Write UP Perlombaan Capture The Flag Hology UB 2.0

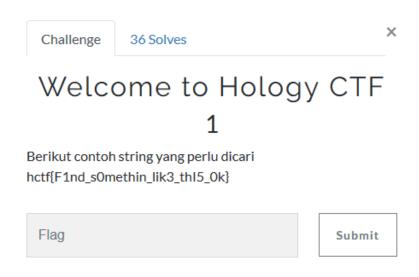


Speedraw

M.Hendro Junawarko M.Nur Hasan Aprilian Dicky Hermawan

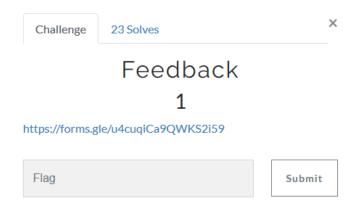
Universitas Teknokrat Indonesia

Misc



Hanya perlu copy paste flag yang sudah disediakan.

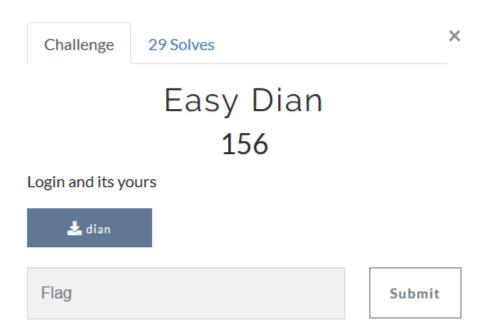
Flag: hctf{F1nd_s0methin_lik3_thI5_0k}



Klik link google form yang sudah disediakan oleh panitia lalu isi beberapa pertanyaan kemudian submit maka anda akan mendapatkan flagnya.

 $Flag: \textbf{hctf} \{ \textbf{thank_you_very_much_hahahahahahaha} \}$

Reverse



Diberikan file ELF 64 bit dimana meminta sebuah inputan

lakukan analisis buka dengan IDA Pro

```
int64 fastcall main( int64 a1, char **a2, char **a3)
 2 {
 3
     char *s; // [sp+70h] [bp-10h]@1
 4
     s = (char *)calloc(1uLL, 0x3EuLL);
 6
    puts("Masukkan kode: ");
 7
     fgets(s, 62, stdin);
 8
           ftch' != *( DWORD *)s
          't3L{' != *((_DWORD *)s + 1)
 9
10
                  != *((_DWORD *)s + 2)
11
           NR4' != *((_DWORD *)s +
          'īdn3'
12
                  != *(( DWORD *)s +
13
                  + *((_DWORD *)s +
14
          '1s_5' != *((_DWORD *)s + 6)
          'ylpm' != *((_DWORD *)s + 7)
'ba6_' != *((_DWORD *)s + 8)
15
16
       || '}09f' != *((_DWORD *)s + 9)
17
18
       || 10 != *((_DWORD *)s + 10) )
19
20
       printf("Whoops, https://youtu.be/rgrdCIYXSjM", 62LL, a2);
21
22
     else
23
       puts("Selamat!!!");
24
25
26
     return OLL;
27
```

terlihat pada pseudocode diatas terdapat kondisi yang menampilkan string yang merupakan flag, reverse setiap string tersebut dan gabungkan menjadi flag utuh

 $flag: hctf\{L3ts_le4RN_3ndianeS5_s1mply_6abf90\}$

Cryptography

ありあと



Disaat sensei ari sudah berkata tugas kriptografi. 9 dari 10 Mahasiswa akan mengerjakan tugas mata kuliah lain.

🕹 old.odt	
Flag	Submit

diberikan sebuah file document odt

PWFU-LZ-AW-DI DYJWGZPZF YOZZF LIHFUQHZ WFLWP AQJY PYJLZAQWDI. OIF AWF EZJI AIFU-LH-SH ZEZSZQ GZFYDAZQZF OIDAWFZSIZM JZEYF GZLZQ EZJI EYDZP AIFLZJZ. MCZF SIHFU IEYFLIP EYFUZF ZJNZ EZDZJ. MYEZFUPZF NZFU-CI-MI-MZ AIMZ AYJZJLI QNZFU CIMYMZ ZSIZM CIPJZDZCZJEQZFZ, ZLZW AIMZ GWSZ QNZFU GYJFZQ DYFOZEI JZOZ EI PYEWZFNZ MZDZ-MZDZ DYFWJWL AZAZE LZFZQ OZCI EZF MYJZL PZFEZ, LHPHQ ZJNZ EZDZJ ZEZSZQ ZFZP AJZCIOZNZ EZJI MYHJZFU JZPMZMZ GYJYDGWZF AYJFZDZ YFEZFU MZMDIFLZGWJZ. OZEI, ZJNZ EZDZJ ZEZSZQ PZPZP LIJI MYPZSIUWM ZFUPZL JZEYF DYFWJWL PJHFIP LIHFUPHP EI ZLZM, JZEYF GZLZQ ZEZSZQ GWLJZ AQJY PYJLZAQWDI, MYEZFUPZF MCZF SIHFU ZEZSZQ GWLJZ QNZFU CIMYMZ EZJI MYHJZFU MYSIJ AYJEZJZQ LIHFUPHP. PIMZQ IFI LYJPYMZF SYAIQ DZMWP EZJIGZEZ WJZIZF AZAZE EZF XYJMI MYJZL.

 ${\tt QRLT\{MHDYLIDYM_CY_HFSN_FYYE_LH_LQIFP_RJYZLIXY_TAZREYTVBNW\}}$

MYSZFOWLFNZ EIPIMZQPZF GWSZ, MYLYSZQ PYPZSZQZF PWFU-LZ-AW-DI, DZOZGZQIL GWF DYFOZEI AZCZQZF EYDZP. AYPZM PYJZOZZF AYMZJ IFI PYDWEIZF EIGYJIFLZQ HSYQ FNHH SZN CZ, MYHJZFU LIHFUQHZ DWMSID MYAZUZI AWGZLI. GZEZ LZQWF 1486FNHH SZN CZ LYCZM PZJYFZ WFOWP JZMZ GYFEWEWP GJIAWDI. DZPZ, OIF AWF GWF DYFUZFUPZL IGZJFNZ, NZILW GZ-AW-LZ-SZ, DYFZFLW PWFU-LZ-AW-DI, MYAZUZI AWGZLI AZJW.

LHPHQ GZ-AW-LZ-SZ IEYFLIP EYFUZF GJZAQW FZLQZ UIJIFEJZCZJEQZFZ ZSIZM ENZQ JZFZCIOZNZ EZSZD GJZMZMLI OINW 1486. OZEI, DYFWJWL AYJILZ LIHFUPHP LYJMYAWL, ENZQ JZFZCIOZNZ ZSIZM AQZLZJZ CIOZNZ ZEZSZQ MZWEZJZ IGZJ MYPZSIUWM AWGZLI AZCZQZF JZEYF GZLZQ. EYFUZF PZLZ SZIF, AQJZ CIOZNZ ZEZSZQ DYFZFLW AQJY PYJLZAQWDI DYFWJWL PJHFIP LIHFUPHP. PYJWFLWQZF DZOZGZQIL[MWFLIFU | MWFLIFU MWDAYJ]

GYJIMLICZ JWFLWQFNZ PYJZOZZF DZOZGZQIL NZFU AYJGWMZL EI LJHCWSZF, DHOHPYJLH EINZPIFI LYJOZEI GZFZ I ZOWF 1478 FYFIJZF IZOZ I YJZPOJIFNZ AJZCIOZNZ X OZS IFI MYAZIJZIDZFZ I YJI WSIM FZSZD MYJZI

diketahui enkripsi tersebut menggunakan substitution cipher, mencoba pada https://quipqiup.com/

dilakukan pemetaan pada setiap huruf mengacu pada format flag yaitu hctf{ .

Puzzle: QRLT{MHDYLIDYM CY HFSN FYYE LH LQIFP RJYZLIXY TAZREYTVBNW} Clues: For example G=R QVW=THE q=h r=c l=t t=f 0 -2.150 HCTF{SOMETIMES_WE_ONLY_NEED_TO_THING_CREATIVE_FBACDEFJZYK}

Didapat flag nya dan coba submit ternyata masih salah, flag pada format awal sudah benar dan tinggal akhir nya saja yang salah, dilakukan pemetaan huruf selanjutnya

```
Puzzle:

QRLT{MHDYLIDYM CY HFSN FYYE LH LQIFP RJYZLIXY TAZREYTVBNW}

Clues: For example G=R QVW=THE

q=h r=c l=t t=f m=s h=o d=m y=e l=t i=i c=w y=e f=n e=d q=h p=g r=c j=r z=a x=v

0 -2.150 HCTF{SOMETIMES_WE_ONLY_NEED_TO_THING_CREATIVE_FBACDEFJZYK}
```

didapat flag yang tersisa 2 huruf lagi
hctf{sometimes_we_only_need_to_think_creative_fbacdef??yu}

lalu kami lakukan setiap pemetaan pada huruf tersebut sehingga menjadi berikut

Puzzle:

QRLT{MHDYLIDYM CY HFSN FYYE LH LQIFP RJYZLIXY TAZREYTVBNW}

q=h r=c l=t t=f m=s h=o d=m y=e l=t i=i c=w y=e f=n e=d q=h r=c j=r z=a x=v s=l w=u a=b n=y p=k u=g

SASMINTA?URA. JADI, ARYA DAMAR ADALAH KAKAK TIRI SEKALIGUS AYAH ANGKAT RADEN ?ATAH. MENUR RADEN ?ATAH ADALAH ?UTRA BHRE KERTABHUMI, SEDANGKAN SWAN LIONG ADALAH ?UTRA HYANG WISESA TIONGKOK. KISAH INI TERKESAN LEBIH MASUK AKAL DARI?ADA URAIAN VERSI BABAD DAN SERAT. HCTF{SOMETIMES_WE_ONLY_NEED_TO_THINK_CREATIVE_FBACDEF??YU} SELANJUTNYA DIKISAHKAN ?ULA, S MAJA?AHIT ?UN MENJADI BAWAHAN DEMAK. BEKAS KERAJAAN BESAR INI KEMUDIAN DI?ERINTAH OLEH NY MUSLIM SEBAGAI BU?ATI. ?ADA TAHUN 1486NYOO LAY WA TEWAS KARENA UNJUK RASA ?ENDUDUK ?RIBUM I?ARNYA, YAITU ?A-BU-TA-LA, MENANTU KUNG-TA-BU-MI, SEBAGAI BU?ATI BARU. TOKOH ?A-BU-TA-LA GIRINDRAWARDHANA ALIAS DYAH RANAWIJAYA DALAM ?RASASTI JIYU 1486. JADI, MENURUT BERITA TIO

diketahui tersisa huruf yang bellum dilakukan substitusi yaitu Q, X, Z

lalu kami coba tebak dengan huruf yang tersisa tersebut dan flag didapat pada

flag: hctf{sometimes we only need to think creative fbacdefxzyu}

Forensics

Green Milky way

diberkan file alice.zip dan sebuah enc.pyc, dimana file zip berisi potongan gambar yang dipecah.

buka file enc.pyc dengan uncompyle6 didapat source code berikut

```
uncompyle6 version 3.3.1
  Python bytecode 3.7 (3394)
 Decompiled from: Python 2.7.16 (default, Apr 6 2019, 01:42:57)
 [GCC 8.3.0]
 Embedded file name: enc.py
 Size of source mod 2**32: 487 bytes
from PIL import Image
def crop(image path, coords, saved location):
    image_obj = Image.open(image_path)
    cropped image = image obj.crop(coords)
    cropped image.save(saved location)
    cropped image.show()
                                    Forensics
if name == ' main ':
    l Gren Milky way
    for k in range(20):
      dibirkan@ile alice.zip dan sebuah enc.pyc
         for i in range(20):
             image = 'Done.png'
name = 'foto' + str(k) + '_' + str(i) + '.png'
crop(image, (j, l, j + 80, l + 80), name)
             i += 80
         1 += 80
 okay decompiling enc.pyc
```

disini saya mencoba dengan menggunakan tools linux yaitu montage untuk menggabungkan potongan gambar tersebut

```
montage -mode concatenate -title 50x50 $(ls -v *) flag.jpg
```



didapat gambar utuh yang berisi sebuah flag.jpg

 $flag: hctf\{l3Ts_Mak3_a_Scr1pt_f0r_Thi5_ChalLange\}$

Eyes N Closed

Diberikan Sebuah file crt text berisi nilai rsa tersebut, diketahui nilai c n dan e seperti ini

c =

822771793134222725965388057340774806017683102992549844704514234955 01149986396526959207256445320568510116948563902704353

n =

227010481295437363334259960947493668895875336466084780038173258247 009162675779735389791151574049166747880487470296548479

e = 31337

lakukan faktor di http://factordb.com/ untuk mendapat nilai p dan q

 $p = 327414555693498015751146303749141488063642403240171463406883 \\ q = 693342667110830181197325401899700641361965863127336680673013$

```
import gmpy2

def num_to_str(num):
    res = ""
    while num > 0:
    res = chr(num % 256) + res
    num = num / 256
    return res

p = 327414555693498015751146303749141488063642403240171463406883
q = 693342667110830181197325401899700641361965863127336680673013
t = (p-1)*(q-1)
```

```
e = 31337

d = gmpy2.invert(e,t)

c = 822771793134222725965388057340774806017683102992549844704514234955011499863965269592

07256445320568510116948563902704353

n = 227010481295437363334259960947493668895875336466084780038173258247009162675779735389

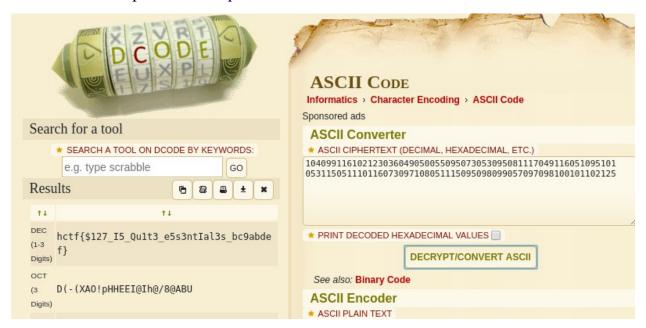
791151574049166747880487470296548479

m = pow(c,d,n)
```

jalankan dan didapat hasil berikut

```
| Table Plan | Fact Plan | Fac
```

lakukan decode pada web https://www.dcode.fr/ascii-code



 $flag: hctf \{\$127_I5_Qu1t3_e5s3ntIal3s_bc9abdef\}$