HGAME WEEK3 WP

——EkkoSonya

RE

FAKE

被弄懵的一题 刻苦铭心

1.将其拖入ida后会有警示，并没有注意进入后看到main函数 首先是输入36长度的字符串后存入双字节中进入判断函数

2.进入判断函数 乍一看 好家伙 第一次见这么长的 f5时一开始不知为什么还没用导致还卡着，后来成功后看了下是36个方程组求解啥的(主要问了下出题人，"果然"证实了我的猜想)不假思索的进行求解 很傻的记录(纯手打)把所有系数记录下来后构成系数矩阵 将其进行线性求解(期间还有几个系数打错，对照了几遍) 好家伙 刚开始出来可激动

```
[104. 103.  97. 109. 101. 123.  64.  95.  70.  65.  75.  69.  95. 102.
 108.  97. 103.  33.  45. 100. 111.  95.  89.  48. 117.  95. 107. 110.
 111. 119.  95.  83.  77.  67.  63. 125.]
```

结果将其ascii码得出来后 hgame{@_FAKE_flag!-do_Y0u_know_SMC?}

原来这才是题目FAKE的含义 TAT

3.emm，这是在星期五得出来的，查询smc(self-Modifying Code)后知道是一种防止静态调试的技术，好像是在真正运行的时候会自动对某段代码自修改 TAT

4.重新研究后只发现几点

(1)真正运行的时候输入假flag是wrong的 但从debug调试结果又是真的 不知道咋回事

(2) 在ida看别的函数中发现一个函数会对原来判断的函数修改

```
1  __int64 __usercall sub_40099B@<rax>(__int64 a1@<rbp>)
2  {
3    __int64 result; // rax
4    unsigned int i; // [rsp-Ch] [rbp-Ch]
5
6    __asm { endbr64 }
7    sub_4010E0();
8    for ( i = 0; ; ++i )
9    {
10     result = i;
11     if ( i > 0x43E )
12       break;
13     *((_BYTE *)sub_401216 + (signed int)i) ^= byte_409080[i];
14   }
15   return result;
16 }
```

但是试过让其运行时并没有找到关联 TAT

Crypto

LikiPrime

还是上周白给RSA 套用上周脚本 就得到flag

```
570893384134068466208821377109160724312908349444
hgame{Mers3nne~Pr!Me^re4l1y_s0+5O-li7tle!}
```

HappyNewYear

看了题目 群发 提示了小明文广播攻击

(最开始只注意到群发 就没发现并不是所有都是群发 只有个别是群发)

于是最笨的方法手动组合 一开始是三三组合 四四组合没往 两两组合方向想 都得不出来正确答案

最后得到

```
Hello Liki4:

I am afraid that there are too many blessings on the 30th night, you will not see my greetings,
I am afraid that the firecrackers in the first grade are too noisy, you will not hear my blessings,

@ind3r~YOu^9ot=i7}
```


```
Hello Liki4:

I am afraid that there are too many blessings on the 30th night, you will not see my greetings,
I am afraid that the firecrackers in the first grade are too noisy, you will not hear my blessings,

@ind3r~YOu^9ot=i7}
```


Web

Forgetful

通过题目提示和搜索引擎查询

进行尝试{{2+4}} 发现结果返回是 6

进一步尝试 {{"".**class**.**bases**[0].**subclasses**()}}找到<class 'os._wrap_close'>的位置后 进行下一步尝试

再进行 {{"".**class**.**bases**[0].**subclasses**()[117].**init**.**globals**"popen".read() }} 后却得到一个提示

Stop!!!

卡了一会儿

尝试 {{"".**class**.**bases**[0].**subclasses**()[117].**init**.**globals**"popen".read() }}发现成功导出base64加密的flag

解码后得到flag

Base64 编码或解码的结果:

hgame{h0w_4bou7+L3arn!ng~PythOn^Now?}