

WRITEUP Final FIND-IT! CTF 2022

Disusun oleh: pwnpeko, Universitas Diponegoro

1. Kategori: web

Nama: static

Langkah Pengerjaan:

- 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.
- 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").1;1 8=5.6("8").1;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
uccess|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
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\[\]=""](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](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

```
55 FindITCTF{ind0ne51A_tan4h_41rku}
56 FindITCTF{4ku_berj4nji padamu}
57 FindITCTF{m3njunjung tanah airku}
58 FindITCTF{t4nah_aIрку_indonesi4}
59 FindITCTF{kampu4n9_n4njaUh_di}
60 FindITCTF{ast4gA astaga aja si}
61 FindITCTF{m3n4rik_b4n93T serius}
62 FindITCTF{m3n4r1 di Atas men4r4 api1}
63 FindITCTF{m3n4r1_di_Atas_meN4r4}
64 FindITCTF{s4b4ng_s4mpai_mer4uk3e}
65 FindITCTF{m3n4r1 di Atas jalan tol}
66 FindITCTF{m3n4rik_b4n93T sii}
67 FindITCTF{m3n4r1_di_Atas_meN4r4}
68 FindITCTF{s3j4k_Ku_jump4 dirimu}
69 FindITCTF{ast4gA kalo dibacasatusatu}
70 FindITCTF{m3n4r1 di Atas langit}
71 FindITCTF{g4tau_d3h sama lo gw}
72 FindITCTF{astaga la bang ga_kenal gw}
73 FindITCTF{d4r1 sabang_sampai merauk3}
74 FindITCTF{berj4jAr pulau pulau}
```

- 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>

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'

★ BROWSE THE FULL DCODE TOOLS LIST

Results

dCode tried to find the correct alphabet and its substitution automatically.
The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

LXYPFRSZEOMKTVCAHJGQDWIU

FIND IT! (FUTURE INNOVATIONS AND DISCOVERY IT) IS A NATIONAL LEVEL COMPETITION IN THE FIELD OF INFORMATION TECHNOLOGY AT JOGJA. FIND IT! IS AN EVENT THAT AIMS TO EXPLORE AND EDUCATE THE PUBLIC ABOUT VARIOUS ELEMENTS IN THE FIELD OF INFORMATION TECHNOLOGY. FIND IT! CONSISTS OF VARIOUS SERIES OF EVENTS, INCLUDING HACKATHON, COMPETITIVE PROGRAMMING, DATA ANALYTICS COMPETITION, ESPORTS COMPETITION, CAPTURE THE FLAG COMPETITION AND NATIONAL WEBINARS.

Mono-alphabetic Substitution - dCode

Tag(s) : Substitution Cipher

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to dCode!

MONO-ALPHABETIC SUBSTITUTION
Cryptography • Substitution Cipher • Mono-alphabetic Substitution

MONOALPHABETIC SUBSTITUTION DECODER

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	X	Y	P	F	R	S	Z	E	O	M	K	T	V	C	A	B	H	N	J	G	Q	D	W	I	U

⇒ PQOWIEURYTLAKSJDVFGMZXNBCH (Original Encryption Alphabet)
⇒ LXYPFRSZEOMKTVCAHJGQDWIU (Reciprocal Decryption Alphabet)

E	Y	S	W	Y	M	I		(E	Z	M	Z	F	I		Y	S	S	J	N	P	M	Y	
F	I	N	D	I	T	!		(F	U	T	U	R	E		I	N	N	O	V	A	T	I	
J	S	G		P	S	W		W	Y	G	O	J	N	I	F	C	Y	M)		Y	G		
O	N	S		A	N	D		D	I	S	C	O	V	E	R	Y		I	T)		I	S	
P	S	P	M	Y	J	S	P	A		A	I	N	I	A		O	J	K	D	I	M	Y	M	
A	N	A	T	I	O	N	A	L		L	E	V	E	L		C	O	M	P	E	T	I	T	
Y	J	S		Y	S	M	R	I		E	Y	I	A	W		J	E	Y	S	E	J	F		
I	O	N		I	N	T	H	E		F	I	E	L	D		O	F	I	N	F	O	R		
K	P	M	Y	J	S		M	I	O	R	S	J	A	J	U	C		P	M		T	J	U	T
M	A	T	I	O	N		T	E	C	H	N	O	L	O	G	Y		A	T		J	O	G	J
P	.		E	Y	S	W		Y	M	!		Y	G		P	S		I	N	I	S	M	M	
A	.		F	I	N	D		I	T	!		I	S		A	N		E	V	E	N	T		
R	P	M		P	Y	K	G		M	J		I	B	D	A	J	F	I		P	S	W		I
H	A	T		A	I	M	S		T	O		E	X	P	L	O	R	E		A	N	D		E
W	Z	O	P	M	I		M	R	I		D	Z	Q	A	Y	O		P	Q	J	Z	M		N
D	U	C	A	T	E		T	H	E		P	U	B	L	I	C		A	B	O	U	T		V
P	F	Y	J	Z	G		I	A	I	K	I	S	M	G		Y	S		M	R	I		E	Y
A	R	I	O	U	S		E	L	E	M	E	N	T	S		I	N		T	H	E		F	I
I	A	W		J	E		Y	S	E	J	F	K	P	M	Y	J	S		M	I	O	R	S	J
E	L	D		O	F		I	N	F	O	R	M	A	T	I	O	N		T	E	C	H	N	O
A	J	U	C	.		E	Y	S	W		Y	M	!		O	J	S	G	Y	G	M	G		J
L	O	G	Y	.		F	I	N	D		I	T	!		C	O	N	S	I	S	T	S		O
E	N	P	F	Y	J	Z	G		G	I	F	Y	I	G		J	E		I	N	I	S	M	
F	V	A	R	I	O	U	S		S	E	R	I	E	S		O	F		E	V	E	N	T	
G	,		Y	S	O	A	Z	W	Y	S	U		R	P	O	L	P	M	R	J	S	,	O	
S	,		I	N	C	L	O	D	I	N	G		H	A	C	K	A	T	H	O	N	,	C	
J	K	D	I	M	Y	M	Y	N	I		D	F	J	U	F	P	K	K	Y	S	U	,	W	
O	M	P	E	T	I	T	I	V	E		P	R	O	G	R	A	M	M	I	N	G	,	D	
P	M	P		P	S	P	A	C	M	Y	O	G		O	J	K	D	I	M	Y	M	Y	J	S
A	T	A		A	N	A	L	Y	T	I	C	S		C	O	M	P	E	T	I	T	I	O	N
,		I	G	D	J	F	M	G		O	J	K	D	I	M	Y	M	Y	J	S	,	O	P	
,		E	S	P	O	R	T	S		C	O	M	P	E	T	I	T	I	O	N	,	C	A	
D	M	Z	F	I		M	R	I		E	A	P	U		O	J	K	D	I	M	Y	M	Y	J
P	T	U	R	E		T	H	E		F	L	A	G		C	O	M	P	E	T	I	T	I	O
S		P	S	W		S	P	M	Y	J	S	P	A		X	I	Q	Y	S	P	F	G	.	
N		A	N	D		N	A	T	I	O	N	A	L		W	E	B	I	N	A	R	S	.	

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

```
f. flag = "oydrif_oydrif_cig_dpdp"
g. ori = "ABCDEFGHIJKLMNOPQRSTUVWXYZ".lower()
h. sub = "LXYPFRSZEOMKTVCAHJGQDWIU".lower()
i.
j. for c in flag:
k.     if c == '_':
l.         print('_', end='')
m.     else:
n.         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

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

b. Setelah diperhatikan tabel tersebut memiliki pola seperti ini

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

c. Berikut hasil yang sudah terisi

O	S	W	H	L	P
K	8	C	5	9	T
G	4	0	1	D	X
Z	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 mencocokkan dengan template yang diberikan



e. Maka flag : FindITCTF{DUHHNYUS54HIN4J4L0OKZ}

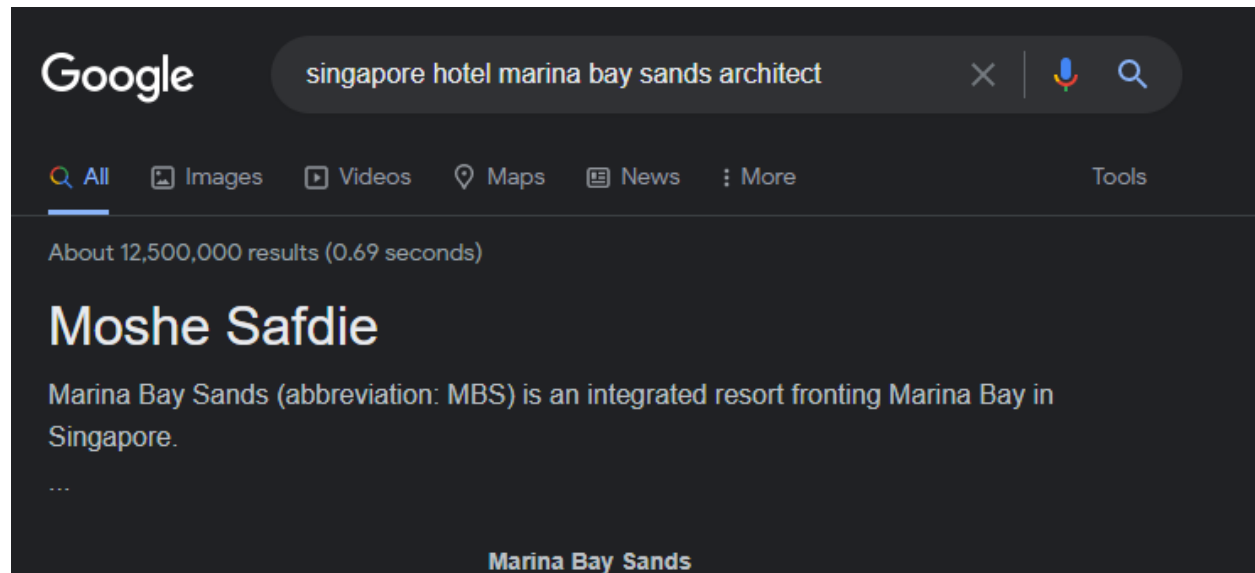
7. Kategori: osint

Nama: architect

Langkah Pengerjaan:

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



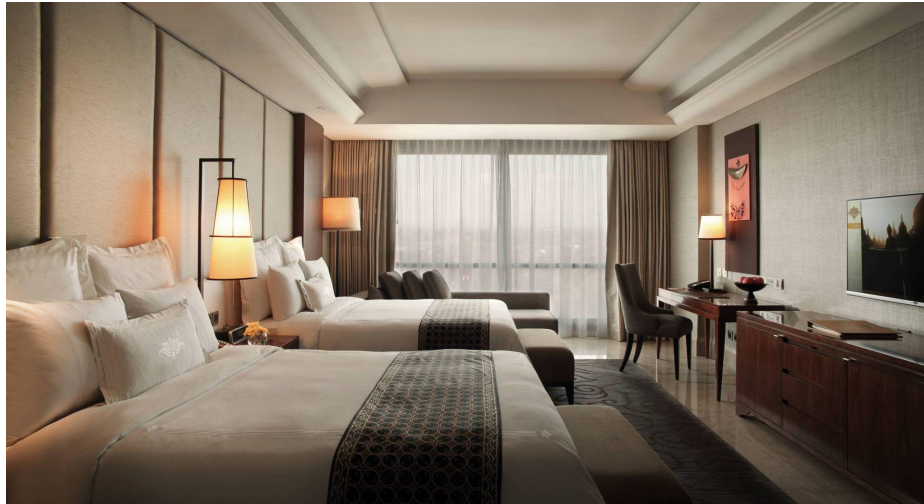
- b. Karena saya bermain valorant, maka saya langsung mengenalinya :). Map tersebut bernama Split dan google search menunjukkan bahwa map tersebut berdasarkan negara Jepang.
- c. Maka Flag: FindITCTF{Jepang}

9. Kategori: osint

Nama: wine

Langkah Pengerjaan:

- a. Diberikan gambar berikut pada soal:



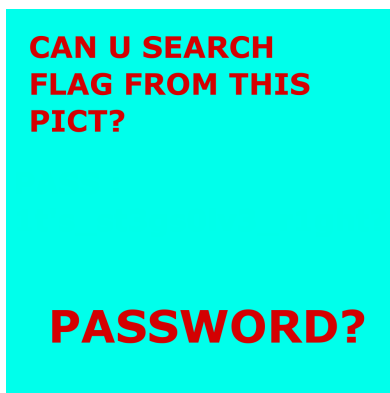
- b. Dengan menggunakan google reverse image search, ditemukan bahwa gambar tersebut diambil pada Hotel Tentrem Yogyakarta. Sisanya adalah mencari apapun tentang hotel tersebut yang berhubungan dengan wine.
- c. Melihat twitternya tidak ada yang berhubungan dengan wine. Namun pada instagram terlihat 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:

PASS :
1t's_st3gs0lv3_r1ght?

- 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?}