WRITEUP Final FIND-IT! CTF 2022

Disusun oleh: pwnpeko, Universitas Diponegoro

1. Kategori: web
   Nama: static
   Langkah Pengerjaan:
   a. Pada soal hanya disediakan sebuah link kepada suatu webpage. Pada saat mengunjungi webpage tersebut, akan disambut dengan prompt login (username dan password), namun yang aneh adalah meskipun ada batas try, try tersebut tidak menghasilkan request apapun terhadap server. Ketika dicek source pada html webpagenya, ditemukan script javascript 1 line yang sangat panjang.
   b. Ketika javascript tersebut dibeautify menggunakan code beautifier, akan ditemukan kode yang telah ter-obfuscated:

```
eval(function (p, a, c, k, e, r) {
   e = function (c) {
        return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a)
> 35 ? String.fromCharCode(c + 29) : c.toString(36))
   };
   if (!''.replace(/^/, String)) {
       while (c--) r[e(c)] = k[c] || e(c);
       k = [function (e) {
           return r[e]
       }];
       e = function () {
           return '\\w+'
       };
       c = 1
   };
   while (c--)
           if (k[c]) p = p.replace(new RegExp('\\b' + e(c) +
'\\b', 'g'), k[c]);
   console.log(p, e)
   return p
}('f g(9){1 a=[];p(1 i=0;i<9.q;i++){a[i]=(9.r(i).h(s)).t(-4)}b
a.u("")}1    c="c";1    j="v";w    k=g(j).h();1    2=3;f    x(){1
7=5.6("7").l;1                8=5.6("8").l;m(7=="c"&&8==k){n("y
```

```
z");A.B="C.D";b        o}E{2--;n("F        G        H        "+2+"
2;");m(2==0){5.6("7").d=e;5.6("8").d=e;5.6("I").d=e;b    o}}}',
45,                                                          45,
'|var|attempt|||document|getElementById|username|password|str|
arr|return|admin|disabled|true|function|shex|toString||mypass|
login|value|if|alert|false|for|length|charCodeAt|16|slice|join
|admindabest|let|validate|Login|successfully|window|location|s
ucess|html|else|You|have|left|submit'.split('|'), 0, {}))
```

c. Dilakukan proses deobfuskasi. Proses deobfuskasi hanya dengan meng-outputkan fungsi eval, ditemukan script sebagai berikut:

```
function shex(str) {
   var arr = [];
   for (var i = 0; i < str.length; i++) {
       arr[i] = (str.charCodeAt(i).toString(16)).slice(-4)
   }
   return arr.join("")
}
var admin = "admin";
var mypass = "admindabest";
let login = shex(mypass).toString();
var attempt = 3;

function validate() {
   var username = document.getElementById("username").value;
   var password = document.getElementById("password").value;
   if (username == "admin" && password == login) {
       alert("Login successfully");
       window.location = "sucess.html";
       return false
   } else {
       attempt--;
       alert("You have left " + attempt + " attempt;");
       if (attempt == 0) {
                document.getElementById("username").disabled =
true;
                document.getElementById("password").disabled =
true;
          document.getElementById("submit").disabled = true;
```

```
            return false
        }
    }
}
```

d. Proses validasi dilakukan pada string username “admin” dan password yang merupakan output string dari fungsi shex diatas, yaitu string “61646d696e646162657374”.
e. Melakukan login dengan credential tersebut akan ditemukan flag
f. Flag: `FindITCTF{7ed4_Se73N4K}`

2. Kategori: web
   Nama: pemanasan
   Langkah Pengerjaan:
   a. Mengunjungi link yang disediakan oleh soal akan memberikan source code php sebagai berikut:

```php
<?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;
}
?>
```

   b. Untuk melihat flagnya, maka kita harus melewati komparasi string parameter flag dengan flag yang akan dicari. Artinya strcmp tersebut harus mengembalikan 0. https://hydrasky.com/network-security/php-string-comparison-vulnerabilities/ mengatakan bahwa komparasi apapun dengan array kosong akan selalu mengembalikan NULL. Dalam php, loose comparison akan membuka serangan type juggling php, artinya NULL disini juga dapat diartikan sebagai 0.
   c. Melakukan request
   http://47.243.63.167:13400/?flag[]=””

akan mengarahkan kita kepada flag

d. Flag: `FindITCTF{S3m4ng4t_G4nS1s_C3munguDh_3a_456456101100}`

3. Kategori: web

   Nama: audit

   Langkah Pengerjaan:

   a. Mengunjungi link yang disediakan oleh soal akan memberikan source code php sebagai berikut:

```
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__);
}
```

   b. yang harus dilakukan untuk mendapatkan flagnya adalah melewati kedua pass if

```
if ($_GET['username'] == $_GET['password'])
```

   dan

```
else if (md5($_GET['username']) ===
md5($_GET['password']))
```

   artinya kita harus mencari parameter post username dan password yang ketika di komparasikan akan bernilai true, dan harus berbeda satu sama lain

   c. Seperti pada soal sebelumnya, komparasi dengan array kosong akan selalu mengembalikan 0, maka tinggal melakukan request dengan:

   http://47.243.63.167:13405/?username[]=asfg&password[]=asdf

   akan menampilkan flag

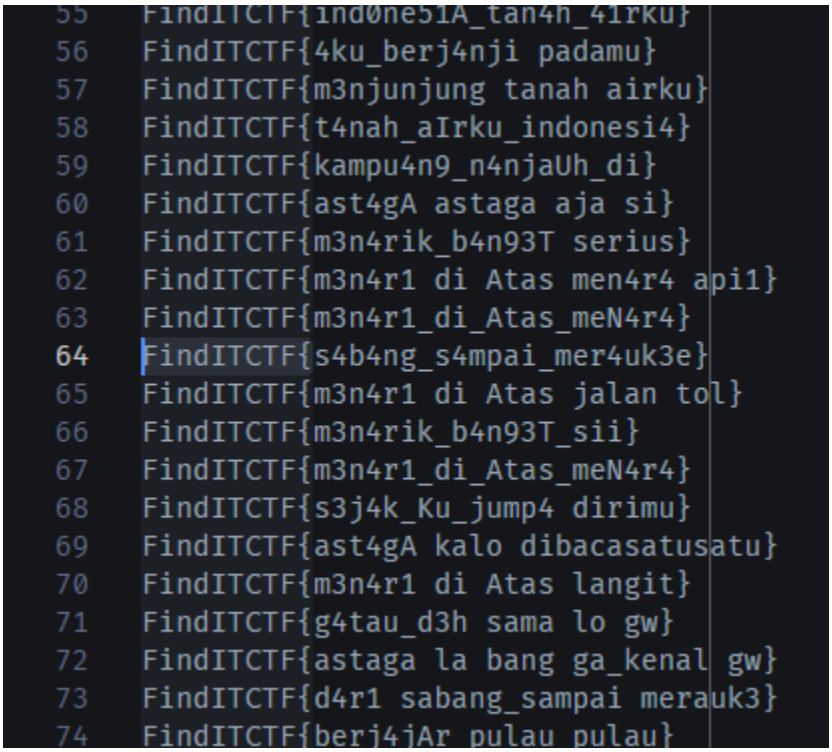
   d. Flag: `FindITCTF{w3ll_h3llo_4gain_my_fr13nds_447788}`

4. Kategori: misc

   Nama: findme

   Langkah Pengerjaan:

   a. Saya melakukan pencarian scanning dengan bantuan ruler di vscode. Dari beberapa kandidat ditemukan di line 64



   b. Flag : FindITCTF{s4b4ng_s4mpai_mer4uk3e}

5. Kategori: crypto

   Nama: rail-sub

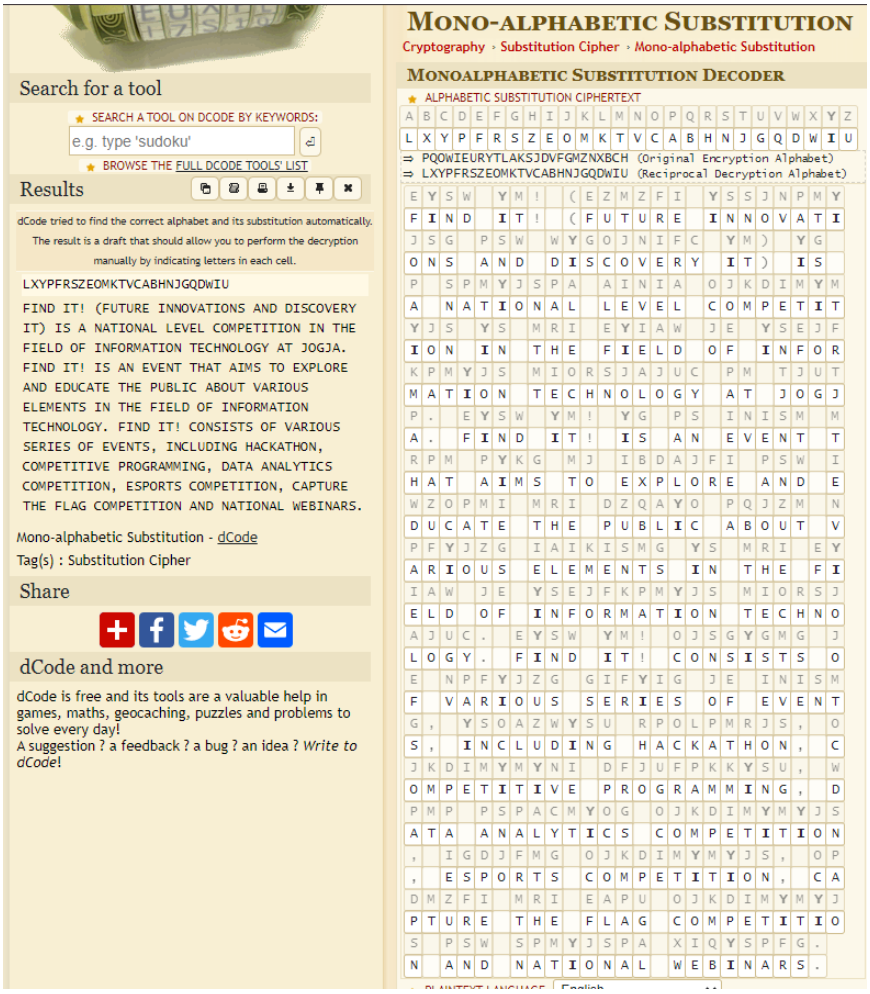
   Langkah Pengerjaan:

   a. Di line terakhir soal.py ditunjukan dilakukan substitusi dulu kemudian rail fence. Pertama kita melakukan dekripsi rail fence menggunakan kode dari geeks for geeks ini https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/

   b. Dari flag o_fdyfoi__pdiyrcgdrdip didapatkan oydrif_oydrif_cig_dpdp

   c. Sekarang kita perlu melakukan reverse substitusi. Untungnya diberikan sample teks untuk menjadi patokan substitusi untungnya dcode.fr menyediakan tools untuk melakukan attack untuk bahasa inggris

https://www.dcode.fr/monoalphabetic-substitution



d. Didapatkan substitution key nya LXYPFRSZEOMKTVCABHNJGQDWIU
e. Dari key tersebut kita akan gunakan untuk mendekripsi flag tersebut

```
flag = "oydrif_oydrif_cig_dpdp"
ori = "ABCDEFGHIJKLMNOPQRSTUVWXYZ".lower()
sub = "LXYPFRSZEOMKTVCABHNWGQDJIU".lower()

for c in flag:
    if c == '_':
        print('_', end='')
    else:
        print(sub[ori.find(c)], end='')
```

o. flag : FindITCTF{cipher_cipher_yes_papa}

6. Kategori: crypto

   Nama: table

   Langkah Pengerjaan:

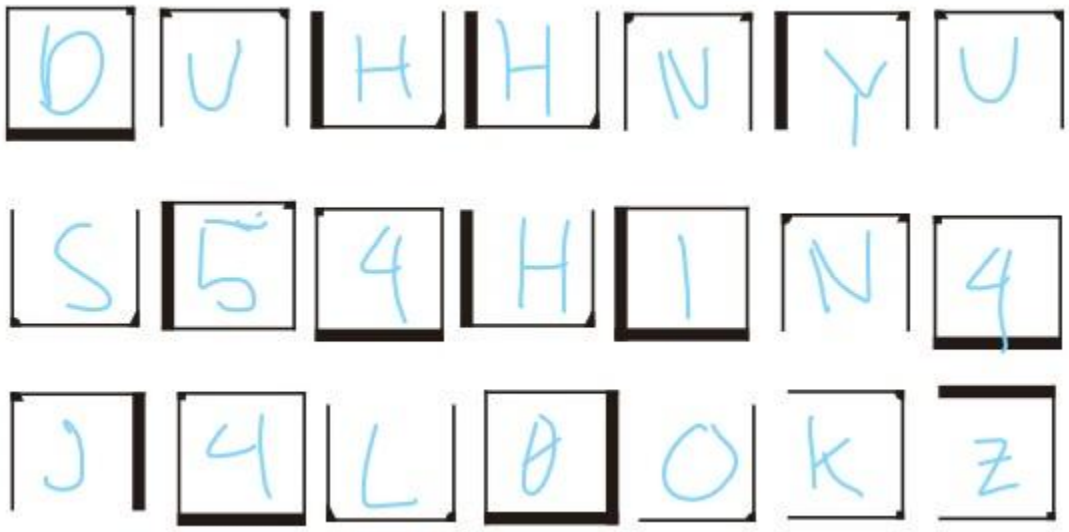
   a. Diberikan sebuah table seperti sudoku dengan pattern seperti ini

   b. Setelah diperhatikan tabel tersebut memiliki pola seperti ini

c. Berikut hasil yang sudah terisi

O	9	W	H	L	P
K	8	C	5	9	T
G	4	0	1	D	X
2	F	3	2	6	I
V	B	7	E	A	M
R	N	J	Y	U	Q

d. Dengan menggunakan tabel yang sudah lengkap, kita akan mencocokan dengan template yang diberikan



e. Maka flag : FindITCTF{DUHHNYUS54HIN4J4L0OKZ}

7. Kategori: osint

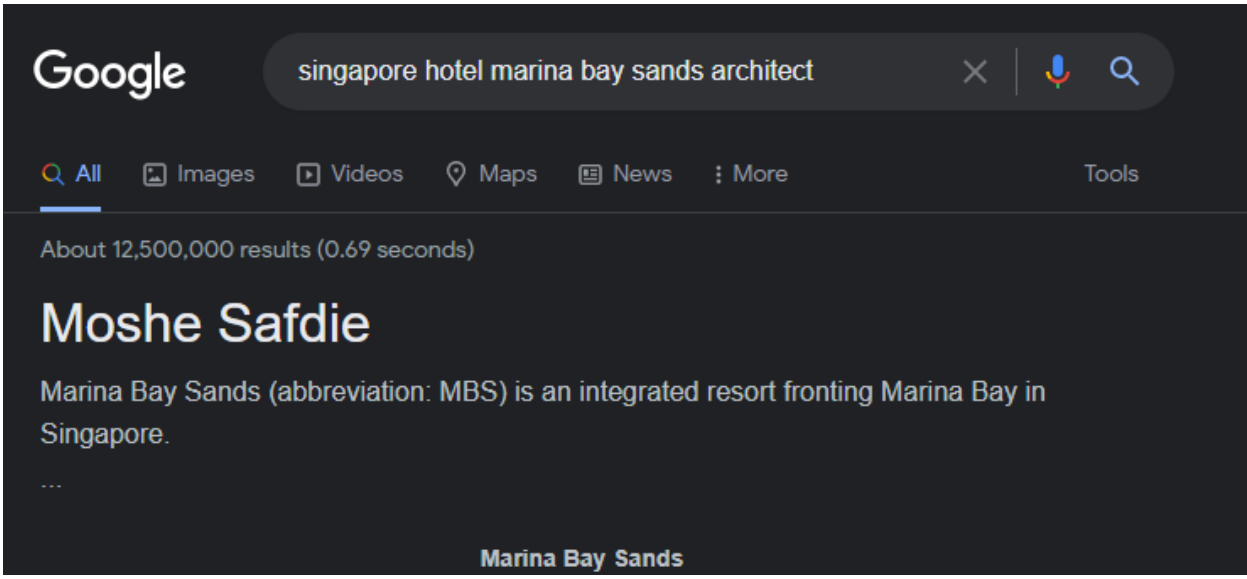
   Nama: architect

   Langkah Pengerjaan:

   a. Dengan klu “detective” dan “sapphire”, sepertinya menunjuk kepada film detective conan “The Fist of Blue Sapphire”

   b. Di web ini https://www.detectiveconanworld.com/wiki/The_Fist_of_Blue_Sapphire dijelaskan bahwa kasusnya berlatar di Singapore Marina Bay Sands Hotel

c. Ketika mencari “Singapore Marina Bay Sands Hotel architect” kita menemukan ini



d. Maka flag FindITCTF{moshesafdie}

8. Kategori: osint

   Nama: whereisit

   Langkah Pengerjaan:

   a. Pada soal disediakan gambar berikut:

   b. Karena saya bermain valorant, maka saya langsung mengenalinya :). Map tersebut bernama Split dan google search menunjukkan bahwa map tersebut berdasarkan negara Jepang.

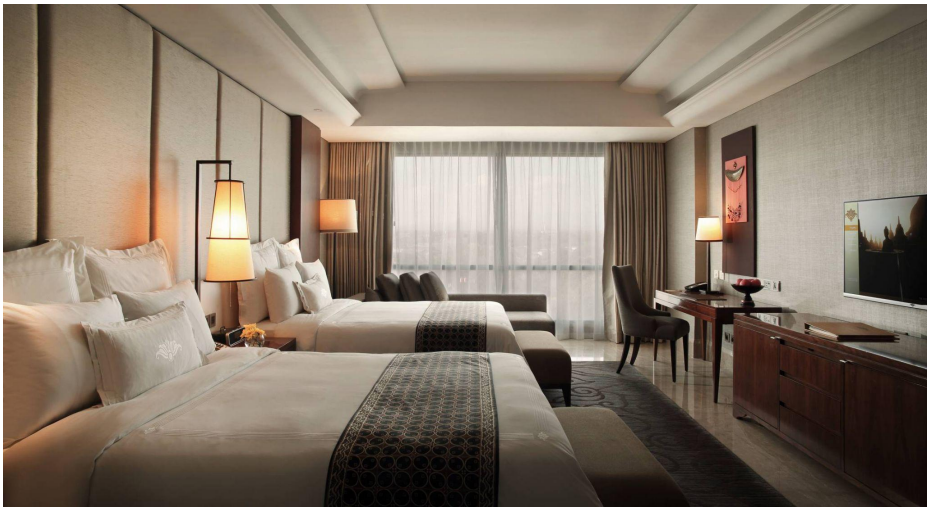
   c. Maka Flag: `FindITCTF{Jepang}`

9. Kategori: osint

   Nama: wine

   Langkah Pengerjaan:

   a. Diberikan gambar berikut pada soal:



   b. Dengan menggunakan google reverse image search, ditemukan bahwa gambar tersebut diambil pada Hotel Tentrem Yogyakarta. Sisanya adalah mencari apapun tentang hotel tersebut yang berhubungan dengan wine.

   c. Melihat twitternya tidak ada yang berhubungan dengan wine. Namun pada instagram terlihat postingan tentang wine yang dibuat oleh Carmen. Quick google search menunjukkan bahwa Carmen berasal dari Chile.

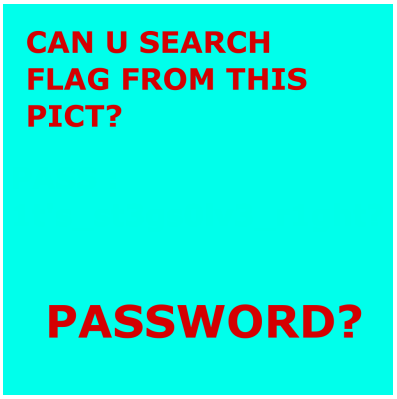
   d. Maka flag: `FindITCTF{Chile}`

10. Kategori: forensics

    Nama: Stegs

    Langkah Pengerjaan:

    a. Diberikan sebuah gambar oleh challenge:



b. Hal yang pertama dilakukan pada gambar ini adalah dilakukan binwalk pada gambar tersebut dan ditemukan beberapa file. Salah satu diantaranya adalah file zip yang terproteksi password dan gambar lagi.
c. Melakukan Stegsolve pada gambar ditemukan password zip tersebut pada filter blue plane 0:

d. Memasukkan password tersebut kepada zip akan diberikan suatu textfile yang berisi hex string:
`46696e6449544354467b346e30746833725f737433676f5f7231676874 3f7d`
Mengkonversikannya menjadi ascii string ditemukan flag
e. Flag: `FindITCTF{4n0th3r_st3go_r1ght?}`