

Write Up Hology 2.0

Ashabul Kahfi



Ahmad Fauzzan Maghribi

Rio Darmawan

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

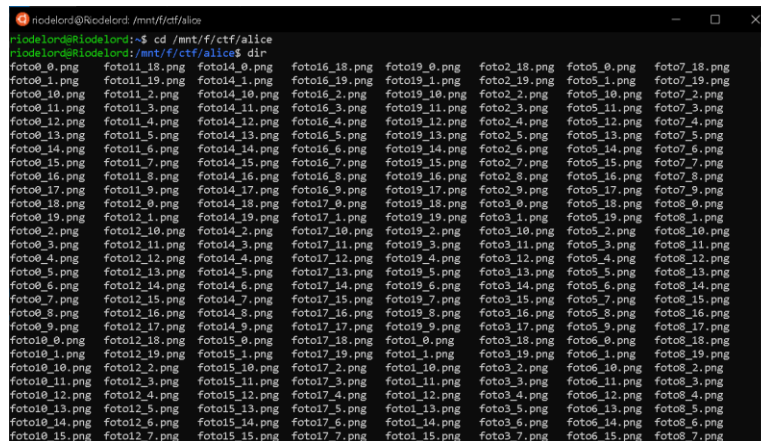
Forensik

Green Milky Ways



Kita di beri dua buah file , alice.zip yang berisi gambar banyak sekali dan enc.pyc sebuah program. Dari sini saya langsung menyimpulkan harus menggabungkan gambar yang terpisah untuk mendapatkan flagnya.

Pertama saya extract terlebih dahulu semua file yang ada didalam zip kedalam 1 folder.

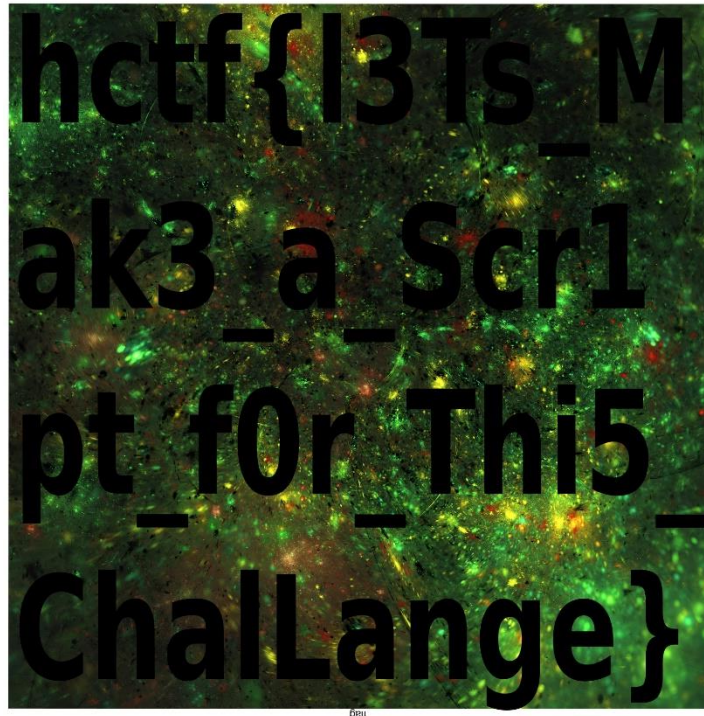


Setelah diextract kedalam 1 folder, saya menjalankan aplikasi montage untuk menyatukan semua gambar yang terpisah. Disini saya tidak menggunakan script cukup menggunakan aplikasi montage saja.

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

```
riodelord@riodelord:~/mnt/f/ctf/alice$ montage -mode concatenate -title flag $(ls -v *) flag.jpg
riodelord@riodelord:~/mnt/f/ctf/alice$
```

Nah skrg kita buka file yang sudah menyatu bernama flag.jpg



Flag

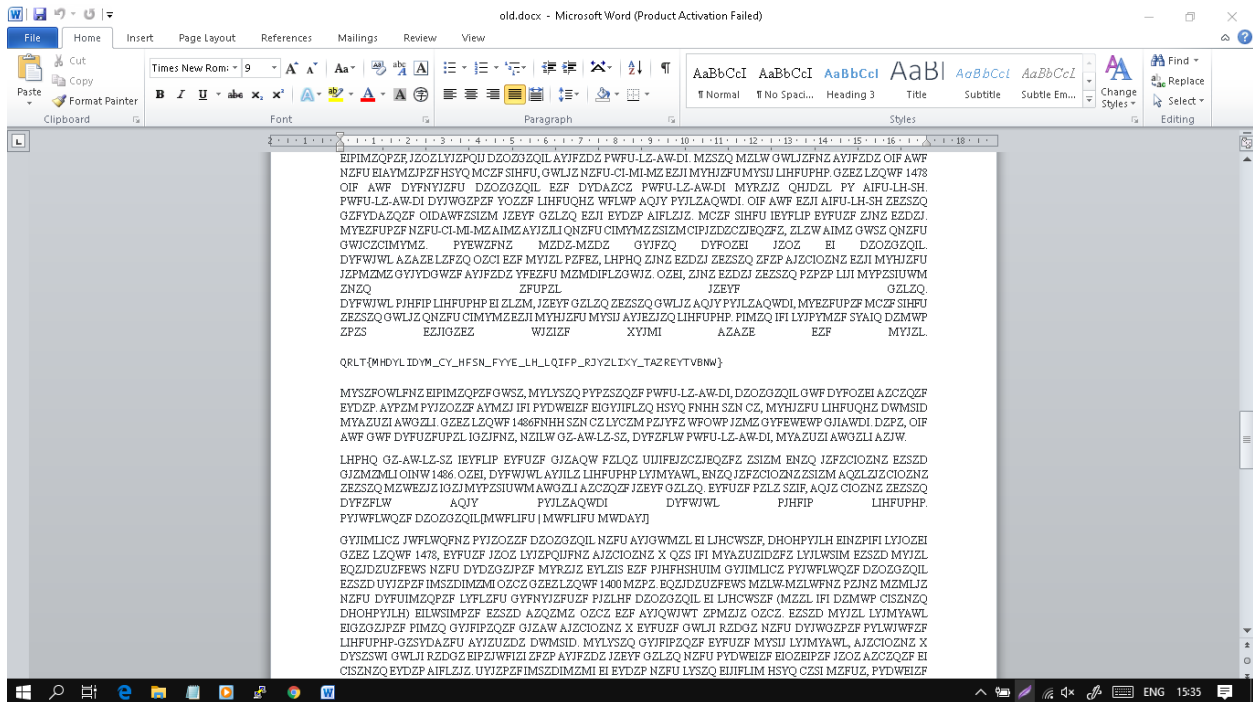
Hctf{l3Ts_Mak3_a_Scr1pt_f0r_Thi5_Challange}

Crypto

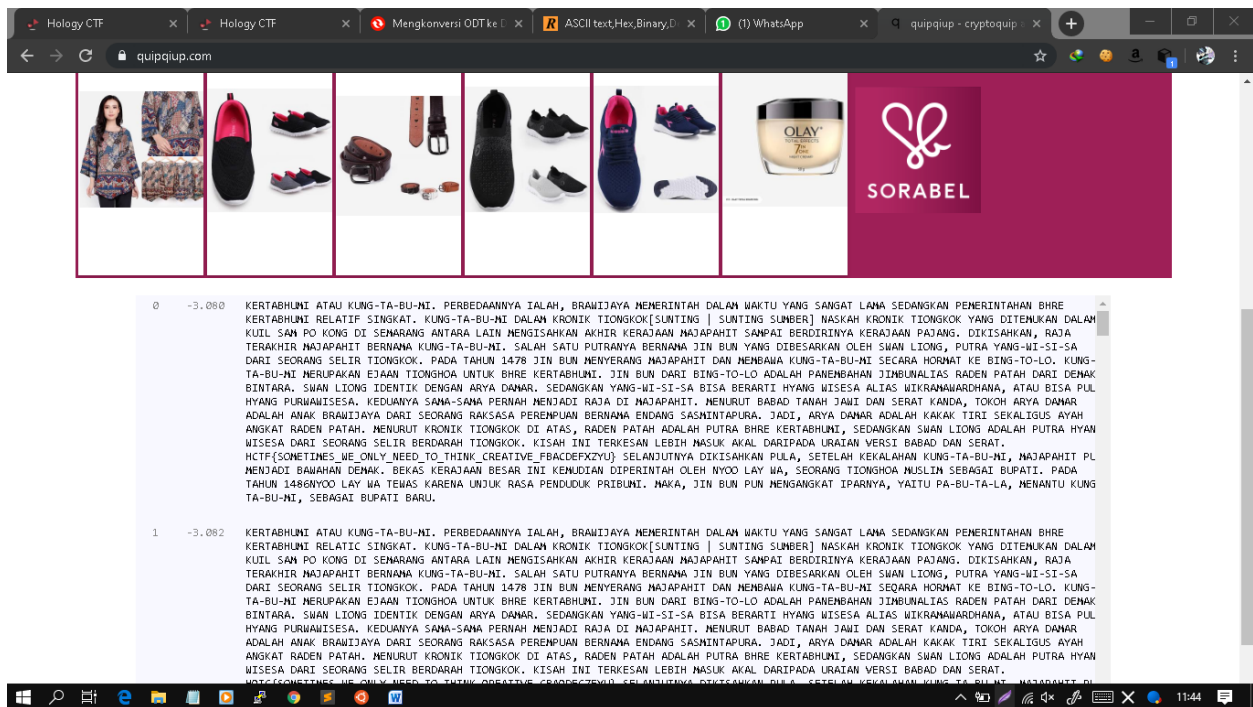
Arigatou

Cara Pengerjaan

Diberikan sebuah file old.odt kemudian dibuka lalu isinya seperti ini, langsung kepikiran Cryptoquip.



Lalu kunjungi website <https://quipqiup.com> kemudian didapat flagnya.

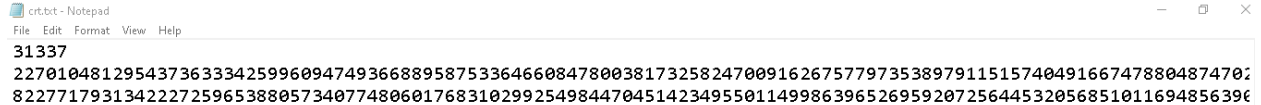


Flag

HCTF{SOMETIMES_WE_ONLY_NEED_TO_THINK_CREATIVE_FBACDEFXZYU}

eyes n closed

Pertama kita download soal yang diberikan , setelah dibuka munculah nilai berikut. Bisa disimpulkan itu rsa, dengan urutan e,n,c sesuai dengan judul soal.



31337
2270104812954373633342599609474936688958753364660847800381732582470091626757797353897911515740491667478804874702
8227717931342227259653880573407748060176831029925498447045142349550114998639652695920725644532056851011694856396

Langsung saja bikin script buat decrypt rsa, seperti ini

```
Solver.py
from Crypto.Util.number import inverse
e = 31337
n =
22701048129543736333425996094749366889587533646608478003817325824700916267577
9735389791151574049166747880487470296548479
c =
82277179313422272596538805734077480601768310299254984470451423495501149986396
526959207256445320568510116948563902704353

p = 693342667110830181197325401899700641361965863127336680673013
q = 327414555693498015751146303749141488063642403240171463406883

phi = (p-1)*(q-1)
d = inverse(e,phi)
m = pow(c,d,n)
print m

m =
10409911610212303604905005509507305309508111704911605109510105311505111011607
3097108051115095098099057097098100101102125
```

Kemudian hasil diubah ke bentuk ascii, didapat flag.

ASCII text

```
hctf{$127_I5_Qu1t3_e5s3ntIal3s_bc9abdef}
```

Hex (bytes)

```
68 63 74 66 78 24 31 32 37 5F 49 35 5F 51 75 31 74 33 5F 65 35  
73 33 6E 74 49 61 6C 33 73 5F 62 63 39 61 62 64 65 66 7D
```

Binary (bytes)

```
01101000 01100011 01110100 01100110 01111011 00100100  
00110001 00110010 00110111 01011111 01001001 00110101  
01011111 01010001 01110101 00110001 01110100 00110011
```

Decimal (bytes)

```
104099116102123036049050055095073053095081117049116051095101053  
115051110116073097108051115095098099057097098100101102125
```

Flag

```
hctf{$127_I5_Qu1t3_e5s3ntIal3s_bc9abdef}
```

Reverse

Easy dian

Diberikan file elf-64 bit, langsung dibuka menggunakan ida pro 64, lalu dilihat pseudocodenya, seperti ini.

```
1  int64 __fastcall main(__int64 a1, char **a2, char **a3)
2  {
3      char *s; // [rsp+70h] [rbp-10h]
4
5      s = (char *)calloc(1uLL, 0x3EuLL);
6      puts("Masukkan kode: ");
7      fgets(s, 62, stdin);
8      if ( *(_DWORD *)s != 'ftch'
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         || '\n' != *((_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 ada flag yang terbalik, langsung buat script python untuk otomatis balik string tersebut. Ketika dijalankan munculla flag.

Kode

Flag.py

```
lol = ["ftch",
"t3L{",
"el_s",
"_NR4",
"idn3",
```



```
"Sena",  
"1s_5",  
"ylpm",  
"ba6_",  
"}09f",]  
  
print "".join(i[::-1] for i in lol)
```

Flag

hctf{L3ts_1e4RN_3ndianeS5_s1mply_6abf90}