HGAME 2022 Week2 writeup by Northward

[TOC]

REVERSE

WEB

webpack-engine

在开发者工具中可以找到Fl4g*1*sher3.vue文件，打开发现base64编码的flag

Pokemon

提示是sql注入，先试着用sqlmap寻找/index.php?id=1是否存在注入点，发现了一处302。

之后改用bp测试几次后发现id=-1时会返回302，关注重定向，来到/error.php?code=404页面，按照hint，通过双写、=改like、空格改回车来构造查询语句绕过waf 通过information_schema库，分别得到库名、表明、列名，得到flag

```
> /error.php?code=404%0aununionion%0aselselectect%0a1,group_concat(table_name)%0afrfromom%0ainfoorrmation_schema.tables%0awhwhereere%0at
```

MISC

CRYPTO

RSA Attack

通过factordb.com这个网站可以直接通过n分解出pq，之后利用脚本可解得flag

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

RSA Attack2

三个task应该是分别利用模不互素、小明文、共模攻击三种方法求解，但因为可以直接从n分解出pq，所以我前两关就是直接强解了，task3解题脚本如下

```
from libnum import *
from gmpy2 import invert
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)

def main():
  n =
  c1 =
  c2 =
  e1 =
  e2 =
  s = egcd(e1, e2)
```

```
  s1 = s[1]
  s2 = s[2]
  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
  print(n2s(m))

if __name__ == '__main__':
  main()
```

IoT