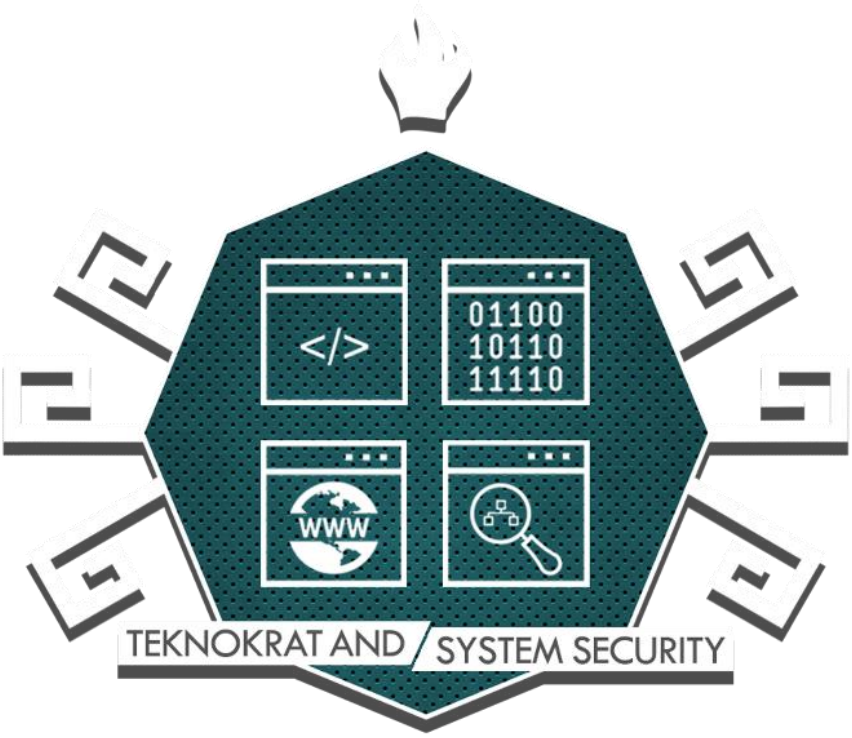
CTF Writeups By

TENESYS

"IDSECCONF 2016"

#fredrica



Judul : Sequence

Nilai : 100 pt

Kategori : Misc

Soal yang diberikan berupa ip address service soal yaitu 128.199.236.209 dengan port 17845, setelah coba untuk test koneksi dengan perintah `nc 128.199.236.209 17845`, muncul output pertanyaan untuk menjawab deret pola segitiga ke `-n`, dengan waktu tertentu dan semakin berkurang setiap pertanyaan. Ternyata ada 8 pertanyaan. Untuk menjawab pertanyaan ini dapat diselesaikan dengan script python seperti berikut,

```
from pwn import *
import math
import sys
sys.setrecursionlimit(10000)
r = remote('128.199.236.209',17845)
def pola(n):
      Un = ((0.5)*n)*( n + 1 )
      return Un
print r.recv()
for waktu in range(9):
      respon =  r.recv()
      print respon
      respon2 = respon.split(' ')
```

```
      nilai = respon2[-1]
      nilai = int(nilai.strip('\n'))

      coba = pola(nilai)
      coba = int(coba)
      r.sendline(str(coba))

print r.recv()
```

Ternyata tidak sampai disitu, kita dihadapi dengan pertanyaan bertipe lain yaitu deret Fibonacci ke `-n`, dan ternyata ada 7 pertanyaan,

```
from pwn import *
import math
import sys
sys.setrecursionlimit(10000)
r = remote('128.199.236.209',17845)
print r.recv()

def fib(n):
    a, b = 0, 1
    for i in range(0, n):
        a, b = b, a + b
    return a

for fibo2 in range(8):
        respon =  r.recv()
        print respon
        respon2 = respon.split(' ')
        nilai = respon2[-1]
        nilai = int(nilai.strip('\n'))
     nilai = nilai-1
        hasil = fib(nilai)
        r.send(str(hasil)+'\n')

print r.recv()
```

Pada tahap terakhir terdapat satu pertayaan yang berupa deret Fibonacci ke`-n` , akan tetapi n bernilai sangat besar dan waktu untuk menjawab tidak boleh lebih dari 2 detik,

```
from pwn import *
import math
import sys
sys.setrecursionlimit(10000)
r = remote('128.199.236.209',17845)

print r.recv()

def fib(n):
    a, b = 0, 1
```

```
    for i in range(0, n):
        a, b = b, a + b
    return a

respon =  r.recv()
print respon
respon2 = respon.split(' ')
nilai = respon2[-1]
nilai = int(nilai.strip('\n'))
nilai = nilai-1
hasil = fib(nilai)
r.send(str(hasil)+'\n')

print r.recv()
print r.recv()
print r.recv()
```

Jadikan satu semua script diatas menjadi berikut,

```
from pwn import *
import math
import sys
sys.setrecursionlimit(10000)
r = remote('128.199.236.209',17845)
def pola(n):
     Un = ((0.5)*n)*( n + 1 )
     return Un
print r.recv()
for waktu in range(9):
     respon =  r.recv()
     print respon
     respon2 = respon.split(' ')
     nilai = respon2[-1]
     nilai = int(nilai.strip('\n'))

     coba = pola(nilai)
     coba = int(coba)
     r.sendline(str(coba))

print r.recv()

def fib(n):
    a, b = 0, 1
    for i in range(0, n):
        a, b = b, a + b
    return a

for fibo2 in range(8):
        respon =  r.recv()
        print respon
        respon2 = respon.split(' ')
```

```
        nilai = respon2[-1]
        nilai = int(nilai.strip('\n'))
      nilai = nilai-1
        hasil = fib(nilai)
        r.send(str(hasil)+'\n')

print r.recv()

respon =  r.recv()
print respon
respon2 = respon.split(' ')
nilai = respon2[-1]
nilai = int(nilai.strip('\n'))
nilai = nilai-1
hasil = fib(nilai)
r.send(str(hasil)+'\n')

print r.recv()
print r.recv()
print r.recv()
```

Setelah di-running maka akan mendapat flag yaitu **flag{_mamat_dan_sekur_selalu_bersama_}**

Judul : Webwob

Nilai : 100 pt

Kategori : Web

Pada soal ini, kita diberikan alamat web yaitu *http://128.199.96.39/* Pada halaman itu pula telah diberi source codenya seperti berikut,

```
<?php

function length($x) {
      if (is_array($x))
            return count($x);
      return strlen($x);

}

require("flag.php");

$pass = $_GET["password"];

$ok = length($pass)==4;

for ($i=0; $i<length($pass); $i++) {
      if (strcmp($pass[$i], $password[$i])!=0) {
            $ok = false;
                print "invalid $i";
            break;
      }
}

if ($ok) {
      echo "The Flag is: ".$FLAG;
      exit(0);
} else {
      if (isset($_GET["password"]))
            print "Invalid";
}
```

Setelah source code tersebut dianalisa, kita akan mendapatkan flag apabila password yang kita inputkan sama dengan password yang ada di variable `$password`, maka password yang kita inputkan dibandingkan dengan strcmp, karena jumlah password yang diminta hanya 4 karakter, hal pertama yang terpikirkan adalah dengan cara bruteforce dengan bantuan aplikasi *Burp*. Karena pengecekan dilakukan perkarakter dan apabila ada pemberitahuan karakter yang salah, maka bruteforce dapat dilakukan satu karakter-satu karakter.

Password yang didapat adalah Ungu, setelah iinputkan dan mendapat flag : **flag{AVariant_Of_Strcmp}**

Judul : Kopi

Nilai : 50 pt

Kategori : Reversing

Soal yang diberikan berupa file zip dan setelah di ekstrak berupa file *.class*, Dengan bantuan tool online decompiler, kita dapatkan source seperti berikut,

```
import java.io.PrintStream;
import java.util.Stack;

class Kopi
{

    Kopi()
    {
        flag = new StringBuilder();
    }

    private String getFlag()
    {
        return flag.toString();
    }

    private boolean checkPassword(String s)
        throws Exception
    {
        String as[] = s.split("-");
        Stack stack = new Stack();
        Stack stack1 = new Stack();
        String as1[] = as;
        int j = as1.length;
        for(int k = 0; k < j; k++)
        {
            String s1 = as1[k];
            stack.push(Integer.valueOf(Integer.parseInt(s1)));
        }

        int i = ((Integer)stack.pop()).intValue();
        stack1.push(Integer.valueOf(i));
        j = ((Integer)stack.pop()).intValue();
        stack1.push(Integer.valueOf(j));
        while(!stack.empty())
        {
            int l = ((Integer)stack.pop()).intValue();
            if(l != i - j)
                return false;
            stack1.push(Integer.valueOf(l));
            i = j;
            j = l;
        }
        if(i * (j / i) != 1)
            return false;
        for(int i1 = 0; i1 < buff.length; i1++)
        {
```

```
            buff[i1] -= ((Integer)stack1.pop()).intValue();
            flag.append((char)buff[i1]);
        }

        return true;
    }

    public static void main(String args[])
    {
        if(args.length != 1)
        {
            System.out.println("Usage: Kopi <password>");
            return;
        }
        System.out.println((new StringBuilder()).append("Checking ...
").append(args[0]).toString());
        Kopi kopi = new Kopi();
        boolean flag1 = false;
        try
        {
            flag1 = kopi.checkPassword(args[0]);
        }
        catch(Exception exception)
        {
            System.out.println("Invalid password");
            return;
        }
        if(flag1)
            System.out.println((new StringBuilder()).append("The flag is:
").append(kopi.getFlag()).toString());
        else
            System.out.println("Invalid password");
    }

    private StringBuilder flag;
    private static int buff[] = {
        103, 109, 99, 106, 128, 81, 89, 126, 141, 156,
        163, 241, 351, 474, 715, 1097, 1664, 2668, 4251, 6890
    };

}
```

Dari source code diatas, password yang kita masukkan akan diubah menjadi integer kode ascii dan dimasukkan kedalam stack, kemudian pada isi stack pertama di masukkan kedalam stack kedua dengan pengecekkan kondisi. Dan apabila password yang kita masukkan sesuai dengan kondisi, maka nilai kode ascii nya akan melakukan proses pengurangan dengan array buff yang sudah ada. Karena kita sudah tahu format flag yaitu *flag{}*, kami mencoba melihat pattern yang digunakan untuk pengecekannya.

```
import sys
buff = [103, 109, 99, 106, 128, 81, 89, 126, 141, 156,163, 241, 351,
474, 715, 1097, 1664, 2668, 4251, 6890]
f=['f','l','a','g','{']
for a in range(len(f)):
      sys.stdout.write(str(buff[a]-ord(f[a]))+" ")
```

Dan didapatkan output *1 1 2 3 5*. Yang mana angka-angka tersebut merupakan deret Fibonacci, maka kita dapat langsung menemukan flagnya tanpa harus menganalasia algoritma pengecekannya.

```
import sys
buff = [103, 109, 99, 106, 128, 81, 89, 126, 141, 156,163, 241, 351,
474, 715, 1097, 1664, 2668, 4251, 6890]
fibo = [1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610,
987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025,
121393]
for a in range(len(buff)):
      sys.stdout.write(chr(buff[a]-fibo[a]))
```

Dan didapat string flag yaitu **flag{ILikeJavainCTF}**