

Write Up Perlombaan Capture The Flag Hology UB 2.0



speedraw

**M.Hendro Junawarko
M.Nur Hasan Aprilian
Dicky Hermawan**

Universitas Teknokrat Indonesia

Misc

Welcome to Hology CTF

Challenge 36 Solves x

Welcome to Hology CTF

1

Berikut contoh string yang perlu dicari
hctf{F1nd_s0methin_lik3_th15_0k}

Flag

Submit

Hanya perlu copy paste flag yang sudah disediakan.
Flag : **hctf{F1nd_s0methin_lik3_th15_0k}**

Feedback

Challenge 23 Solves x

Feedback

1

<https://forms.gle/u4cuqiCa9QWKS2i59>

Flag

Submit

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

Flag : **hctf{thank_you_very_much_hahahahahahaha}**

Reverse

Easy Dian

Challenge


29 Solves

×

Easy Dian

156

Login and its yours

 dian

Flag

Submit

Diberikan file ELF 64 bit dimana program meminta sebuah inputan

```
[flintz@shadow] ~/Downloads/hology/reverse$ ./dian
Masukkan kode:
123124
Whoops, https://youtu.be/rgrdCIYXSjM [flintz@shadow] ~/Downloads/hology/reverse$
```

lakukan analisis buka dengan IDA Pro

```

1  _int64 __fastcall main(_int64 a1, char **a2, char **a3)
2  {
3      char *s; // [sp+70h] [bp-10h]@1
4
5      s = (char *)calloc(1uLL, 0x3EuLL);
6      puts("Masukkan kode: ");
7      fgets(s, 62, stdin);
8      if ( 'ftch' != *(_DWORD *)s
9          || 't3L{' != *(_DWORD *)s + 1)
10         || 'el_s' != *(_DWORD *)s + 2)
11         || '_NR4' != *(_DWORD *)s + 3)
12         || 'idn3' != *(_DWORD *)s + 4)
13         || 'Sena' != *(_DWORD *)s + 5)
14         || '1s_5' != *(_DWORD *)s + 6)
15         || 'ylpm' != *(_DWORD *)s + 7)
16         || 'ba6_' != *(_DWORD *)s + 8)
17         || '}09f' != *(_DWORD *)s + 9)
18         || 10 != *(_DWORD *)s + 10) )
19     {
20         printf("Whoops, https://youtu.be/rgrdCIYXSjM", 62LL, a2);
21     }
22     else
23     {
24         puts("Selamat!!!");
25     }
26     return 0LL;
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

Challenge

20 Solves

×

あり あと

307

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

PWPU-LZ-AW-DI DYJWGZPZF YOZZF LIHFUQHZ WFLWP AQJY PYJLZAQWDI. OIF AWF EZJI AIFU-LH-SH ZEVSZQ GZFYDAZQZF OIDAWFZSIZM JZEYF GZLZQ EZJI EYDZP AIFLZJZ. MCZF SIHFU IEYFLIP EYFUZF ZJNZ EVDZJ. MYEFZUPZF NZFU-CI-MI-MZ AIMZ AYJZJLI QNZFU CIMYMZ ZSIZM CIPJZDZCZJEQZFZ, ZLZW AIMZ GWSZ QNZFU GWJZCZCIMYMZ. PYEWZFNZ MZDZ-MZDZ GYJFZQ DYFOZEI JZQZ EI DZOZGZQIL. DYFWJWL AZAZE LZFZQ OZCI EZF MYJZL PZFEZ, LHPHQ ZJNZ EVDZJ ZEVSZQ ZFZP AJZCIZNZ EZJI MYHJZFU JZPMZM GYJYDZWZF AYJFZDZ YFEZFU MZMDIFLZGWJZ. OZEI, ZJNZ EVDZJ ZEVSZQ PZPZP LIJ MYPZSIUWM ZNZQ ZFUPZL JZEYF GZLZQ. DYFWJWL PJHFIP LIHFUPHP EI ZLZM, JZEYF GZLZQ ZEVSZQ GWLJZ AQJY PYJLZAQWDI, MYEFZUPZF MCZF SIHFU ZEVSZQ GWLJZ QNZFU CIMYMZ EZJI MYHJZFU MYSIJ AYJEZJZQ LIHFUPHP. PIMZQ IFI LYJPMZF SYAIQ DZMWP ZPZS EZJIGZEZ WJZIZF XYJMI AZAZE EZF MYJZL.

QRLT{MHDYLIIDYM_CY_HFSN_FYFE_LH_LQIFP_RJYZLIXY_TAZREYTVBNW}

MYSZFOWLFNZ EIPIMZQPZF GWSZ, MYLYSZQ PYPZSZQZF PWPU-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 GYFEWEP GJIAWDI. DZPZ, OIF AWF GWF DYFUZFUPZL IGZJFNZ, NZILW GZ-AW-LZ-SZ, DYFZFLW PWPU-LZ-AW-DI, MYAZUZI AWGZLI AZJW.

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

GYJIMLICZ JWFLWQFNZ PYJZOZZF DZOZGZQIL NZFU AYJGWMZL EI LJHCWSZF, DHOHPYJLH EINZPIFI LYJOZEI CZFZ IZOWF 1478 EYFUIZF IZQZ IYIZPOHFNZ AIZCIZNZ X QZS IFI MYAZUZIIZFZ IYH WSIM FZSZD MYIZI

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

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

Puzzle:

QRLT{MHDYLIIDYM_CY_HFSN_FYFE_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:

ORLT{MHDYLIDYM CY HFSN FYFE LH LOIFP 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_THINK_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:

ORLT{MHDYLIDYM CY HFSN FYFE LH LOIFP RJYZLIXY TAZREYTVBNW}

MYSZFOWLFNZ EIPIMZOPZF GWSZ, MYLYSZQ PYPZSZQZF PWFU-LZ-AW-DI, DZOGZQIL GWF DYFOZEI AZCZQZF EYDZP. AYI
PYDWEIZF EIGYJIFLZQ HSYQ FNHH SZN CZ, MYHJZFU LIHFUQHZ DWMSID MYAZUZI AWGZLI. GZEZ LZQWF 1486FNHH SZN
GYFEWEWP GJIAWDI. DZPZ, OIF AWF GWF DYFUZFUPZL IGZJFNZ, NZILW GZ-AW-LZ-SZ, DYFZFLW PWFU-LZ-AW-DI, MYA.
LHPHQ GZ-AW-LZ-SZ IEYFLIP EYFUZF GJZAQW FZLQZ UIJIFEJJCZJEQZFZ ZSIZM ENZO JZFZCIOZNZ EZSZD GJZMZMLI O.
AYJILZ LUFUBUB LYJMYAWL FNZG JZFZCIOZNZ ZCIZM AGZLJIZ CIOZNZ ZFZCZO MZJFJIZ ZCIZM MYDZCIZUM AWGZLI A.

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 r=c j=r z=a x=v s=l w=u a=b n=y p=k u=g

BABAD TARIK JARI DAN SERAT KARDA, TOKOH ARYA DAMAR ADALAH ANAK BIRUKATA DARI SEORANG RAK
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 belum 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_fbacdefx
zyu}**

Forensics

Green Milky way

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

```
[flintz@shadow]--[~/Downloads/alice]
$ls
foto0_0.png  foto12_17.png  foto16_13.png  foto2_0.png  foto6_0.png
foto0_10.png  foto12_18.png  foto16_14.png  foto2_10.png  foto6_10.png
foto0_11.png  foto12_19.png  foto16_15.png  foto2_11.png  foto6_11.png
foto0_12.png  foto12_1.png  foto16_16.png  foto2_12.png  foto6_12.png
foto0_13.png  foto12_2.png  foto16_17.png  foto2_13.png  foto6_13.png
foto0_14.png  foto12_3.png  foto16_18.png  foto2_14.png  foto6_14.png
foto0_15.png  foto12_4.png  foto16_19.png  foto2_15.png  foto6_15.png
foto0_16.png  foto12_5.png  foto16_1.png  foto2_16.png  foto6_16.png
foto0_17.png  foto12_6.png  foto16_2.png  foto2_17.png  foto6_17.png
foto0_18.png  foto12_7.png  foto16_3.png  foto2_18.png  foto6_18.png
foto0_19.png  foto12_8.png  foto16_4.png  foto2_19.png  foto6_19.png
foto0_1.png  foto12_9.png  foto16_5.png  foto2_1.png  foto6_1.png
foto0_2.png  foto12_10.png  foto16_6.png  foto2_2.png  foto6_2.png
foto0_3.png  foto12_11.png  foto16_7.png  foto2_3.png  foto6_3.png
foto0_4.png  foto12_12.png  foto16_8.png  foto2_4.png  foto6_4.png
foto0_5.png  foto12_13.png  foto16_9.png  foto2_5.png  foto6_5.png
foto0_6.png  foto12_14.png  foto16_10.png  foto2_6.png  foto6_6.png
foto0_7.png  foto12_15.png  foto16_11.png  foto2_7.png  foto6_7.png
foto0_8.png  foto12_16.png  foto16_12.png  foto2_8.png  foto6_8.png
foto0_9.png  foto12_17.png  foto16_13.png  foto2_9.png  foto6_9.png
```

decompile file enc.pyc dengan uncompyle6 didapat source code berikut untuk recovery gambar tersebut

```

# uncompile6 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()

if __name__ == '__main__':
    l = 0
    for k in range(20):
        for i in range(20):
            image = 'Done.png'
            name = 'foto' + str(k) + '_' + str(i) + '.png'
            crop(image, (j, l, j + 80, l + 80), name)
            j += 80
        l += 80

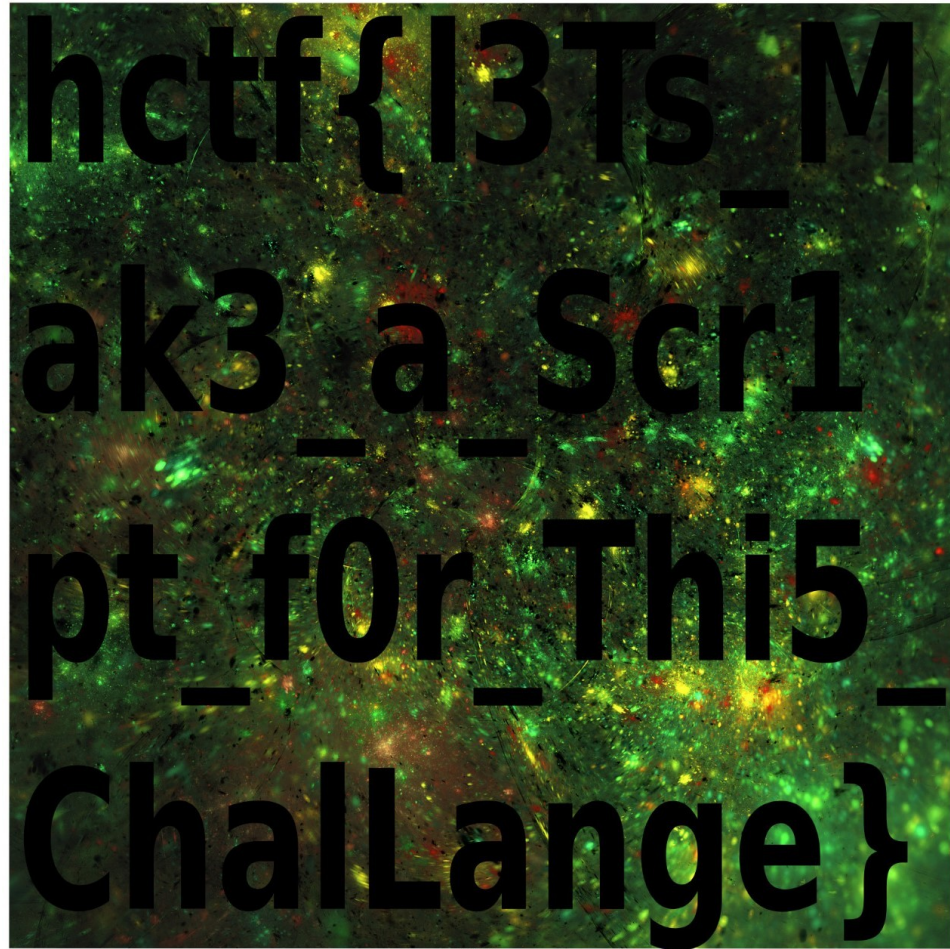
```

Forensics

disini saya tidak memakai script diatas tetapi mencoba dengan menggunakan tools linux yaitu montage untuk menggabungkan potongan gambar tersebut

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

jalankan dan didapat gambar utuh yang berisi sebuah flag



09X09

flaag : **hctf{l3Ts_Mak3_a_Scr1pt_f0r_Thi5_Challange}**

Eyes N Closed

Diberikan Sebuah file crt.txt berisi nilai berikut

```
[x]-[flintz@shadow]-[~/Downloads/hology/crypto]
$cat crt.txt
31337
22701048129543736333425996094749366889587533646608478003817325824700916267577973
5389791151574049166747880487470296548479
82277179313422272596538805734077480601768310299254984470451423495501149986396526
959207256445320568510116948563902704353
```

diketahui nilai c n dan e seperti ini

c =

8227717931342227259653880573407748060176831029925498
4470451423495501149986396526959207256445320568510116
948563902704353

n =

2270104812954373633342599609474936688958753364660847
8003817325824700916267577973538979115157404916674788
0487470296548479

e = 31337

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

p =

3274145556934980157511463037491414880636424032401714
63406883

q =

6933426671108301811973254018997006413619658631273366
80673013

tinggal jalankan rsa tersebut dengan script berikut

```
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 =
822771793134222725965388057340774806017683102992549844704514234955
01149986396526959207256445320568510116948563902704353

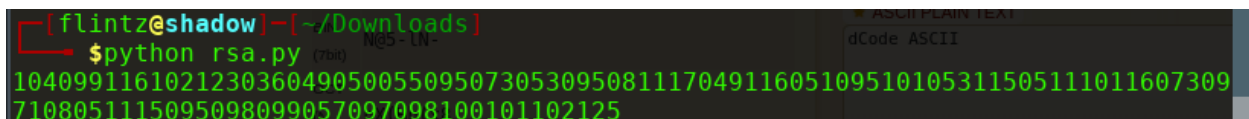
n =
227010481295437363334259960947493668895875336466084780038173258247
009162675779735389791151574049166747880487470296548479

m = pow(c,d,n)

print m

```

jalankan dan didapat hasil berikut



```

flintz@shadow ~ - [~/Downloads]
$python rsa.py
10409911610212303604905005509507305309508111704911605109510105311505111011607309
7108051115095098099057097098100101102125

```

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



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

Results

↑↓

↑↓

DEC (1-3 Digits)	hctf{\$127_I5_Qu1t3_e5s3ntIal3s_bc9abde f}
OCT (3 Digits)	D (- (XAO!pHHEEI@Ih@/8@ABU

ASCII CODE

Informatics > Character Encoding > ASCII Code

Sponsored ads

ASCII Converter

★ ASCII CIPHERTEXT (DECIMAL, HEXADECIMAL, ETC.)

104099116102123036049050055095073053095081117049116051095101
053115051110116073097108051115095098099057097098100101102125

★ PRINT DECODED HEXADECIMAL VALUES ☐

DECRYPT/CONVERT ASCII

See also: [Binary Code](#)

ASCII Encoder

★ ASCII PLAIN TEXT

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