不知道一个不能xss、sql注入，一注入就报错，还全是静态页面，并且服务器为nginx的网站，要怎么入侵比较好，可能是因为安全级别比较高。

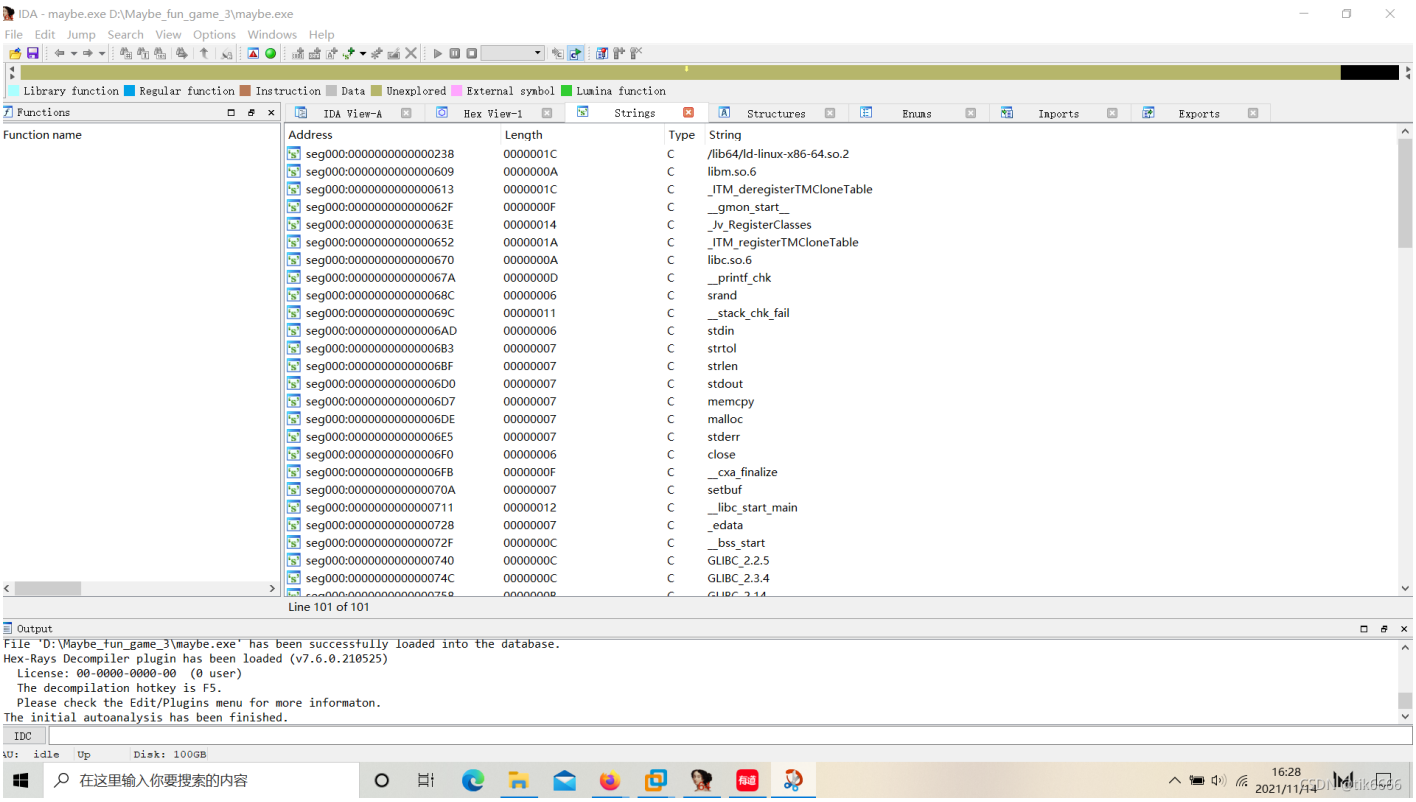
尽人事听天命吧！

啥也扫不出来，pwn的题就是难~这题好像就一个队伍开张,多刷题吧！写代码去了。php、c、xss、sql、asp、python以及汇编代码，该用的时候都有其对应的场合，在ctf场景中，归根结底，这比赛还是写代码的事儿，**毕竟代码可以创造工具，工具可创造不了代码。**

```
┌──(tik㉿tik)-[~]
└─$ sudo su
┌──(root💀tik)-[/home/tik]
└─# nikto -host 123.56.122.14 -port 19812
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 123.56.122.14:19812
---------------------------------------------------------------------------
+ 0 host(s) tested
```

CSDN @tik6666

我王富贵把话放这儿，我之前那半年基本上在学计算机，没有认认真真的打过ctf比赛，**而且更重要的是，计算机的学习跟ctf其实是两码子事儿，有关系但是关系真的不算太大，倒是我之前想岔了。**前期是参加了两三场，但是没学，基本上签个到，然后就摸鱼，看看其他的战队，这是我第一次比较认真的打这个比赛，这段时间也学了一点这个比赛的事情，然后刷了十几道题，我就打算边学边打，边打边学，没有其他的诀窍可言，干就完事了，这次比赛结束后，欸我接着刷题接着学接着黑，很简单的理儿，就这样。



关于maybe_fun_game3这个pwn的题，事先说明一下，我不知道考点在哪里，我只是搁这儿整理一下有用的信息，我以后明白了可以接着来捋思路，又不是说比赛结束了我就不刷题不想这事了对吧！

附件是zip后缀文件，解压，将文件改成了exe后缀，用ida打开，得到上面那些,给了个nc，如图。

我用kali工具测试了一下，nmap、nikto都试了，一无所获。ida的话，文件打开，发现一个支付宝网页链接，一段文字关于扣扣恋爱空间，还有一串有点奇怪的字符串。

```
] seg000:000000000000202C        0000001D                C       http://alipay.com/xiaolanlan
0000000000001F60  00 00 00 00 00 00 00 00  E6 AC A2 E8 BF 8E E8 AE  ........欢..迎...
0000000000001F70  BF E9 97 AE E8 93 9D E8  93 9D E5 92 8C E6 B1 AA  .问..蓝..蓝..和..汪..
0000000000001F80  E7 9A 84 E6 83 85 E4 BE  A3 E7 A9 BA E9 97 B4 E7  的..情..侣..空..间...
0000000000001F90  95 99 E8 A8 80 E6 9D BF  EF BC 81 E8 AF B7 E4 BD  ..言..板..！ ..请...
0000000000001FA0  BF E7 94 A8 E5 8F 8C E8  BE B9 E5 8D 8F E8 AE AE  .用..双..边..协..议..
0000000000001FB0  E5 AE A2 E6 88 B7 E7 AB  AF 28 3D 33 2E 30 29 E8  客..户..端..(=3.0).
0000000000001FC0  BF 9B E8 A1 8C E6 8E A5  E5 85 A5 EF BC 8C E4 BB  ..行..接..入.., ....
0000000000001FD0  A5 E9 98 B2 E4 B9 B1 E7  A0 81 E5 8F 91 E7 94 9F  .防..乱..码..发..生..
0000000000001FE0  EF BC 81 00 00 00 00 00  E5 8F 8C E8 BE B9 E5 8D  ！ ........双..边...
0000000000001FF0  8F E8 AE AE 33 2E 30 E5  AE A2 E6 88 B7 E7 AB AF  .议..3.0客..户..端..
0000000000002000  E7 8E B0 E4 BB B7 E5 8F  AA E9 9C 80 E8 A6 81 EF  现..价..只..需..要...
0000000000002010  BF A5 39 39 39 39 39 E5  85 83 EF BC 81 E8 B4 AD  ..99999元..！ ..购..
0000000000002020  E4 B9 B0 E8 AF B7 E8 AE  BF E9 97 AE 68 74 74 70  买..请..访..问..http
0000000000002030  3A 2F 2F 61 6C 69 70 61  79 2E 63 6F 6D 2F 78 69  ://alipay.com/xi
0000000000002040  61 6F 6C 61 6E 6C 61 6E  00 00 00 00 00 00 00 00  aolanlan........
0000000000002050  E4 B8 8E E6 9C 8D E5 8A  A1 E7 AB AF E7 9A 84 E9  与..服..务..端..的...
0000000000002060  80 9A E4 BF A1 E5 BB BA  E7 AB 8B E6 88 90 E5 8A  ..信..建..立..成...
0000000000002070  9F EF BC 81 E5 BC 80 E5  A7 8B E9 80 9A E4 BF A1  .！ ..开..始..通..信..
0000000000002080  EF BC 81 3E 3E 3E 3E 3E  3E 3E 3E 3E 3E 3E 3E 3E  ！ ..>>>>>>>>>>>>>>
0000000000002090  3E 3E 3E 3E 3E 3E 3E 3E  00 00 00 00 00 00 00 00  >>>>>>>>........
00000000000020A0  08 EE FF FF 88 ED FF FF  08 ED FF FF 60 EC FF FF  ............`...
00000000000020B0  C0 EE FF FF 00 00 00 00  00 00 00 00 00 00 70 40  ..............p@
```

seg000:0000000000002127	00000014	C	!\"#$%&'()*+,-./0123
seg000:0000000000002140	00000040	C	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
seg000:000000000000225F	00000006	C	;*3$\"

在string栏里，看到了函数，大概意思好像是，检查堆栈，随机分配，输入，字符串总和，字符串长度，输出，复制输出，重新分配，_cxa_finalize这个函数肯定有特殊的含义。不知道是冲洗还是覆盖然后爆flag，不是很懂。程序给出四个选择，1、new2、del3、edit4、show，在想是不是跟那个页面有关系？肯定要自己写代码的，知道考点的话，应该可以试着写写。

seg000:0000000000001D44	0000001D	C	Content length toooooo long!

这句话好像有点问题，不知道是不是要搞个栈溢出还是啥？尴尬，考点是啥啊！攻破系统的话不就是那么几种方式？比如栈溢出。

我单方面宣布我王富贵除了没刷crypto和reverse的题，但有刷web、pwn、misc的题，正式入门ctf！前路漫漫，且刷且珍惜！

最后，以小时候经常看的恰同学少年里的毛嗲嗲结尾~

啊对了，线上的比赛是结束了，线下的还没有，或者说，将一直继续，毕竟，人嘛！与自己比赛其乐无穷~不过还是很不爽，毕竟没拿到flag没达到自己想要的效果。

下面这段话送给那群反社会人格：

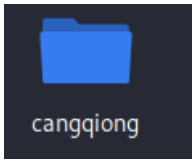
我凭自学走到了今天，不说计算机，就说ctf，在没买资料没找老师没报班的情况下，就凭着自己做题琢磨，就一个星期时间，就能做到这样，以后有好的资料好的老师再加上我自己愿意学愿意钻研，又能达到什么样的高度，相信不用我多说吧！更何况我一直都说，我也不知道自己的极限在哪里？啊对了，那女的也是真恶心，说什么我写的代码啊成果啊都是你的。什么你的你的，你谁啊！死人还想抢成果？为什么不先掂量掂量自己几斤几量？自诩的天才就真把自己当天才了呗！哦对了，我打算写点自己的代码，你能从我这里抢走一个函数试试？对了，不仅抢不走，以前那些你拿着我的想法在外面装13的，我也要一点一点悉数夺回，不用试试，是时机到了，懂？不信命？恶有善报体质？凭脸就能有很多人擦屁股？天才少女？我并没做错什么只是单纯的嫉妒所以就要毁掉我？啧~我倒要看看，其他人是觉得你的命重要呢还是他自己的命重要？不要你觉得，要他们自己觉得，不是在这种无事情况下的回答，而是那种真正死到临头的真情实意的回答，那个时候，你大概就能明白，命运馈赠的礼物早已暗中标好价格的真实含义了吧！再说句不好听的，等我以后实力越来越强，你会明白，你的上限不过是我的下限，还是我随随便便就能达到的那种，不信，擦亮眼睛看着就好。

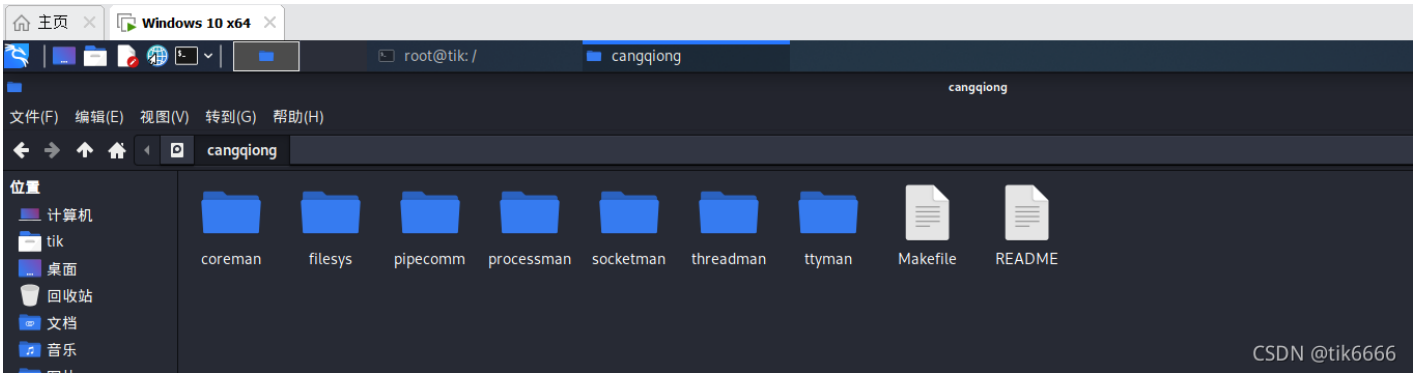
11.15

大家应该都知道为什么黑服务器必须要用php吧！因为服务器能解析php代码，或者说php代码能在服务器里运行，所以，php代码是我们黑进服务器的关键，asp代码同理。至于玩pwn的时候，c语言和汇编语言和二进制同理。

如果你想在实战中取得什么东西，自己造工具是最好的办法，不一定要最牛逼，但是适合自己就行，大概这样。

哦对了，最近要开始写我苍穹系统的代码了，所以，可能不会整天学ctf，但是还是会刷题继续学习。





SSSSSSSS，这是 我的 自研系统，你敢从我这里拿走一个函数试试？既然你敢这么不要脸，那我就敢把你脸皮给你撕了！ 懂？

关于系统内核的想法

11.20

我知乎被禁言了，因为我不友善，我王富贵需要友善这玩意儿？除非你是个好人（最起码心智健全、三观正常）或者你是个好人咱俩还算投缘。

麻了，真的麻了，这几天在整内核代码，昨晚在某扣群里跟人疯狂对线，**以一敌百，舌战群儒，**啧，就是结局有点不太光彩，貌似被人盗号了，啧，没事儿，我现在有点忙，等过了这阵子，肯定会找那些玩意儿要个说法。不过昨晚的对线事件，唯一的好处就是让我意识到了自己能摆的上台面的成果寥寥无几甚至可以称之为“没有"（不是说真的没有成果，毕竟课后习题C代码和几百行的系统内核代码还是写出来了的，只是我自己不满意而已），啊垃圾啊！尤其是对现阶段的自己有了新的认识，不过在努力搞成果，希望能做出一点小小的成绩吧！让自己满意就好。

至于系统内核，真不是我自夸啊！那些大佬们确实厉害，写的代码也是，respect！但是我觉得我可能在系统内核这一块有自己的想法吧！也许以后有幸搞芯片，从底层设计开始，会显现出来，这样子就海阔凭鱼跃，天高任鸟飞了，想咋来就咋来，不过当然是以性能和效率为主，以及，尽可能的大道至简吧！也许会创造出一个不一样的规则或者计算机世界，maybe啦！不过想想就觉得还挺开心的，嘿嘿！毕竟我还没开始做呢！还在很初级很初级的阶段。不过在写代码的过程中有什么好的想法或者思路，我自己会注意一下，以备后面的不时之需。

哦，btw，反正不管怎么样，笑到最后的一定是我，完全不可能是其他人，一丝头发缝的可能性都没有！大概这样。

话说你们这么喜欢看我碎碎念的嘛？我感觉我写的这些，都很废话啊！没啥干货，好吧！whatever！溜了溜了~

11.21

真是不得劲儿啊！我王富贵学计算机这么久，还从未遇到过如此不得劲的时候，哪怕是之前学系统内核，也是被打击打击一段时间，然后爬起来继续学，然后学的还算好吧！最起码看懂了。

但是呢，现在这个阶段是真的，太不得劲了，真心话，就是那种你干点啥其他的，哪怕你在休息在看视频娱乐在放松，你总觉得心里面挂着点啥，那种不上不下的感觉，真是让人无语。想写点不一样的东西，但是谈何容易，头都给你秃掉！**知道我为什么前几天去剪了个板寸吗？这，就是先见之明！复制粘贴很容易，但是不会让你成为创造家，那是做题家的行为。**

不过有在继续努力！好好吃饭好好休息好好思考好好琢磨，毕竟以后这样的阶段还多着呢！耐心、自信心、毅力、恒心就很重要了，当然了，最重要的是运气和灵感，**有跟别人不一样的东西，你才能做出和别人不一样的东西，**大概这样。

就这么跟你们说吧！现在的情况呢，打个比方就是，一栋建筑，它的功能是用来做学校或者食堂或者其他，它的整体大小、架构、房梁、地基等等都给你做好了，包括墙面啊屋顶啊承重啊等等，你呢，就是个装修工，你再怎么装修，也改变不了这栋房子的使用以及功能，你说你不做食堂了，你就要用来做商业楼，这不合理吧！除非你拆了重建，这样我解释的够清楚了吧！哦对了，为啥我要说这么多，因为说了又如何？反正是我脑子里想出来的东西，又不是你们想出来的，更何况，想是一回事，做又是另一回事，肯定也不止我一个人想做出牛逼的芯片吧！

等我把这事儿想明白，底气和实践妥妥的够了之后，就要向你们（fanshehui）宣战了，我有老多事儿老多话了想对你们做和说了，懂？

以前的我认为，最难的是想到，毕竟你得先想到才能做，后面，当我能想到并能付诸行动去实施的时候，发现，其实最难的是实现，尤其是让结果达到自己的预期，也许会经过很多次挫折和失败，但是永远不能停止自己前进的步伐，希望自己这辈子牢记这一点，大概这样。

刚刚意识到，旧瓶也是可以装新酒的，当然了，如果时间精力充裕，还是自己从底层造起更好一些，但是现在条件不太具备，我有点急着出成果。比如同样一个遍历目录下所有文件的功能，不同的人写出来的代码各不相同，最后的效果也不一样，还是挺能看出一个人的代码水平和思维的，这样我就比较放心了，敞开膀子肝就完事了，大概这样。

看了三体（视频版），做人当作云天明，热血忠义，又冷峻无情，英勇果敢又忍辱负重，逻辑也很不错，总之，我自己本身比较欣赏那种杀伐果决的人，有温度，更有风度，但是打起架来做起决策来也能毫不手软、说一不二、绝决到冷酷，还不错。

目前为止，唯一的心愿是，在实现阶段性成果的路上，将自己的技能点使用的越来越熟练，毕竟也才一年多一点，准确的是，天赋技能点点了也才九个月不到，中间还划水摸鱼了三个月，确实，不太熟练也很正常，时间吧！随着时间推移，会越来越熟练的，我坚信。

人类的残酷与宇宙的残酷相比，不值一提。以及，人类目前的科技水平，真的差的太远了。以及尽管我在这个星球上碰到了不好的人和事，但是，我还是喜欢这个蓝色星球的，毕竟，是我需要这个星球，而不是这个星球需要我。

在想，也许智子会不会早已派人潜入地球，挑选好身份，从而扼杀地球科学发展又不引起人类怀疑？

写代码的都知道，指甲一长敲键盘是真的不爽，所以，常备指甲刀长剪指甲，以及希望自己对得起那件格子衫（个人想法，其他人勿对号入座）。

11.23

免费的东西都很贵，以及，从古至今，高风险与高收益一直都是并存的，高风险意味着高收益，反之，高收益也意味着高风险，永远别觉得自己一定能在收获高收益之后能不遭受任何高风险从而全身而退，不要赌，不要赌，不要赌！

不好意思，是我自己误会了，学习期确确实实是六个月每天八小时左右没错，多点时间少点时间什么的都没所谓了，但是成果期是真的要很久很久很久，而且在成果期期间，你还会不停的接触学习新的知识，也算是学习期加成果期的融合了，不如就把前期的学习期叫做基础期好了，这么说来，时间还是过去了挺久的，嗯，小生不才啊！总之，会继续努力的。

基础期的学习记录：大概，学了门C语言，学了点汇编，学了点工具，学了点数据结构，算法导论，计算机操作原理，学了点unix/linux系统内核，学了点kali，打了点CTF比赛，学了点前端html css php mysql，有的学了点是真的学了点，有的学了点是按需学习，但是多多少少也是懂了点，会继续深入，继续学无止境，毕竟，**计算机又不是一门你花半年就能学会学完的学科，它是要花一辈子，你才能勉强称得上熟练的东西。**

11.24

最近要做一件很重要的事情，具体是什么，得看情况了。

在做这件事情的过程中，我也不由得思考，自己到底是个什么水平？跟别人比起来竞争力如何？又能做到何种地步达到何种高度？等等，都是需要我不停思考的东西，我需要得到答案，哪怕答案不够好，也没关系，因为我知道自己会继续努力，永不停止前进的步伐。

加油啊tik要继续努力，要更努力才行！

11.27

如果有条件的话，明年希望能进入芯片行业工作呀！反正我学东西学的快，又肯下功夫努力，还有决心有毅力有自信，希望能有所小小成就吧！哦对了，物理学习也是必不可少的，毕竟是对世界本质的探索，也许就发现了什么了不得的事情呢！Maybe吧！

加油哦！Tik！

12.2

最近在找工作，计算机相关，各位要是觉得看的还不过瘾，欢迎去我的知乎瞧瞧，下载知乎，搜索TiK2KK，也许会让你觉得更“惊喜”~

知乎 首页 会员 发现 等你来答 接受不了孩子平庸怎么办 提问

编辑封面图片

TiK2KK 未来科学家，达则兼济天下，目标星辰大海(星辰安全团队队长)

所在行业

个人简介 这世上我只听神哥和脑哥（想做MM豆彩虹客）穿的越粉，打架越狠，不解释。不知道什么是天才，只知道唯有努力才能换想要的

收起详细资料

编辑个人资料

动态 回答 362 视频 0 提问 17 文章 25 专栏 0 想法 148 收藏 2 关注

我的动态

发布了想法 12-01 18:58

TiK2KK

创作中心 Lv 6 草稿箱 (5)

情感树洞

情感树洞