HGAME 2022 Week2writeup by 给爷点一杯奶茶

笔记本:	My Notebook		
创建时间:	2022/2/4 16:33	**更新时间:**	2022/2/4 16:46
作者:	cjx		
URL:	https://hgame.vidar.club/#/challenge/list		

HGAME 2022 Week2writeup by 给爷点一杯奶茶

WEB

webpack

webpack漏洞，vue文件泄露，chrome看源码即可看到flag
base64解码两次即可得到flag

CRYPTO

RSA Attack

已知enc求明文
写个脚本

```python
from libnum import n2s,s2n

def gcd(a, b):   #求最大公约数
    if a < b:
        a, b = b, a
    while b != 0:
        temp = a % b
        a = b
        b = temp
    return a
def egcd(a,b):          #扩展欧几里得算法
    if a==0:
        return  (b,0,1)
    else:
        g,y,x=egcd(b%a,a)
        return (g,x-(b//a)*y,y)

def modinv(a,m):
    g,x,y=egcd(a,m)
    if g!=1:
        raise Exception('modular inverse does not exist')
    else:
        return x%m
if __name__ == '__main__':
    p =715800347513314032483037
    q =978782023871716954857211
    e = 65537
    d =modinv(e,(p-1)*(q-1))
    c =122622425510870177715177368049049966519567512708
    n =p*q
    m = pow(c,d,n)
    print(n2s(m))
```

RSA Attack 2

分别考察共模攻击、共素数攻击、小指数公钥攻击
分别写个小脚本

```python
from libnum import n2s, s2n
from gmpy2 import invert

#扩展欧几里得算法
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)



n = 188195091881062303634448133504681620561644346427299
e1 = 2519901323
c1 = 32307797262255448725314411690093070720737545787612
e2 = 3676335737
c2 = 94081859562227916143983671964170784679029465088877
s = egcd(e1, e2)
s1 = s[1]
s2 = s[2]
# 求模反元素
if s1 < 0:
    s1 = - s1
    c1 = invert(c1, n)
elif s2 < 0:
    s2 = - s2
    c2 = invert(c2, n)

m = pow(c1, s1, n) * pow(c2, s2, n) % n
sb=n2s(int(m))
print(sb)
```

```
n11 = gmpy2.mpz(n1)
n22 = gmpy2.mpz(n2)
prime2 = gmpy2.gcd(n11, n22)
print(prime2)
prime1 = n11 // prime2
print(prime1)
prime3 = n22 // prime2

l_n1 = (prime1 - 1) * (prime2 - 1)
l_n2 = (prime2 - 1) * (prime3 - 1)

d1 = gmpy2.invert(e, l_n1)
d2 = gmpy2.invert(e, l_n2)

m1 = pow(int(c1), d1, int(n1))
m2 = pow(int(c2), d2, int(n2))

d1 = gmpy2.invert(e, l_n1)
d2 = gmpy2.invert(e, l_n2)

r1 = libnum.n2s(int(m1))
print(r1)
```

```
from gmpy2 import iroot
import libnum
e = 7
n = 14157878492255346300993349653813018105991884577
c = 10262871020519116406312674685238364023536657844

k = 0
while 1:
    res = iroot(c+k*n,e)  #c+k*n 开3次方根 能开3次方
    if(res[1] == True):
        print(libnum.n2s(int(res[0]))) #转为字符串
        break
    k=k+1
```