PETIR CYBER SECURITY

[2024]

Nama Lengkap	:	Samuel Christian
Jurusan	:	Cyber Security
NIM	:	2702247600
Username	:	Shiroz

Daftar Isi

Forensic

Perfect Network Graphics

Langkah Penyelesaian:
Pertama-tama kita membaca terlebih dahulu file txt yang telah diberikan.

Sample yang didapat adalah sebagai berikut dengan jumlah yang sangat banyak.

August 02, 2024 16:20:02.012550 GET /?user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=0%20AND%20SLEEP(3)%20AND%20%221%22=%221.

Ini merupakan jenis blind sql injection

Yang apabila kita terjemahkan akan mendapatkan ini:

Chop" AND ASCII(SUBSTR((SELECT passwd FROM accounts ORDER BY user LIMIT 0,1),1,1))=1 AND SLEEP(3) AND "1"="1”

Ini merupakan pemeriksaan apakah ASCII dari karakter pertamanya adalah 1. Jika benar, maka akan ada jeda selama 3 detik.

Mengetahui hal tersebut maka kita bisa mencoba extract password apa yang benar dan merupakan flagnya.

Tetapi karena tanggal dan semacamnya membuat codingan tidak dapat membacanya maka dibutuhkan codingan untuk menghilangkan dan menyisakan user samapai angka terakhir.

```python
input_file_path = 'C:/code/log.txt'
output_file_path = 'C:/code/cleaned_log.txt'

with open(input_file_path, 'r') as infile, open(output_file_path, 'w') as outfile:
    for line in infile:
        relevant_part_start = line.find('/?') + 2

        cleaned_line = line[relevant_part_start:]
        outfile.write(cleaned_line)

print(f"Cleaned log saved to {output_file_path}")
```

Setelah melakukan pembersihan isi dari log txt berubah menjadi:

```
user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=0%20AND%20SLEEP(3)%20AND%20%221%22=%221
```

Dari sini kita bisa langsung memasukkan kodingan untuk mengextract password yang ada pada injection tersebut

```python
password_dict = {}

for line in log_lines:
    try:
        start_pos = line.index('),') + 2
        end_pos = line.index(',1))=')
        position = int(line[start_pos:end_pos])

        ascii_start = line.index(')=') + 2
        ascii_end = line.index('%20AND%20SLEEP(3)')
        ascii_value = int(line[ascii_start:ascii_end])

        if 32 <= ascii_value <= 255:
            char = chr(ascii_value)
            password_dict[position] = char
            print(f"Position: {position}, ASCII: {ascii_value}, Char: {char}")
    except ValueError as e:
        print(f"Error processing line: {e}")
        continue

if password_dict:
    password = ''.join([password_dict[i] for i in sorted(password_dict)])
    print(f'\n{password}')
```

Inti dari koding ini adalah untuk membaca log yang berisi SQL Injection, mendapatkan posisi dan karakter dari password, dan habis itu kita Menyusun ulang password dari informasi yang didapat.

Untuk log lines bisa diisi dengan isi dari log.txt yang sudah dibersihkan seperti berikut:

```
log_lines = [
    "user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=0%20AND%20SLEEP(3)%20
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=1%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=2%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=3%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=4%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=5%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=6%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=7%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=8%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=9%20AND%20SLEEP(3)%20AND%
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=10%20AND%20SLEEP(3)%20AND
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=11%20AND%20SLEEP(3)%20AND
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=12%20AND%20SLEEP(3)%20AND
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=13%20AND%20SLEEP(3)%20AND
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=14%20AND%20SLEEP(3)%20AND
"user=Chop%22%20AND%20ASCII(SUBSTR((SELECT%20passwd%20FROM%20accounts%20ORDER%20BY%20user%20LIMIT%200,1),1,1))=15%20AND%20SLEEP(3)%20AND
```

Ketika kita coba codingannya untuk semua line yang ada maka kita akan mendapatkan output:

GoSubmitTheFlag~!ng_t1m3_b4s3d_SQL_1nject!0n}

Kalau kita lihat itu sudah ada format dari flag } tetapi awalnya tidak dimulai dengan PETIR. Setelah, konsultasi dengan probset kalau memang flagnya akan terprint dari password langsung. Maka saya mencoba dari 2000 line lebih terlebih dahulu.

output yang didapatkan
PETIR{y4y_a!56

Artinya kodingannya sudah benar tetapi log line yang dimasukkan terlalu banyak. Dan kita hanya perlu mengecek beberapa kali.
Akhirnya ketemu pada line kode sebanyak 5300an yang Dimana outputnya:

GETIR{y4y_an4lyz!ng_t1m3_b4s3d_SQL_1nject!0n}

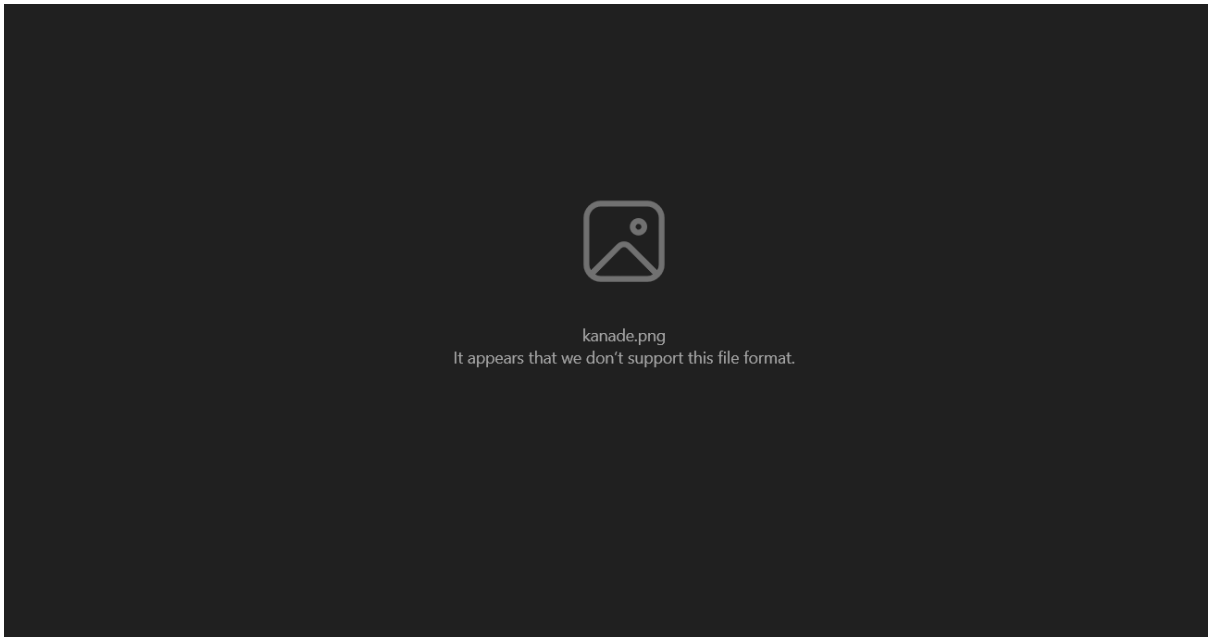
Karna kita sudah tau format flag maka flagnya adalah

PETIR{y4y_an4lyz!ng_t1m3_b4s3d_SQL_1nject!0n}

Pithecanthropus

Langkah Penyelesaian:
Pertama-tama kita membaca terlebih dahulu file telah diberikan.

Dari sini kita mendapatkan kodingan dan sebuah png yang tidak dapat dibuka:




```
from PIL import Image
from random import randint

def to_bytes(i, len):
    return i.to_bytes(len, byteorder='big')

def boo(f, pix, x, y, len):
    try:
        r,g,b,a = pix[x,y]
    except:
        r,g,b = pix[x,y]
    if len == 2:
        r,g,b = (r*2)^0x11, (g*2)^0x12, (b*2)^0x13
    f.write(to_bytes(r ^ randint(50,100), len))
    f.write(to_bytes(g ^ randint(50,100), len))
    f.write(to_bytes(b ^ randint(50,100), len))

def enhance(w, h, pix):
    for y in range(h):
        for x in range(w):
```

```
            ran = randint(1,20)
            len = 2 if (y+1) % ran == 0 else 1
            if len == 2:
                f.write(b'DOPE')
            boo(f, pix, x, y, len)

print('++  PerfectNG, your perfect PNG enhancer')
print('++  "Not Portable, but Perfect!"')
name = input('++  Please input the image file name: ')

try:
    img = Image.open(name)
    pix = img.load()
    w,h = img.size
    img.close()
except:
    print('++  Invalid image file')
    exit()

sign = b'PerfectNG' + to_bytes(w,2) + to_bytes(h,2)
f = open(name, 'wb')
f.write(sign)
f.write(b'DAMN')

enhance(w, h, pix)

f.write(b'DONE')
f.close()

print('++  Done! Your image has been enhanced!')
```

Kodingan ini intinya membuat file gambar png menjadi acak, diberikan perubahan pada piksel warna. Sehingga membuat png tidak bisa dibaca jadi cara kita mendapatkan flag adalah dengan membalikkan logika dari kodingang tersebut. Dengan kata lain kita hanya perlu memodifikasi kodingan yang telah diberikan untuk membuka png yang telah diberikan.

```python
from PIL import Image
from random import randint

def from_bytes(data):
    return int.from_bytes(data, byteorder='big')

def undo_boo(data, pix, x, y, byte_len):
    r = from_bytes(data[:byte_len])
    g = from_bytes(data[byte_len:2*byte_len])
    b = from_bytes(data[2*byte_len:3*byte_len])

    if byte_len == 2:
        r = (r ^ 0x11) // 2
        g = (g ^ 0x12) // 2
        b = (b ^ 0x13) // 2

    r = r ^ randint(50, 100)
    g = g ^ randint(50, 100)
    b = b ^ randint(50, 100)

    pix[x, y] = (r, g, b)
    return 3 * byte_len

def recover_image(filename):
    with open(filename, 'rb') as f:
        data = f.read()

    if not data.startswith(b'PerfectNG'):
        print('Invalid file format')
        return

    w = from_bytes(data[9:11])
    h = from_bytes(data[11:13])
    data = data[17:]

    img = Image.new('RGB', (w, h))
    pix = img.load()

    i = 0
    x, y = 0, 0
    while i < len(data) and y < h:
        if data[i:i+4] == b'DOPE':
            i += 4
            byte_len = 2
        else:
            byte_len = 1

        if i + 3 * byte_len > len(data):
            break

        try:
            i += undo_boo(data[i:], pix, x, y, byte_len)
        except IndexError:
            break

        x += 1
        if x >= w:
            x = 0
            y += 1

    img.save('c:/code/recovered.png')
    print('Image recovered as recovered.png')

recover_image('C:/code/kanade.png')
```

Dari sini kita mendapatkan gambar yang telah disembunyikan

Namun, sayangnya saya masih belum dapat mengubah warna dari gambar tersebut sampai textnya dapat dibaca maka progress saya hanya sampai di sini. Saya telah mencoba mengubah hue dan semacamnya tetapi masih gagal dan tidak menghasilkan text yang dapat dibaca dari png tersebut.