



JUNE 9, 2017 / CTF

## QUADRATHLON 2017 WRITEUP – PART 2

# Permintaan – Forensic 50pts

---

Klei (orang yang berbeda dengan Kley) akhir-akhir ini sering mengirimkan pesan pada Bambang. Dan kamu sering melihat Klei mengedipkan matanya secara manja saat bertemu dengan Bambang. Cari tahu apa yang terjadi diantara Klei dan Bambang (huruf yg ada di flag huruf kecil semua)

Soal ini (lagi-lagi) problem tentang XOR. Gunakan stegsolve untuk menyelesaikannya. Open salah satu file, kemudian pilih Analyse > Image Combiner

**Flag : noobfs3n\_dnud3sl**

# Haus – Forensic 50pts

---

Cari sesuatu yang mencurigakan di dalam minuman ini

Periksa dengan binwalk

```

Terminal File Edit View Search Terminal Help
clayday@prns1c:~/Documents/CTF/Soal/TCyber/for2$ binwalk ntap.jpg

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
325721      0x4F859      PNG image, 2000 x 1972, 8-bit/color RGBA, non-interlaced
325780      0x4F894      Zlib compressed data, default compression
489285      0x77745      JPEG image data, JFIF standard 1.01
507572      0x7BEB4      PNG image, 640 x 400, 8-bit/color RGBA, non-interlaced
507712      0x7BF40      Zlib compressed data, best compression

clayday@prns1c:~/Documents/CTF/Soal/TCyber/for2$

```

Terdapat 2 gambar lain yang ditimpa oleh logo fanta tersebut. Ekstrak gambar yang tersembunyi dengan foremost. Pada folder output/png terdapat flag

**Flag : nooblucanrun\_butucanthide!**

## Nakal – Forensic 100pts

Karena semalam nonton bola, Supri lupa mengerjakan tugas di elearning. Supri yang kebingungan lalu meminta Wahyu untuk mengirimkannya kodingan tugas itu. Namun Wahyu malah mengirim file yang tidak terduga. Karena waktu yang sempit, bantulah Supri untuk mencari kodingan Wahyu

Terdapat file pcapng yang menjadi attachment. Buka file tersebut dengan Wireshark. Lalu untuk melihat apa saja laman yang dikunjungi Wahyu, gunakan filter ***http.request.method == "GET"*** didapatkan Wahyu mengakses setidaknya 3 laman. [elearning.if.its.ac.id](http://elearning.if.its.ac.id), [elearning.if.its.ac.id/login/index.php](http://elearning.if.its.ac.id/login/index.php), dan [ideone.com/jWyOOu](http://ideone.com/jWyOOu). Dimana jika laman ketiga dibuka, akan ada kodingan Wahyu dan flagnya

**Flag :noobIngopi\_kodingan\_hehe!**

## Jack 1 – Web 75pts

Another simple login for you. [Try this](#)

Kali ini disajikan web yang merupakan halaman login. Langsung coba suntik pakai SQL Injection dengan masukan **username: 'OR 1=1–** . Ternyata laman diproteksi dengan javascript. Karena javascript berjalan di client-side, maka cukup nonaktifkan javascript browser anda, lalu refresh halaman. Kemudian masukkan kembali injeksi yang sama. Maka akan didapatkan flag

**Flag :noob!motor\_injeksi!**

## Jack 2 – Web 150pts

---

Now it's not that simple. Hope all the best for you, noob. [Try this](#)

Kembali disajikan laman web dengan login form. Namun kali ini ada tombol hint di bawahnya. Dan ketika diklik akan muncul tabel **myflag** dengan flag yang disensor. Berarti dapat kita asumsikan kita harus menampilkan isi sebenarnya dari tabel myflag. Coba dengan injeksi username: ' union select flag from myflag– . Ternyata hasilnya muncul

Error: The used SELECT statements have a different number of columns

Error ini muncul karena 2 query yang di union memiliki jumlah kolom yang berbeda. Maka dari itu, kita harus membuat hasil dari query injeksi kita menjadi 2 kolom. Dengan username: ' union select 1,flag from myflag– . Namun ternyata masih muncul error yang sama. Maka tambah lagi menjadi 3 kolom dengan **username: ' union select 1,2,flag from myflag–** . Dan didapatkan sebuah flag

**Flag :noob!mantap\_anjer!**

## Mantan – Web 75pts

---

Kley adalah lelaki idaman wanita. Dia mempunyai banyak sekali mantan, sampai-sampai dia harus membuat sebuah galeri untuk mengingatnya. Namun Kley ternyata diketahui menyembunyikan mantan terindahnya.

Siapakah dia? Hint : Foto mantan terindah kley disimpan di tempat yang berbeda.  
Mantan terindah kley adalah dijah</p>

Challenge kali ini adalah mengenai Local File Inclusion. LFI adalah suatu celah keamanan dimana client dapat mengakses direktori server yang tidak seharusnya.

Web ini menampilkan semua gambar yang ada di suatu direktori di server. Seperti yang dilihat pada url, terdapat parameter **p** dimana parameter ini merujuk pada direktori mana gambar yang akan ditampilkan. Kita bisa mengakses parent folder dengan menambahkan `../` pada parameter p. Maka web tersebut akan menampilkan gambar yang terdapat di parent folder dari folder yang seharusnya diakses. Jika terus ditelusuri, foto dijah akan muncul ketika kita mengakses parent ketiga dari folder, yaitu dengan memasukkan `p=../ ../ ../`

**Flag :noobImantan\_naudzubillah}**

## Hacked – Web 75pts

---

Hahahahahaha, seorang noob yang sok-sokan pro (Clayday) mendapatkan getahnya! Akhirnya webnya di hack oleh noobies yang lain. Clayday kebingungan dimana si hacker menyembunyikan flagnya! Hint: flag disembunyikan dengan client side scripting

Jika diklik tombol **Click to Get the Flag**, maka anda akan diarahkan ke laman `http://clayday.id:8000/web/haha/nottheflag.php`. Untuk mendapatkan flagnya, cukup melihat source code nya (Ctrl+U pada chrome). Disana terlihat bahwa tombol tersebut sebenarnya mengarah ke laman `http://clayday.id:8000/web/haha/nottheflag.php` yang sebenarnya merupakan link asli sebelum diubah dengan javascript pada file `custom.js`

**Flag :noobIjs\_changed\_the\_link}**

## Hitung – Web 200pts

---

Kata sapa penjumlahan 2 bilangan itu gampang? Cobain ini deh

Sebelumnya, sepertinya saya salah memberikan kategori pada challenge ini. Karena sebenarnya setelah dipikir-pikir challenge ini lebih ke programming daripada web exploit.

Web tersebut menampilkan soal penjumlahan 2 bilangan yang terdiri dari beberapa level, dimana tiap level harus diselesaikan dalam waktu kurang dari 3 detik. Tentunya kita akan kesusahan apabila melakukan penjumlahan dan memasukkan hasilnya secara manual. Untuk itu kita harus membuat script untuk ini. Untuk mengakses laman web, dapat dilakukan dengan memanfaatkan python requests. Sedangkan untuk scrapping operasi penjumlahan, dapat menggunakan library regex dari pyhon yaitu re.

```
#!/usr/bin/env python

import requests
import re

url = 'http://clayday.id:8000/web/hitung/'

print "Menghitung..."
s = requests.Session()

def scrape_and_send( text ):

    challenge = re.findall('\((.*)\)', text)[0]
    answer = str(eval(challenge))
    r = s.post(url, data={"ans": answer})
    if ( 'FLAG' in r.text ):
        print r.text
        exit()
        scrape_and_send(r.text)

r = s.get(url)
scrape_and_send(r.text)
```

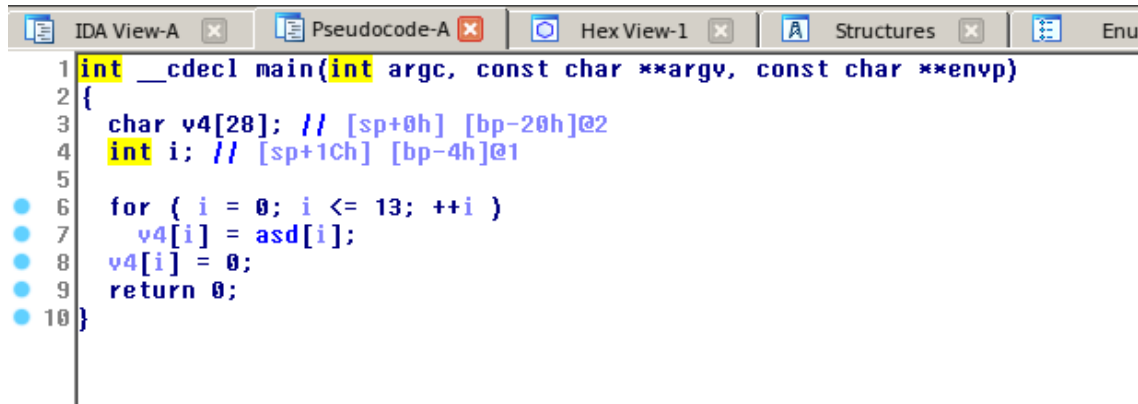
**Flag :noob!why\_you\_gotta\_b3\_so\_noobz!**

## Easy – Reversing 100pts

---

Simple nan manis

Pertama coba eksekusi executable tersebut. Namun ternyata tidak mengeluarkan apa-apa. Buka dengan IDA-PRO x64. Lalu dapatkan pseudocode nya dengan menekan F5



```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char v4[28]; // [sp+0h] [bp-20h]@2
4     int i; // [sp+1Ch] [bp-4h]@1
5
6     for ( i = 0; i <= 13; ++i )
7         v4[i] = asd[i];
8     v4[i] = 0;
9     return 0;
10 }

```

Program tersebut melakukan perulangan untuk mengkopi isi dari array asd ke array v4. Untuk melihat isi dari array asd, cukup klik dua kali. Maka akan muncul



```

.data:0000000000601040 ; int asd[]
.data:0000000000601040 asd
.data:0000000000601044
.data:0000000000601045
.data:0000000000601046
.data:0000000000601047
.data:0000000000601048
.data:0000000000601049
.data:000000000060104A
.data:000000000060104B
.data:000000000060104C
.data:000000000060104D
.data:000000000060104E
.data:000000000060104F
.data:0000000000601050
.data:0000000000601051
.data:0000000000601052
.data:0000000000601053
.data:0000000000601054
.data:0000000000601055
.data:0000000000601056
.data:0000000000601057
.data:0000000000601058
.data:0000000000601059

public asd
dd 6Eh
db 6Fh ; o
db 0
db 0
db 0
db 6Fh ; o
db 0
db 0
db 62h ; b
db 0
db 0
db 7Bh ; {
db 0
db 0
db 0
db 65h ; e
db 0
db 0
db 7Ah ; z
db 0

```

*Flag :nooblez\_reevv!*

# Habis – Reversing 200pts

Just do the reverse bro, and you will know what's goin on :)

Run executable tersebut, ternyata kita diminta memasukkan kode rahasia yang dimana kode tersebut adalah flag dari challenge ini. Seperti biasa pertama kita analisa menggunakan IDA-PRO

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    /* variabel lokal */

    strcpy(s, "d4WsnTwJspaFwAl3yXzMYWGRqwaeyN8E7");
    printf("Selamat datang di portal kley\n", argv, envp, *(_QWORD *)s, v7, v8, v9, v10);
    printf("Masukkan kode rahasia (flag) : ", *(_QWORD *)s, v7, v8, v9, v10);
    __isoc99_scanf("%s", v11);
    v12 = strlen(s);
    v3 = strlen(v11);
    if ( v3 == v12 )
    {
        v13 = 0;
        for ( i = 0; ; ++i )
        {
            v4 = i;
            if ( v4 >= strlen(v11) )
                break;
            if ( wadaw[i] == v11[i] + 155 - s[i] )
                ++v13;
        }
        if ( v13 == v12 )
            printf("Correct!\n", *(_QWORD *)s, v7, v8, v9, v10);
        else
            printf("Wrong.\n", *(_QWORD *)s, v7, v8, v9, v10);
        }
        else
        {
            printf("Maaf, anda terlalu 'pro' untuk masuk portal kley.\n", *(_QWORD *)s, v7, v8, v9, v10);
        }
    }
```

```

    return 0;
}

```

Terdapat sebuah string yang disimpan di variable **s**, yaitu **d4WsnTwJspaFwAl3yXzMYWGRqwaeyN8E7**. Lalu inputan kita (flag) dimasukkan ke variabel **v11**. Lalu dari percabangan pertama, didapatkan kesimpulan bahwa panjang **v11** harus sama dengan panjang **s**. Lalu setiap karakter pada **v11** akan diperiksa apakah **v11[i] + 155 - s[i] = wadaw[i]**. Jika iya, maka increment variabel **v13**. Program lalu akan mengeluarkan output "Correct!" jika nilai **v13** sama dengan panjang **s**, artinya pemeriksaan pada setiap karkter **v11** semuanya bernilai benar.

Jadi untuk mendapatkan nilai **v11** yang sebenarnya, kita dapat melakukan dengan pseudocode seperti berikut

```

for i = 0 to strlen(s)
    v[i] = wadaw[i] - 155 + s[i]

```

Untuk lebih mudahnya, dapat dibuat script sebagai berikut

```

wadaw = [ 165, 214, 179, 138, 168, 187, 137, 189, 137, 147, 153, 189, 133, 188,
          152, 219, 129, 182, 150, 178, 163, 172, 179, 192, 139, 143, 174, 171, 129, 182,
          209, 191, 225 ]

s = "d4WsnTwJspaFwAl3yXzMYWGRqwaeyN8E7"

flag = ""

for i in range(0,33):
    woi = wadaw[i] - 155 + ord(s[i])
    flag += chr(woi)

print flag

```

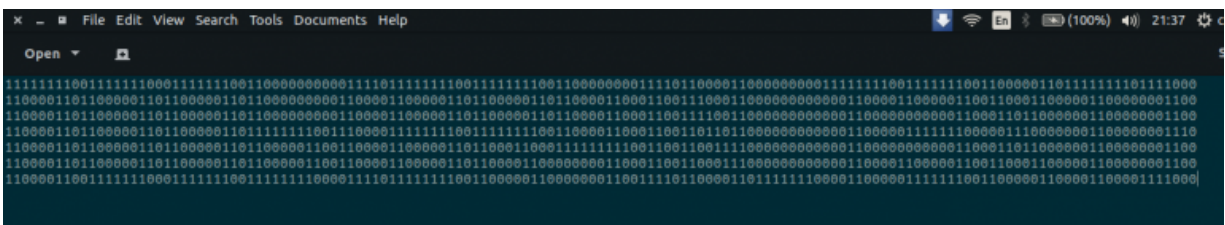
**Flag :noob{telah\_habis\_sudah\_waktu\_inih}**

## Rahasia – Misc 100pts



1507

C

Ja  
pe  
de  
pa

U

***F***

PR

EM

## N

Q1

**CATEGORIES**

CTF

**BE FIRST TO COMMENT**

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Enter Your Comment...

Your Name\*

Your Email\*

Your URL

Post Comment

# CLAYDAY BLOG

## ARCHIVES

JUNE 2017

MAY 2017

## LIFE





