HSCTF 3 Writeups

Oleh tim ***Tenesys***

High School Capture The Flag 3 adalah acara tahunan yang diadakan di USA diperuntukan bagi siswa-siswa SMA sederajat yang ada disana, namun pada event ini kami hanya ikut untuk meramaikan sekaligus menambah pengalaman. Tak banyak yang dapat kami selesaikan karena kesibukan aktivitas kami, Berikut sedikit writeups dari kami :

- ## Optional Survey – 50 Kategori *Non-Programming*

  Pada misi ini sebenarnya hanya point bonus saja karena kami diminta untuk mengisi survey mengenai pendapat tentang tim dan beberapa hal seperti pertanyaan yang menyangkut pada individu, lalu pada bagian akhir survey akan didapat flag yaitu : ***readytodotheactualcompetition***

- ## There's Always One – 100 Kategori *Cryptography*

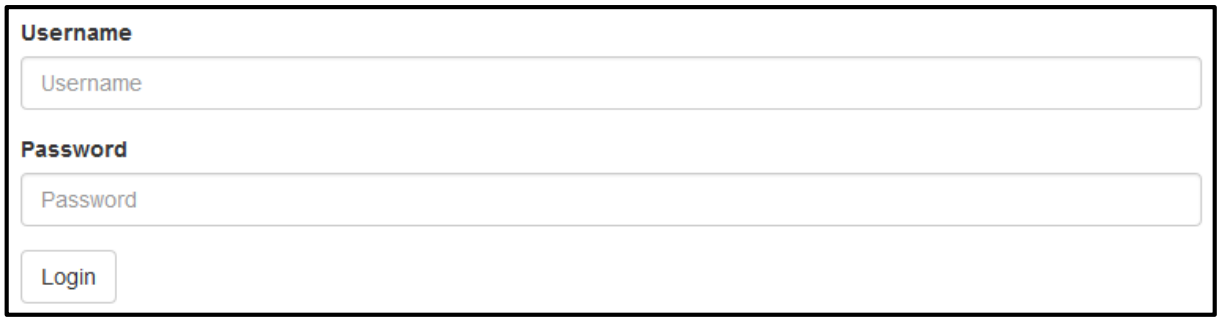
  Soal yang didapat berupa text yaitu :

  - You know what to do: jeaud_squiqh_syfxuh_fherbuc
  - Hint : Cipher named after Roman dude

  Langsung terpikir oleh kami bahwa ini merupakan chiper text jenis ***caesar chiper***, apabila di decode maka akan mendapatkan flag : ***token_caesar_cipher_problem***

- ## Login 1 – 100 Kategori *Exploitation*

  Didapat sebuah link login dengan menginputkan username dan password,

Pada bagian source akan menampilkan hal menarik yaitu,

```
<script>
    $(document).ready(function(){
        $("#login").submit(function(e){
            e.preventDefault();

            var username = $("#username").val();
            var password = $("#password").val();

            if(username == "admin" && password == "supersecure") {
                document.location = "success.php";
            } else {
                alert("Incorrect username and password!");
            }

        });
    });
</script>
```

Didapatkan informasi untuk ***username == admin*** dan ***password == supersecure*** lalu login dan mendapatkan flag yaitu : ***super_secure_javascript_login***

- **Login 2 – 100 Kategori *Exploitation***

Didapat sebuah link login yang sama persis seperti soal ***Login 1 – 100*** namun disini yang membedakan adalah pada bagian source yang akan menampilkan hal menarik yaitu,

```
<script>
    $(document).ready(function(){
        $("#login").submit(function(e){
            e.preventDefault();

            var username = $("#username").val();
            var password = $("#password").val();

            if(username == "admin" && md5(password) == "d5aa1729c8c253e5d917a5264855eab8") {
                document.location = "success.php?password=" + password;
            } else {
                alert("Incorrect username and password!");
            }

        });
    });
</script>
```

Didapatkan informasi untuk ***username == admin*** dan sebuah password yang di encrypt menggunakan md5, hanya perlu men-decrypt hash tersebut kamimendapatkan sebuah string ***freedom*** lalu login dan mendapatkan flag yaitu : ***super_secure_javascript_login_with_md5_support***

- **Thue 100 – 100 Kategori *Algorithms***

Soal yang didapat berupa penjelasan algoritma seperti berikut :

- www.dropbox.com/s/8esjlxrsowwu3g0/Thue%20100%20-%20100.txt

Pemecahan masalah adalah hanya bagaimana kita memainkan logika yang sudah tertera pada soal, sehingga kami dapatkan flag yang berupa : ***ab=ba;***

- **Keith vs DJ Khaled – 100 Kategori *Reversing***

Soal yang didapat berupa penjelasan algoritma seperti berikut :

- www.dropbox.com/s/drwscamvckcprfn/Reversing.java

Diberikan sebuah source program java dimana kami diharuskan untuk mendecode strings yang tertera agar mendapatkan flag :

```
import java.util.Base64;
import java.util.Scanner;

public class flag {
    public static String decode(String w) {
        String string = "";
        char c = 't';
        String[] bits = w.split("");
        for(int i = 0; i < bits.length; i++) {
            char y = bits[i].charAt(0);
            for (int v = 0;v<255;v++){
                if(y == (char)(Math.pow(v, 2) / 120)){
                    c = (char)v;
                }
            }
            bits[i] = c + "";
            string += bits[i];
        }
        return string;
    }

    public static String decode2(String w) {
        byte[] c = Base64.getDecoder().decode(w);
        w = new String(c);
        return w;
    }

    public static void main(String[]args) {

        String ans = "TmRmcFpVbEtmZFU=";
        System.out.println(decode(decode2(ans)));
    }
}
```

Apabila dirunning maka akan menampilkan flag yaitu = ***another_one***

- **Keith Smash – 100 Kategori *Reversing***

Soal yang didapat berupa penjelasan algoritma seperti berikut :

- www.dropbox.com/s/tious8uzrs9wdqm/plshalp.java

Diberikan sebuah source program java sama seperti pada misi diatas namun sedikit berbeda, berikut sedikit syntax yang kami perbaiki agar mendapatkan flag yaitu :

```
import java.util.Random;
import java.util.Scanner;

public class PlsHalp {
    public static void main(String[] args) {
        String tot = "my feet smell and nose runs";
        args = tot.split("");
        if(tot.equals("my feet smell and nose runs"))
            System.out.println("Use knee on frame: " + (args[0] + args[2] + args[4] + args[6]).
                replace(" ", "").hashCode());
    }
}
```

Flag = ***107996***

- **Keith Is A Troll– 100 Kategori *Exploitation***

Soal yang didapat berupa source code java,

- www.dropbox.com/s/imefn11k1kbjsdi/login1.java

```
import java.util.Scanner;

public class KeithLikesToTroll {
    public static void main(String[] args){
        int key;

        Scanner scn = new Scanner(System.in);
        System.out.print("Enter key: ");
        key = scn.nextInt();
        scn.close();

        if(1338557220 / key * key != 1338557220 && key > 0){
            System.out.println("Login succesful. The flag is the smallest key which will let you log in.");
        }else{
            System.out.println("Login rejected.");
        }
    }
}
```

Dijelaskan pada kode diatas bahwa jika kita menginputkan nilai terkecil dari perhitungan : ***1338557220 / key * key != 1338557220 && key > 0*** maka itu merupakan flagnya, lalu kami lakukan exploit pada kode diatas menjadi,

```
import java.util.Scanner;

public class Main {
    public static void main(String[] args){
        int kunci;
            for(kunci=1;kunci<=100;kunci++){
                if(1338557220 / kunci * kunci != 1338557220 && kunci > 0){
                    System.out.println("Login sukses. Flag adalah kunci terkecilnya.");
                }else{
                    System.out.println("Login ditolak.");
                }
            }
    }
}
```

Maka akan didapat hasil nilai terkecilnya adalah : ***8***

- **Keith Is A Troll 2 – 100 Kategori *Exploitation***

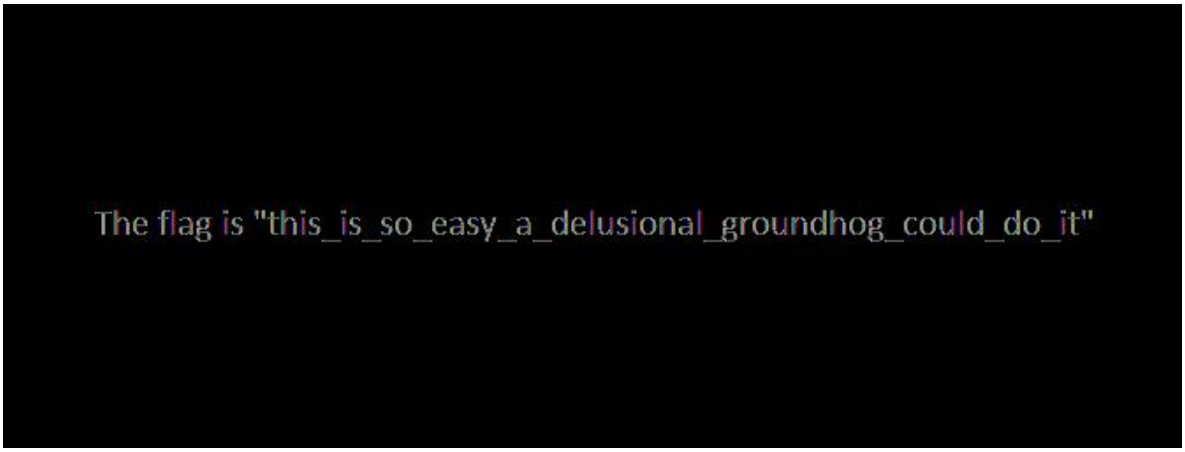
Didapat sebuah source code javayang hampir sama seperti soal ***Keith Is A Troll – 100***

- www.dropbox.com/s/yrza3kx4nmbsm7u/login2.java

Namun disini yang membedakan adalah pada bagian variabel kunci dimana angka lebih kecil dibandingkan soal sebelumnya berupa : ***24.0 / key * key != 24.0 && key > 0*** langkah yang kami lakukan pun sama, hanya perlu meng-exploit kode diatas dan akan mendapat sebuah flag yaitu : ***47***

- **Black Square – 100 Kategori *Forensics***

  Terdapat soal yang merupakan sebuah gambar, namun hanya gambar hitam kosong yang langsung terpikirkan oleh kami untuk mencoba menggunakan photshop dan sedikit memainkan pada bagian curves maka akan tampak flag yang tersembunyi,



  Yap, flag sudah tampil yaitu : ***this_is_so_easy_a_delusional_groundhog_could_do_it***

- **Keith's Party – 200 Kategori *Cryptography***

  Soal yang didapat berupa chipertext yang bertipe subtitusi seperti berikut :

  - ANURT MPT EPPM

    OUJWIOZPIN ANPGQFN ENPD XPJJFN ONBJGUJF

    BRM OUJWB MPVV EPN ZPIN XUXGFN

  Apabila didecode akan menampilkan hasil yang merupakan flag :

  - ***BRING DOG FOOD***

    PICK UP YOUR BROTHER FROM SOCCER PRACTICE

    AND PICK A DOLL FOR YOUR SISTER

- **Permuted Numbers – 200 Kategori *Cryptography***

  Soal yang didapat :

  For any odd number p, 2 to the power of n mod p is a different value for each n that is at most p-1 and at least 1 (the value of ⁍x mod y⁍ is the same as the remained of x divided by y and is sometimes expressed as ⁍x%y⁍). The values range from 1 to p - 1.

  For example, when p is 5:

  when n is 1: (2 ^ 1) % 5 = 2

  when n is 2: (2 ^ 2) % 5 = 4

  when n is 3: (2 ^ 3) % 5 = 3

  when n is 4: (2 ^ 4) % 5 = 1

This function is called a permutation on (1,2,3,4) as it can be seen as an assignment of each of these numbers to another unique number within the set (ordered as (2, 4, 3, 1) in this case). A permutation can be used for encoding list of integers by running it on each value in the list. We've encoded the flag by transforming the character into numbers by their place in the alphabet (a -> 1, b -> 2, c -> 3, and so on), with '{' going to 27, and '_' going to 28. We then used the above method with p set to 29.
(23, 24, 2, 23, 1, 10, 2, 26, 28, 23, 1, 5, 3, 13, 11, 1, 24, 2, 13, 16, 1, 23, 27, 1, 4, 13, 3, 2, 18, 1, 2, 6, 23, 3, 13, 1, 2, 7, 7)

Pemecahan masalah :

```
import sys
def permut(n):
    for a in range(1,n):
        c = (2**a)%n
        sys.stdout.write(str(c)+",")

f = [23, 24, 2, 23, 1, 10, 2, 26, 28, 23, 1, 5, 3, 13, 11, 1, 24, 2, 13, 16, 1, 23, 27, 1, 4,
    13, 3, 2, 18, 1, 2, 6, 23, 3, 13, 1, 2, 7, 7]
j = {2 : 'A',4 : 'B',8 : 'C',16 : 'D',3 : 'E',6 : 'F',12 : 'G',24 : 'H',19 : 'I',9 : 'J',18 : '
    K',7 : 'L',14 : 'M',28 : 'N',27 : 'O',25 : 'P',21 : 'Q',13 : 'R',26 : 'S',23 : 'T',17 : 'U'
    ,5 : 'V',10 : 'W',20 : 'X',11 : 'Y',22 : 'Z',15 : ' ',1 : '_'}
for c in f:
    sys.stdout.write(j[c])
```

Flag = ***THAT_WASNT_VERY_HARD_TO_BREAK_AFTER_ALL***

- ## Had Had Had – 200 Kategori *Algorithms*

Soal yang didapat :

Eve and Eva were in class. They both tried to describe a man that was once sick. Eve said "The man had a cold." Eva said "The man had had a cold." According to English grammar, Eva was correct.

Now imagine their two teachers, Bill and Bob: Bob was a little off, and said that "Eve, while Eva had had 'had had', had had 'had'; 'had' had had the better grammar." Bill corrected him, saying "Eva, while Eve had had 'had', had had 'had had'; 'had had' had had the better grammar."

Continuing this pattern, the knowledgeable supervisor would note that "Bill, while Bob had had 'had had had had had had had had had had', had had 'had had had had had had had had had had

Pemecahan masalah :

```
a=1
b=2
for c in range(2,101):
    d = (b+2)+(a+2)+(a+2)
    e = (a+2)+(b+2)+(b+2)
    a = d
    b = e
print a
```

Flag yang didapat = ***773066281098016996554691694648431909053161282998***

- **Wondrous Numbers – 200 Kategori*Algorithms***

Soal yang diberikan :

- Legend has it that, given an infinite number of steps, you can reduce any given number 'n' to 1 by repeating the following steps:

  - If the number is even, divide by two.

  - If the number is odd, multiply it by three and add one.

  What number between 1 and 100 requires the largest amount of these steps before 1 is reached?

Pemecahan masalah :

```
def num(n,a):
    if (n==1):
        return a
    if (n%2==0):
        n=n/2
        a+=1
        return num(n, a)
    if (n%2!=0):
        n = (n*3)+1
        a+=1
        return num(n, a)
b = num(1,1)
for a in range(1,101):
    c = num(a,1)
    if(b<c):
        b = c
        d = a
print d
```

Flag yang didapat = ***97***

- **Black Square 2 - 300 Kategori *Forensics***

Soal yang didapat adalah sebuah gambar, apabila gambar tersebut diterangkan, akan menampilkan beberapa warna pixel yang berbeda dimana itu merupakan nilai dari 1, sedangkan yang bewarna lain merupakan nilai dari 0, lalu kami mencoba membuat script agar flag yang ada dalam gambar dapat terekstrak, yaitu seperti berikut :

```
import os, sys
import Image
import binascii
import base64

im = Image.open("BlackSquare2.png")
im = im.convert('RGB')
a=""
for y in range(0,398):
    for x in range (0,16):
        r, g, b = im.getpixel((x, y))
        a += str(b)
n = int(a, 2)
imgstring = binascii.unhexlify('%x' % n)


imgdata = base64.b64decode(imgstring)
filename = '2.png'
with open(filename, 'wb') as f:
    f.write(imgdata)

im = Image.open("2.png")
im = im.convert('RGB')
a=""
for y in range(0,51):
    for x in range (0,32):
        r, g, b = im.getpixel((x, y))
        if(b==255):
            a += "0"
        else:
            a += "1"
n = int(a, 2)
print base64.b64decode(binascii.unhexlify('%x' % n))
```

Setelah di running akan menampilkan flag yang berupa =

cea682feb5f4691e10905cf4c976b716292d3cd56537dc47d68879e6f7504ae53c66932a6f9ab8b7924a383d3fce85381af7fa69c3c2c72a1627314ed76c1c63