攻防世界 Reverse高手进阶区 2分题 SignIn

原创

思源湖的鱼 于 2021-01-07 14:57:19 发布 192 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse rsa

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112310546

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

本篇是SignIn的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

PE查壳

扔进IDA

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char v4; // [rsp+0h] [rbp-4A0h]
  char v5; // [rsp+10h] [rbp-490h]
  char v6; // [rsp+20h] [rbp-480h]
  char v7; // [rsp+30h] [rbp-470h]
  char v8; // [rsp+40h] [rbp-460h]
  char v9; // [rsp+B0h] [rbp-3F0h]
  unsigned __int64 v10; // [rsp+498h] [rbp-8h]

  v10 = __readfsqword(0x28u);
  puts("[sign in]");
  printf("[input your flag]: ", a2);
  __isoc99_scanf("%99s", &v8);
  sub_96A(&v8, &v9);
  __gmpz_init_set_str(&v7, "ad939ff59f6e70bcbfad406f2494993757eee98b91bc244184a377520d06fc35", 16LL);
  __gmpz_init_set_str(&v6, &v9, 16LL);
  __gmpz_init_set_str(&v4, "10346103590081691412139010129904904441395040517371217043416168653987816098454 9", 10LL);
  __gmpz_init_set_str(&v5, "65537", 10LL);
  __gmpz_powm(&v6, &v6, &v5, &v4);
  if ( (unsigned int)__gmpz_cmp(&v6, &v7) )
    puts("GG!");
  else
    puts("TTTTTTTTTql!");
  return 0LL;
}
```



```
size_t __fastcall sub_96A(const char *a1, __int64 a2)
{
  size_t result; // rax
  int v3; // [rsp+18h] [rbp-18h]
  int i; // [rsp+1Ch] [rbp-14h]

  v3 = 0;
  for ( i = 0; ; i += 2 )
  {
    result = strlen(a1);
    if ( v3 >= result )
      break;
    *(_BYTE *)(a2 + i) = byte_202010[(char)(a1[v3] >> 4)];
    *(_BYTE *)(a2 + i + 1LL) = byte_202010[a1[v3++] & 0xF];
  }
  return result;
}
```



```
.data:0000000000202010 byte_202010     db 30h, 31h, 32h, 33h, 34h, 35h, 36h, 37h, 38h, 39h, 61h
.data:0000000000202010                                         ; DATA XREF: sub_96A+47↑o
.data:0000000000202010                                         ; sub_96A+7F↑o
.data:0000000000202010                 db 62h, 63h, 64h, 65h, 66h
.data:0000000000202010 _data           ends
```

先查了下几个函数

```
mpz_powm(op1,op2,op3,op4);    //求幂模函数 即 op1=op2^op3 mod op4;
mpz_init_set_str(b, "200000", 10);  //即 b=200000，十进制
mpz_cmp(b, c);        //b 大于 c，返回 1；b 等于 c，返回 0；b 小于 c，返回-1*/
```

然后看看96A函数

复现一下

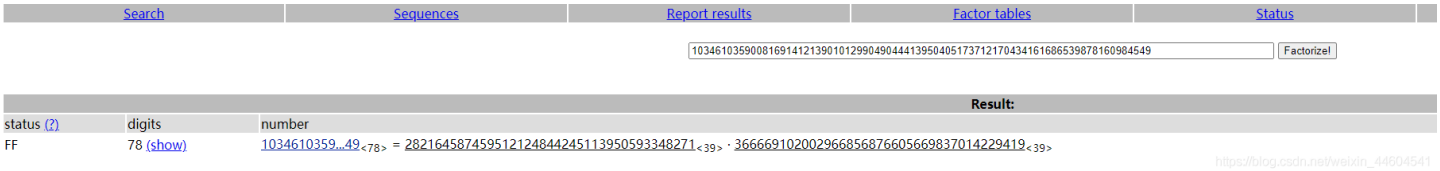
发现是将一串输入转化为 16 进制 ASCII 码的形式

再看看main

是个RSA啊

那就先大数分解

http://www.factordb.com/index.php



然后掏出脚本就是了

```
import libnum
from Crypto.Util.number import long_to_bytes

q = 282164587459512124844245113950593348271
p = 366669102002966856876605669837014229419
e = 65537
c = 0xad939ff59f6e70bcbfad406f2494993757eee98b91bc244184a377520d06fc35
n = 10346103590081691412139010129904904441395040517371217043416168653987816098454 9

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)   # m 的十进制形式
string = long_to_bytes(m)  # m明文
print(string)
```

得到flag: `suctf{Pwn_@_hundred_years}`

结语

其实还是个rsa