WRITE-UP CTF
ARA 2023
(gemush)

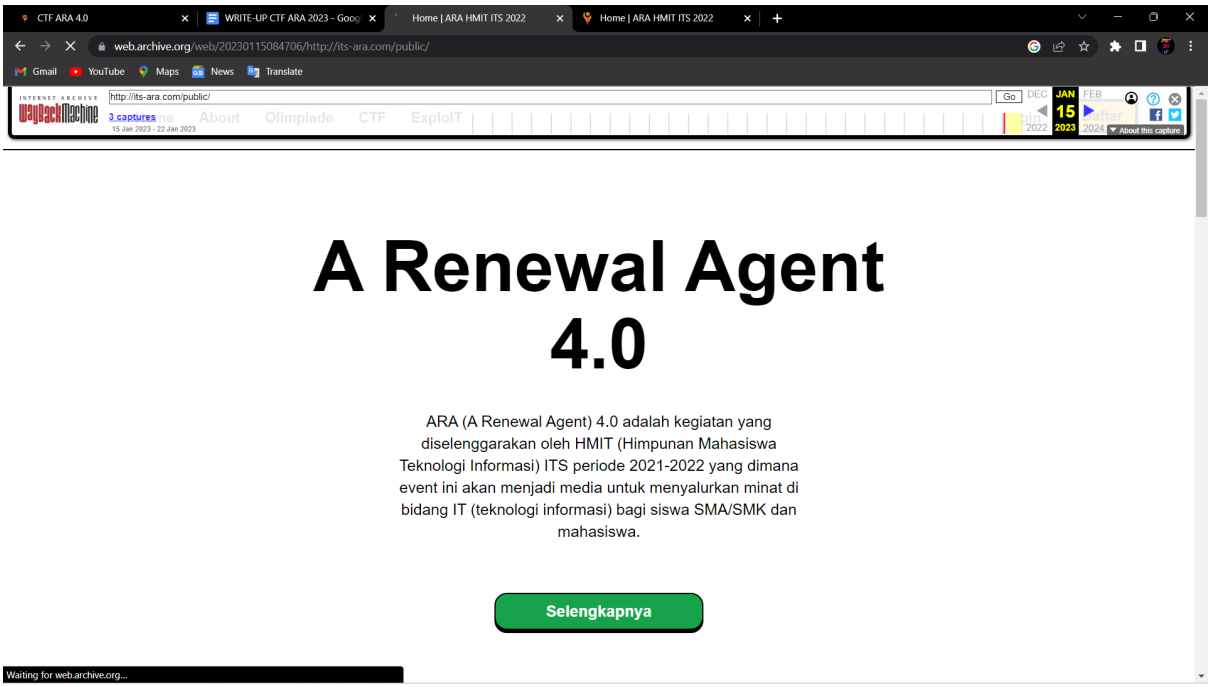
OSINT

- **Time Machine**

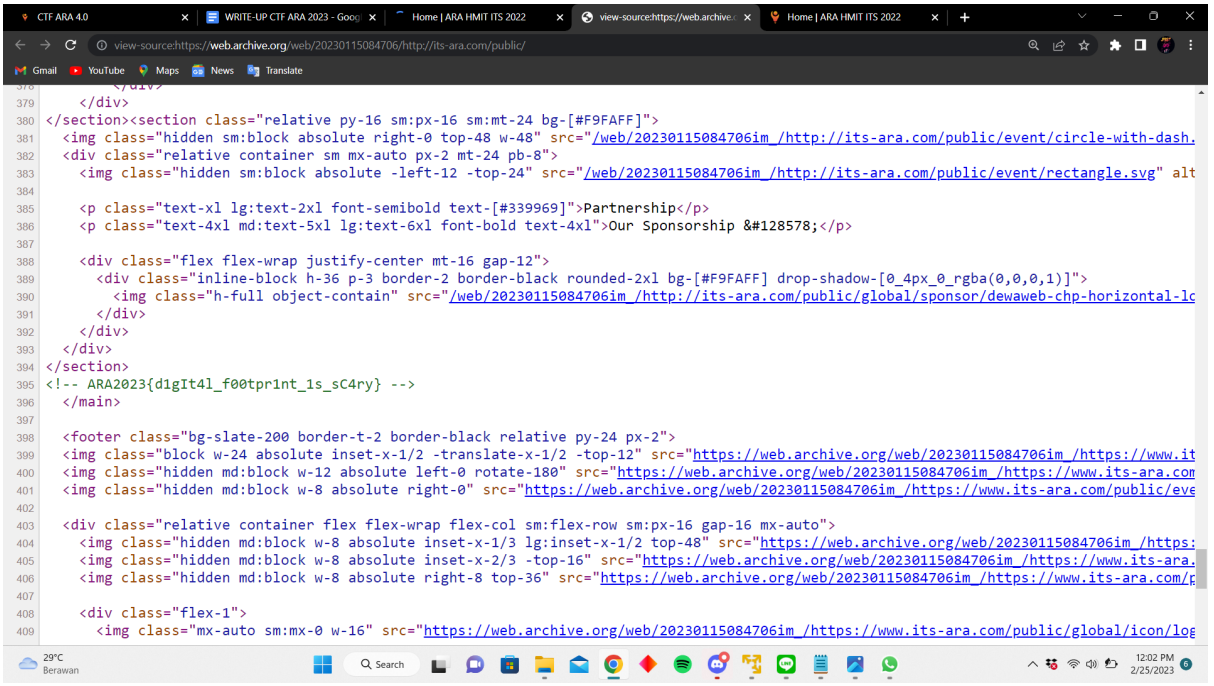
Description:
There was a secret leaked on Official ARA Website. It can only seen on January 22nd 2023. Can you turn back the time?

Steps:

1. Dari soal tersebut diketahui bahwa kita harus membuka web pada tgl 22 januari 2023.
2. Saya menggunakan wayback machine yang terdapat pada internet untuk mengakses halaman web https://www.its-ara.com/public/



3. setelah membuka web pada tgl 22 januari berikutnya saya membuka page sourcenya dan didapatkan lah flagnya



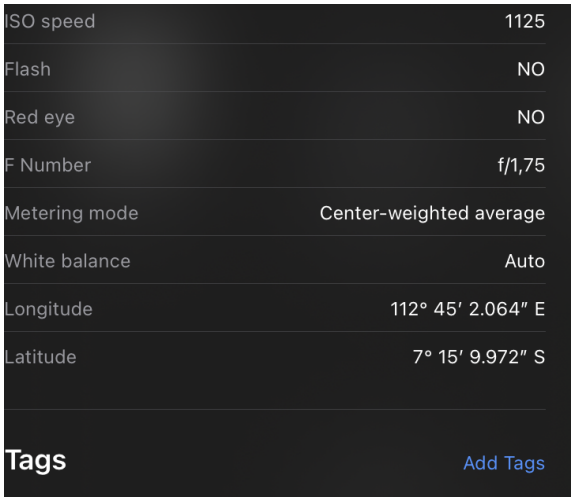
4. flag : ARA2023{d1gIt4l_f00tpr1nt_1s_sC4ry}

- **BACKROOM**

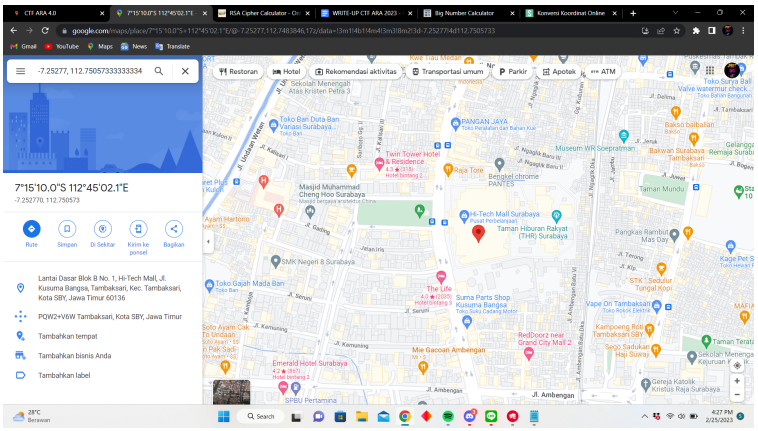
Description:
I found a place that give me a backroom vibes. I think I like this place, so I give this place 5 star. Can you find this place?

Steps:

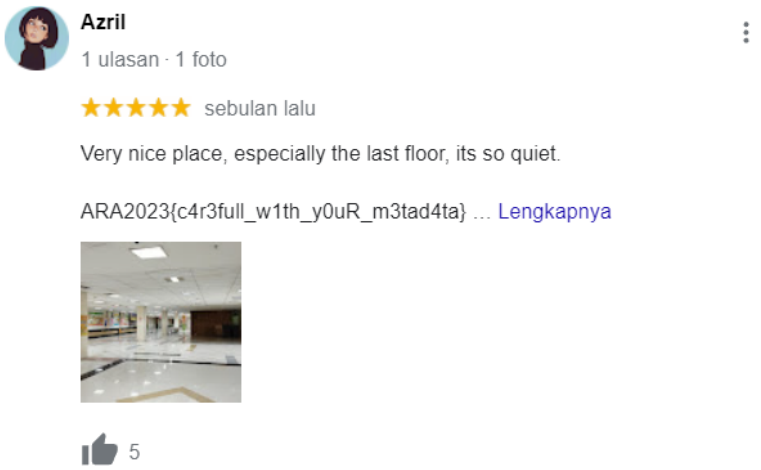
1. Download attachment yang diberikan
2. Ketika attachment terdownload buka details lalu terlihat ada Longtitude dan juga Latitude



3. Search menggunakan google maps



4. Mencari 1 per satu di google maps lalu ditemukan sebuah kolom komentar dengan gambar dan flag seperti dibawah



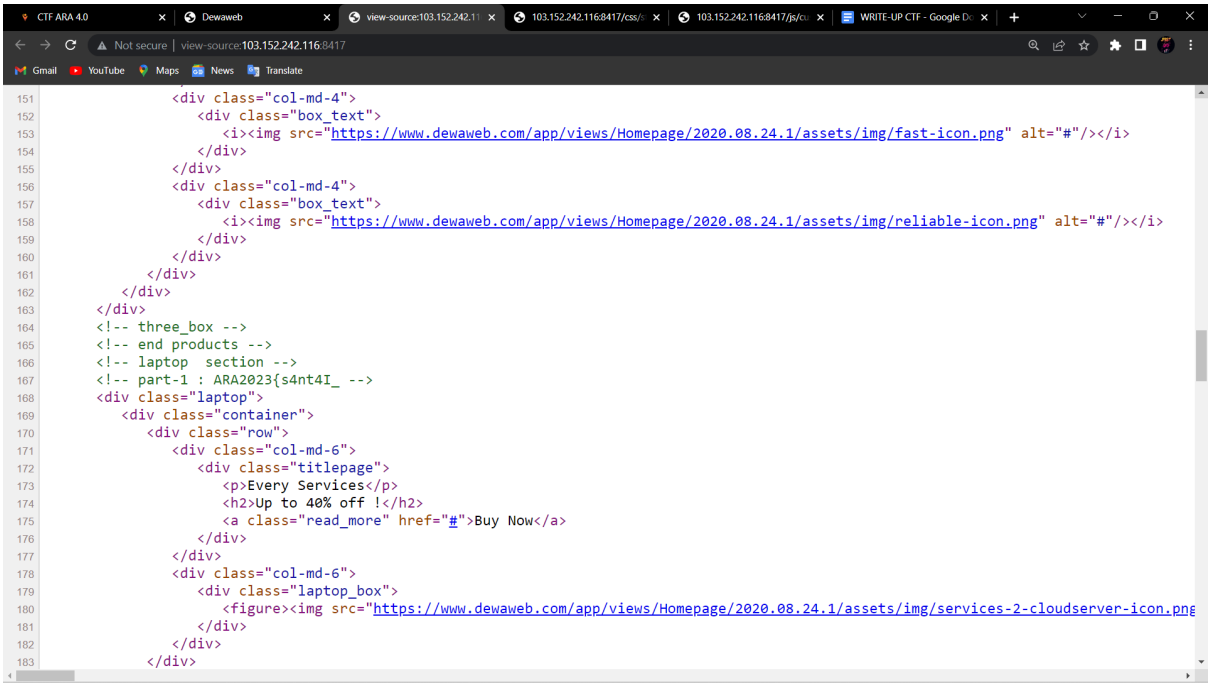
flag: ARA2023{c4r3full_w1th_y0uR_m3tad4ta}

Web Exploitation

- **Dewaweb**

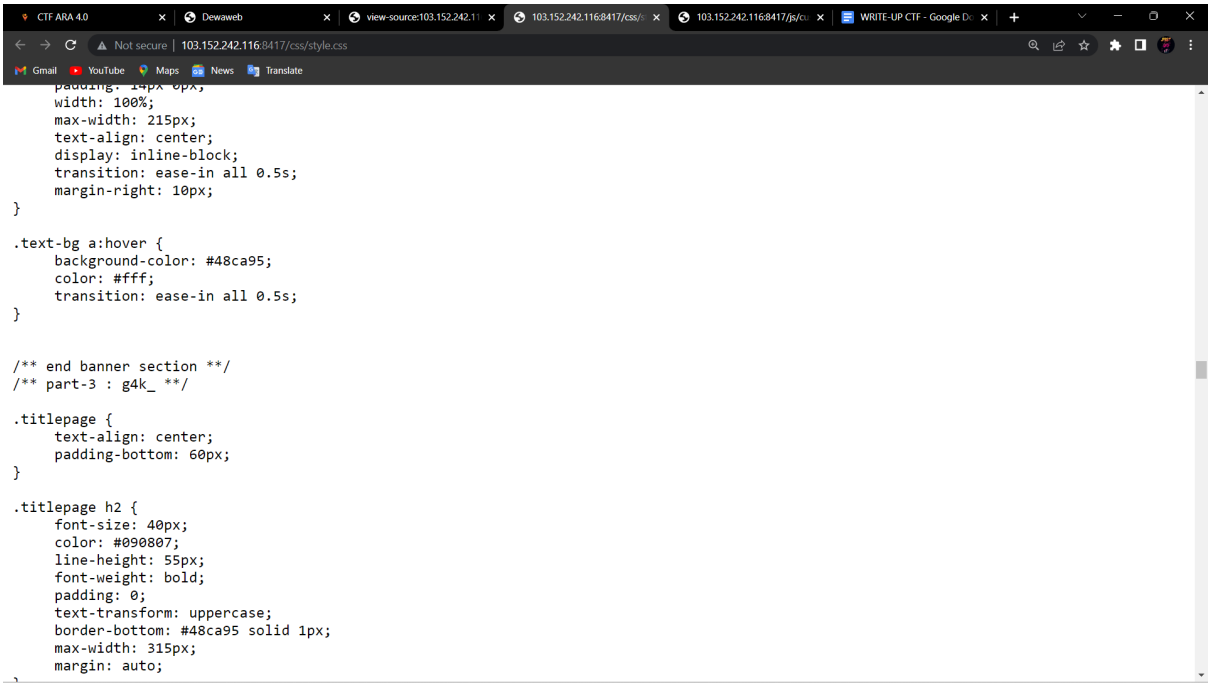
Description:
Dewaweb sedang mencari talenta terhebat!
Kamu adalah seorang inspektur terkenal yang telah dikenal mampu untuk memecahkan seluruh teka-teki. Tidak ada sesuatu yang luput dari penglihatanmu, bahkan untuk sesuatu yang tidak terlihat oleh mata orang biasa. Dewaweb mencari orang sepertimu.
Saat ini Dewaweb ingin menguji keahlian analisamu. Coba temukan apa yang Dewaweb sembunyikan di website ini. Buktikan bahwa kamu adalah seseorang yang pantas untuk Dewaweb!
http://103.152.242.116:8417/

Steps:
1. pada soal terdapat link website target yang dapat diakses
2. ketika diakses dan buka page sourcenya ditemukan flag part 1



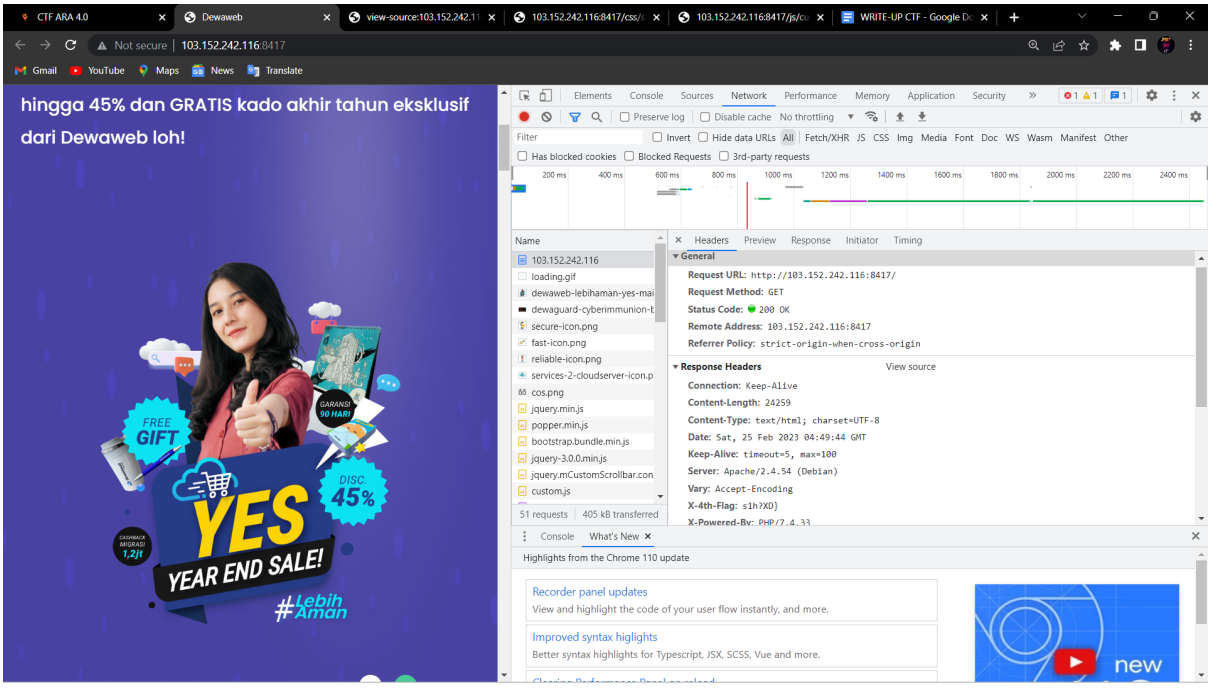
3. lalu pada bagian bawah page source terdapat “js/custom.js” dan ketika dibuka didapatkan flag part 2 di bagian paling bawah

4. di bagian page source tersebut juga terdapat “css/style.css” dan didapatkan flag part 3



```
     width: 100%;
     max-width: 215px;
     text-align: center;
     display: inline-block;
     transition: ease-in all 0.5s;
     margin-right: 10px;
}

.text-bg a:hover {
     background-color: #48ca95;
     color: #fff;
     transition: ease-in all 0.5s;
}


/** end banner section **/
/** part-3 : g4k_ **/

.titlepage {
     text-align: center;
     padding-bottom: 60px;
}

.titlepage h2 {
     font-size: 40px;
     color: #090807;
     line-height: 55px;
     font-weight: bold;
     padding: 0;
     text-transform: uppercase;
     border-bottom: #48ca95 solid 1px;
     max-width: 315px;
     margin: auto;
```

5. dan part terakhir didapatkan dari tab network pada inspect source dengan mengecek response headernya



6. maka hasilnya adalah
   part-1 : ARA2023{s4nt4l_
   part-2 : dUlu_ */
   part-3 : g4k_ **/
   part-4 : s1h?XD}

   flag: ARA2023{s4nt4l_dUlu_g4k_s1h?XD}

Forensic

- **Thinker**

Description:
I always overthink about finding other part of myself, can you help me?

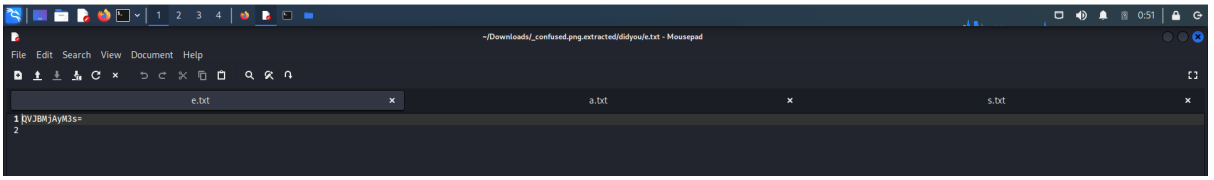
Attachments

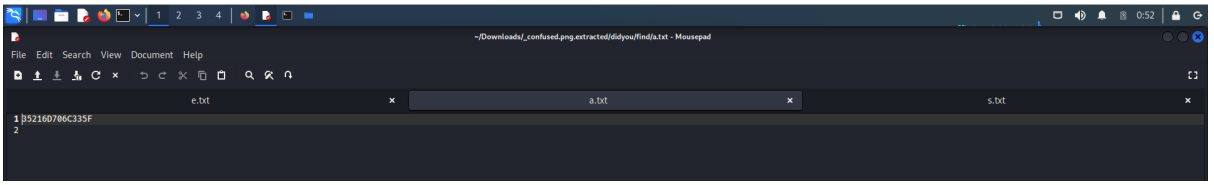
Steps:

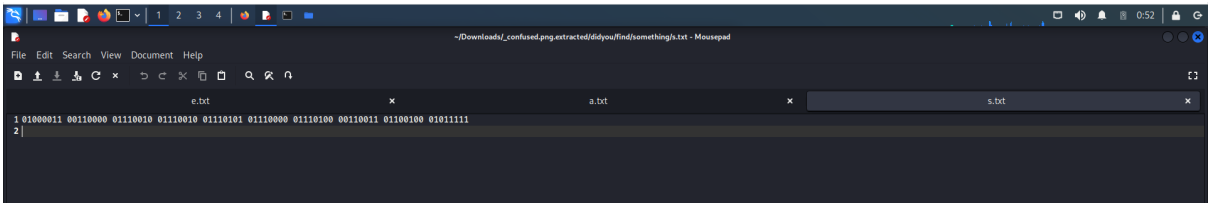
1. pada soal terdapat file attachment berupa gambar png.
2. ketika dilakukan binwalk terdapat banyak file di dalamnya

```
┌──(kali㉿kali)-[~/Downloads]
└─$ binwalk -e confused.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 720 x 881, 8-bit/color RGB, non-interlaced
6170          0×181A          Zlib compressed data, best compression
321663        0×4E87F         TIFF image data, big-endian, offset of first image directory: 8
321693        0×4E89D         Zip archive data, at least v1.0 to extract, name: didyou/
321758        0×4E8DE         Zip archive data, at least v1.0 to extract, compressed size: 13, uncompressed size: 13, name: didyou/e.txt
321841        0×4E931         Zip archive data, at least v1.0 to extract, compressed size: 10568, uncompressed size: 10568, name: didyou/find.zip
332460        0×512AC         End of Zip archive, footer length: 22
332726        0×513B6         End of Zip archive, footer length: 22
```

3. ketika di extract terdapat banyak file zip yang di dalamnya terdapat file .txt
4. lalu setelah mengextract semua file zip didapatkan “e.txt”, “a.txt”, “s.txt”, dan “y.png”





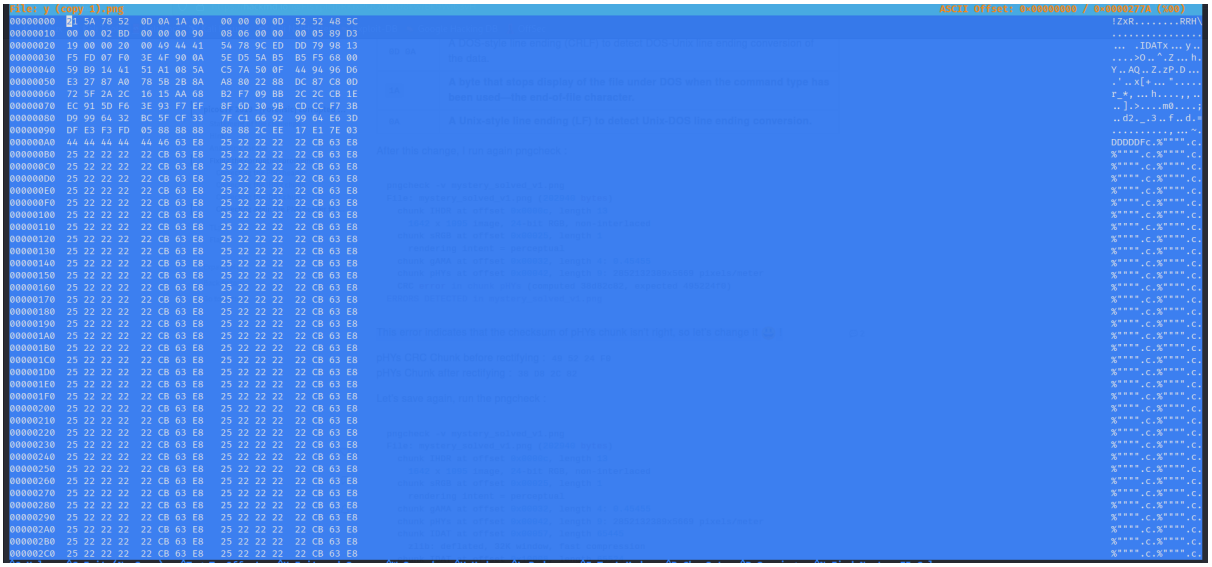


5. berikutnya masing-masing kode tersebut di translate menggunakan tools online sesuai dengan metode yang digunakan
   e.txt (base 64)
   QVJBMjAyM3s= → ARA2023{

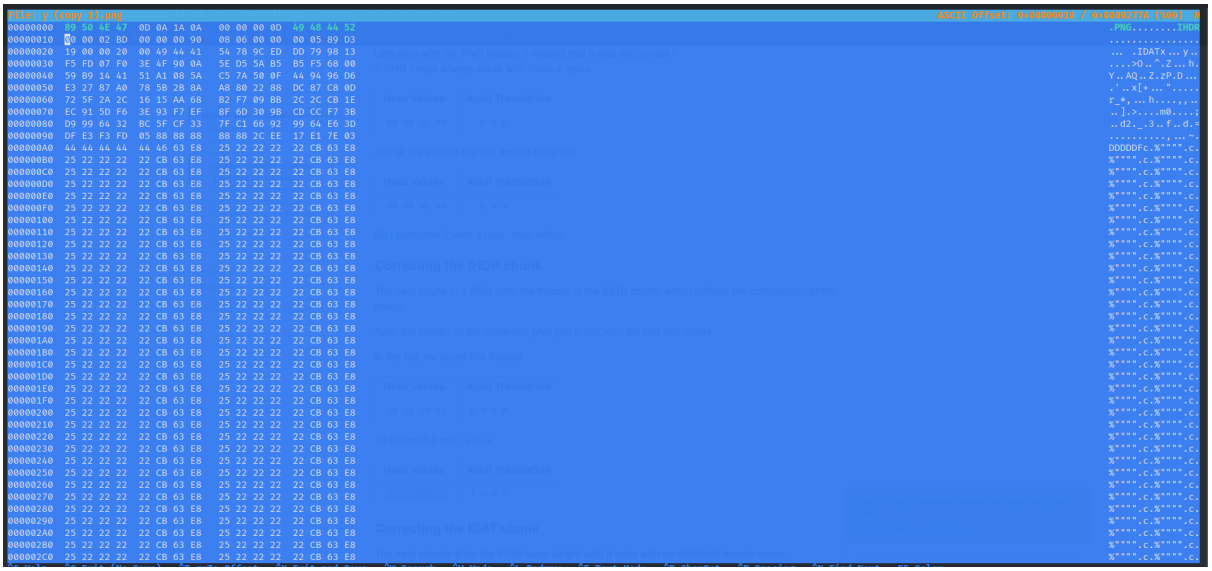
   a.txt (hex)
   35216D706C335F → 5!mpl3_

   s.txt (binary)
   01000011 00110000 01110010 01110010 01110101 01110000 01110100 00110011 01100100 01011111 → C0rrupt3d_

6. sedangkan untuk y.png merupakan sebuah file .png yang corrupted.



7. lalu saya merubah “!ZxR” (21 5A 78 52) menjadi “.PNG” (89 50 4E 47) dan “RRH\” (52 52 48 5C) menjadi “IHDR” (49 48 44 52)



8. maka file y.png skrg sudah dapat dibuka

49 109 52 103 101 53 125

9. dari gambar tersebut terdapat bilangan ascii dan saya rubah menggunakan online tools menjadi
   49 109 52 103 101 53 125 → 1m4ge5}

10. terakhir gabungkan semua bagian dan didapatkan flagnya
    flag: ARA2023{5!mpl3_C0rrupt3d_1m4ge5}

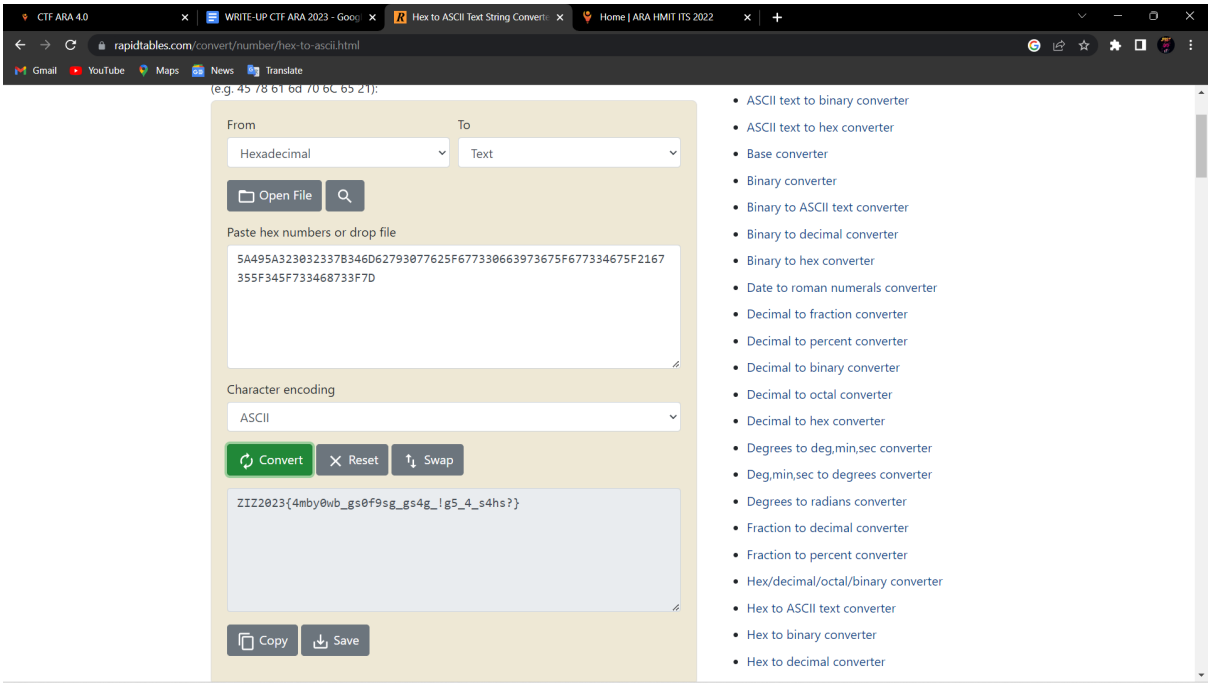
Misc

- **@B4SH**

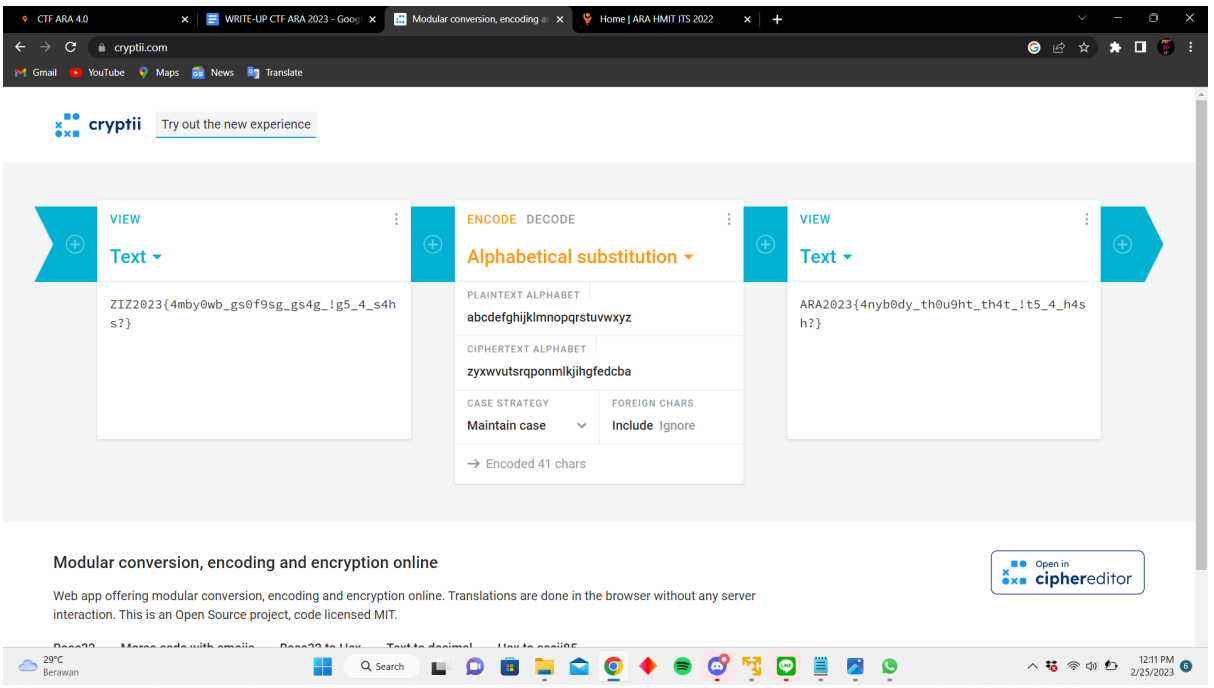
Description:
Ailee had just moved out to a boarding house in the countryside to escape the fast-paced and hectic city life. She was very excited to start her life with a new environment, she was very happy before she found out that the room she rented was very dark. Suddenly she found out 2 strange papers on the wall behind the door that says:
"5A495A323032337B346D62793077625F677330663973675F677334675F2167355F345F733468733F7D".
Help Ailee to find what's behind the text written on the paper.

Steps:

1. Dari kode yg terdapat pada soal diketahui bahwa itu merupakan bilangan hex, maka saya menggunakan online tools untuk merubah hex ke ascii



2. Didapatkan lah hasil “ZIZ2023{4mby0wb_gs0f9sg_gs4g_!g5_4_s4hs?}”
3. berikutnya saya menggunakan online tools untuk decode string yang didapatkan sebelumnya dengan alphabetical substitution.



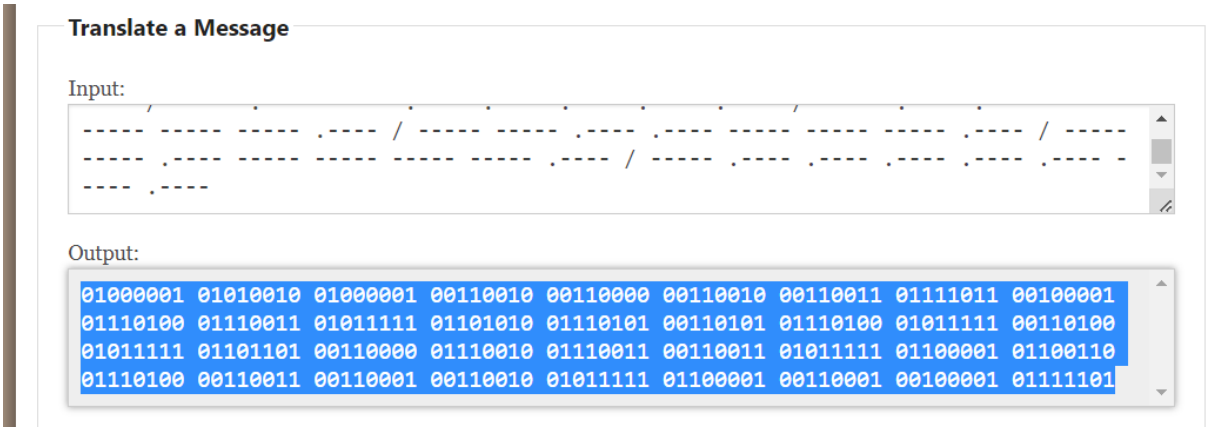
4. Dan didapatkan lah flagnya: ARA2023{4nyb0dy_th0u9ht_th4t_!t5_4_h4sh?}

- **D0ts N D4sh3s**

Description:
Albert was lost in a deep forest surrounded by a sea and tried to escape by sending a SOS signal containing a code.
Jack who works at a lighthouse realized that someone was sending a SOS signal and responses as fast as he can.
What do you think Albert tries to say?
Chall File :
https://drive.google.com/file/d/1h5ht0z64ChQ3v28o9Uq-GI0Uk21camH2/view?usp=sharing

Steps:

1. pada file tersebut terdapat titik dan strip atau yang dikenal dengan sandi morse
2. saya menggunakan online tools untuk merubah kode morse tersebut dan didapatkan hasil bilangan biner



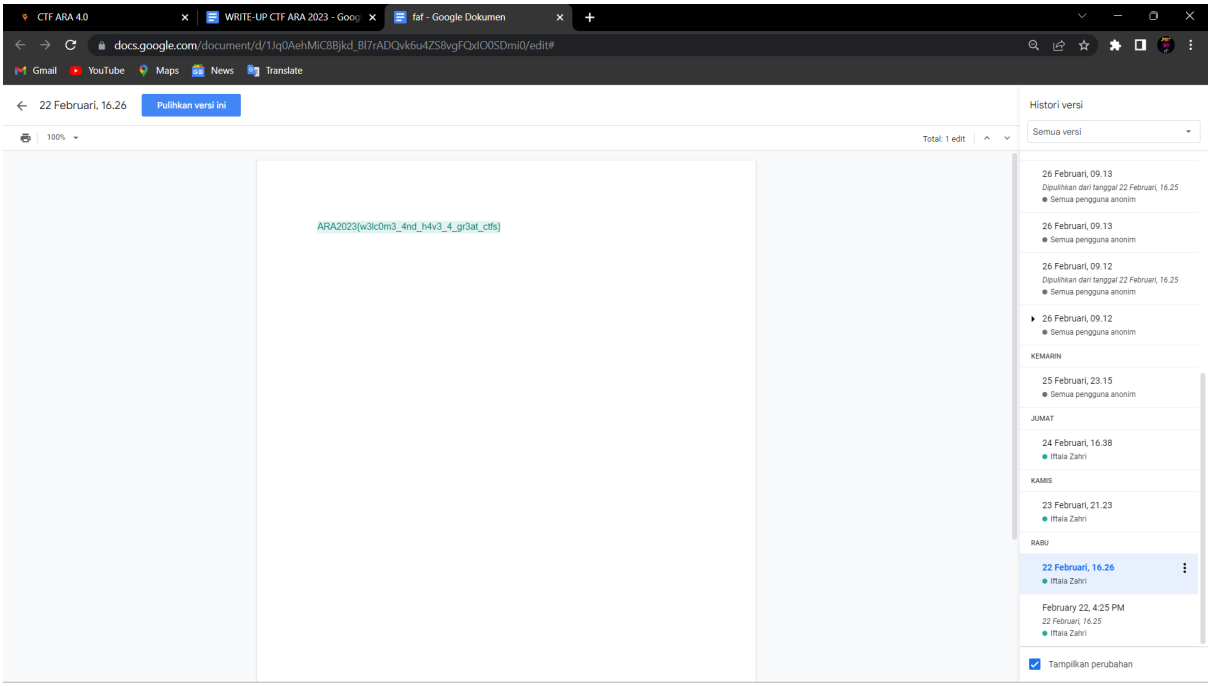
3. setelah itu saya merubah bilangan biner menjadi ascii atau text dan hasilnya adalah flag: ARA2023{!ts_ju5t_4_m0rs3_aft312_a1!}

- **in-sanity check**

Description:
Even the flag for sanity check is gone?
Attachments

Steps:

1. dari attachment tersebut meneruskan kita ke halaman google docs
2. lalu saya mencari di history versinya dan ditemukan flagnya di versi tgl 22 februari



flag: ARA2023{w3lc0m3_4nd_h4v3_4_gr3at_ctfs}

Cryptography

- **Secret Behind a Letter**

Description:
Melon and Edith went to a labyrinth and they should break the code written on a letter in a box in order to escape the labyrinth.
Open the letter and break the code
Attachments

Steps:

1. Dari file tersebut diketahui menggunakan RSA encryption dan diketahui

```
p:
125753336941212676905219718556916381441368103311882482367708803389058118834850641048656498349278197256176955544721003413618961620223116533015328101013442 73
q:
124974834261750724658521679369605262322848918767879810806711627835614115216758091122045736173583897427325462935027095851292058857260784924171098675123987 47
```

```
c:
360629344957317929086395350628331806510228135895355928518025722643282990274064139273468524542176277933151448929420268869808236222401574057174997879599430405407341221428388984827675412726778370913038246699129635727146561394220118530281335561114050725265098398467015701334377461027276449823447125718443322802 18

e = 65537
```

2. lalu untuk mengetahui nilai n maka saya mengalikan nilai p dan q dan didapatkan hasil
   n =
   157160024420901491275151303069558764137050893302421347934387021008089237099810507796321179096121981028783897823233632195586634474912619396653573608824563160857023115897873377741534603027448436268381580865625824923605685676143251077544500774868513248046965603355789718863272350469604253881073075594395008259 31

3. berikutnya dengan menggunakan tool online untuk men-decrypt RSA didapatkan lah hasil sebagai berikut

flag: ARA2023{1t_turn5_0ut_to_b3_an_rsa}

- **babychall**

Welcome to ARACTF! To start the CTF, please translate this flag that I get from display banner! Good Morning

Format : ARA2023{lowercase_flag}

Attachments

Author: circlebytes#5520

Isi daripada sebuah attachment:

c1=5099697310484566310837975113120308543241249019831271466365682364823303847929819286145183424693020814011017369905852791902011543258670540046734564780652233139644765084765013301324667339087922271916924886242027825632296771870170045872920779312475816643864144811231448994586323188198235279076513053500409005367 7
c2=2675086354476975422055414666795504683242305948200761348250028401266882028494792724072473530888031343997988485639367375927974100307107406775103695198800703704181414736281388464205429123159605048186634852771717909704864647112817586024682299987868607933059634279556321476204813521201682662328510086496215821461
c3=3723065824325259074360857110502735786279097298720883321301794117144875381565483990169952665143377132482689535567125594441489394796393497906825731036731593570127080439079912166963515301291640227119072261899750039291173776714331655237649588298693569514697085391427548171740026883264498715798872757513351441919

n1=1054811272672182606121568710177576945501427358240871501067504035798774950592304130461813013558710453571380333433159007322285028757066592448447115384978504130464402705789166459811610008075264270042369184048373634046780294439449506551022524234156319770206258268677288982313827373967288968476180105774204086301 33
n2=9310562105968647481689021549455480283151894842016094170352275912161978585127060863413030745022755798797681816233198228963421503718407586478722368121898260209280675788853358712697409107719024279746131890728075907561257747553462606206096073926982878927413727436397005627613943403931586005255641734069699850927 1
n3=6591850965074227849497136329087484918126836431601265676933912000400702945271942533097529884964063109377036715847176196280943807261986848593000424143320280053279021411394267268255337783494901606319687457351586915314662800434632332988978858085931586830283694881538759008360486661936884202274973387108214754101

Solusi:
Menggunakan script python untuk melakukan perhitungan pada c1, c2, c3, n1, n2, dan n3.

```python
import math
from sympy.functions.elementary.miscellaneous import cbrt
from Crypto.Util.number import long_to_bytes
from sympy.ntheory.modular import crt

def extended_gcd(aa, bb):
    lastremainder, remainder = abs(aa), abs(bb)
    x, lastx, y, lasty = 0, 1, 1, 0
    while remainder:
        lastremainder, (quotient, remainder) = remainder, divmod(
            lastremainder, remainder)
        x, lastx = lastx - quotient*x, x
        y, lasty = lasty - quotient*y, y
    return lastremainder, lastx * (-1 if aa < 0 else 1), lasty * (-1 if bb < 0 els>


def modinv(a, m):
    g, x, y = extended_gcd(a, m)
    if g != 1:
        raise ValueError
    return x % m

c1=509969731048456631083797511312030854324124901983127146636568236482330384792981>
c2=267508635447697542205541466679550468324230594820076134825002840126688202849479>
c3=372306582432525907436085711050273578627909729872088332130179411714487538156548>

n1=105481127267218260612156871017757694550142735824087150106750403579877495059230>
n2=931056210596864748168902154945548028315189484201609417035227591216197858512706>
n3=659185096507422784949713632908748491812683643160126567693391200040007029452719>


e = 3
N = n1 * n2 * n3
pt_cubed = crt([n3,n1,n2],[c3,c1,c2])[0]
pt = cbrt(pt_cubed)
flag = str(long_to_bytes(pt)[::])
#flag = flag[2:-1]
print(flag)
```

- **One Time Password**

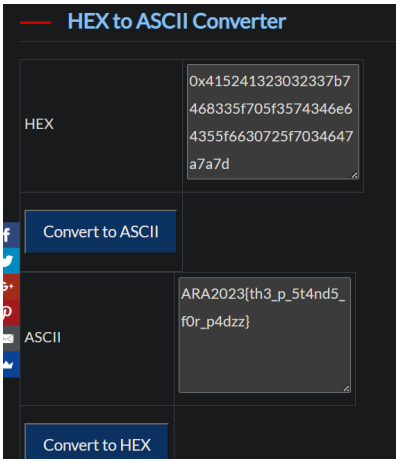
  bwoah, some innovative challenges

  File :
  https://drive.google.com/file/d/1lf1gac5VEmJOGRu9CkkO-CakRcyzEj2K/view?usp=share_link

  Author: circlebytes#5520

  Steps :
  1. Lakukan oprasi XOR kepada kedua variable A dan B
     A ^ B =
     0x415241323032337b7468335f705f3574346e64355f6630725f7034647a7a7d
  2. String diatas memiliki format HEX atau Hexadecimal karena dimulai dengan 0x dan berisi karakter 1-7 A-F lalu kita dapat konfersi string diatas menjadi

format ascii denga site :
https://circuitdigest.com/calculators/hex-to-ascii-calculator



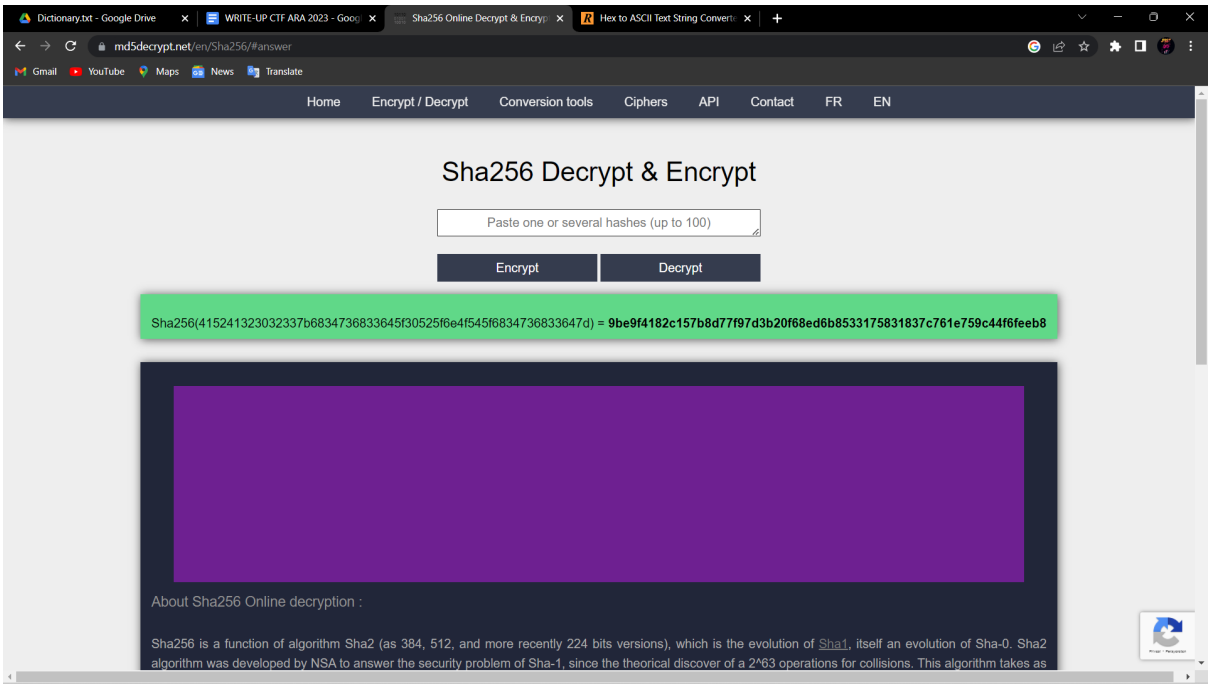
Flag : ARA2023{th3_p_5t4nd5_f0r_p4dzz}

- **SH4-32**

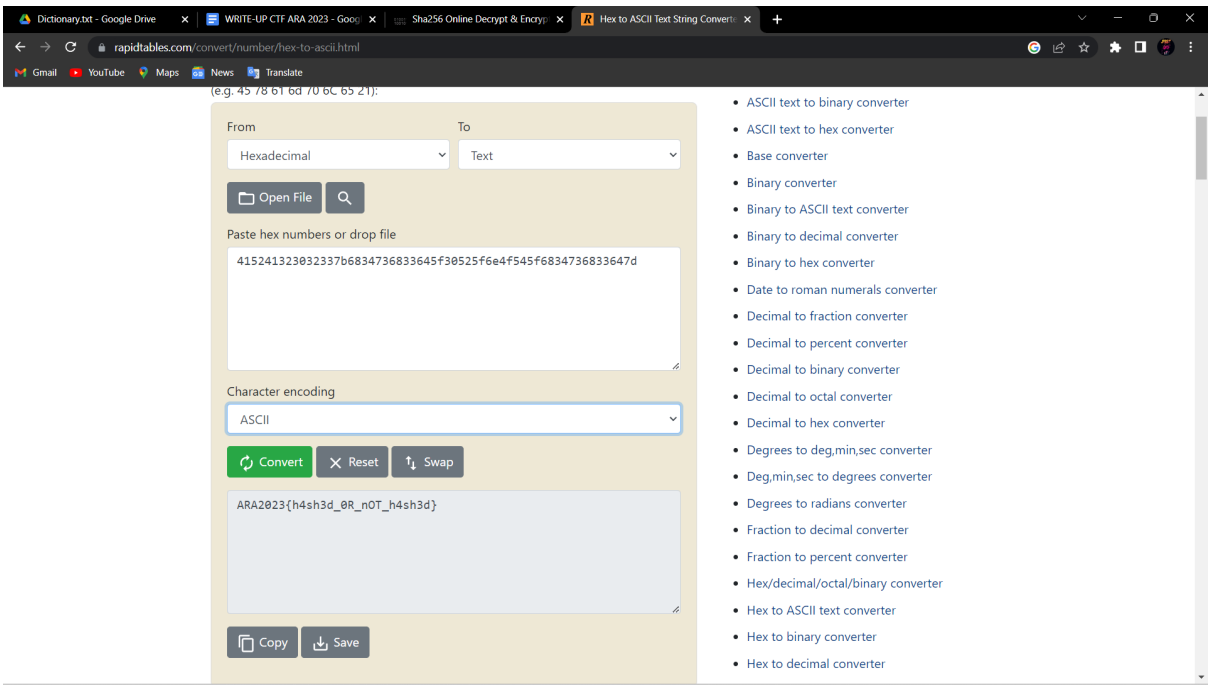
Description:
Sze received an ecnrypted file and a message containing the clue of the file password from her friend.
The clue was a hash value :
9be9f4182c157b8d77f97d3b20f68ed6b8533175831837c761e759c44f6feeb8
Decrypt the file password!
Attachments

Steps:

1. pada file attachment tersebut terdapat banyak sekali strings, saya mencoba melakukan encrypt sha256 pada strings tersebut dan mencocokannya dengan hash value cluenya dan didapatkan lah decrypt dari hash value cluenya



2. didapatkan hasil yang berupa hex 415241323032337b6834736833645f30525f6e4f545f6834736833647d
3. berikutnya saya merubah hex tersebut menjadi ascii atau strings dan didapatkanlah flagnya



flag: ARA2023{h4sh3d_0R_nOT_h4sh3d}

- **L0v32x0r**

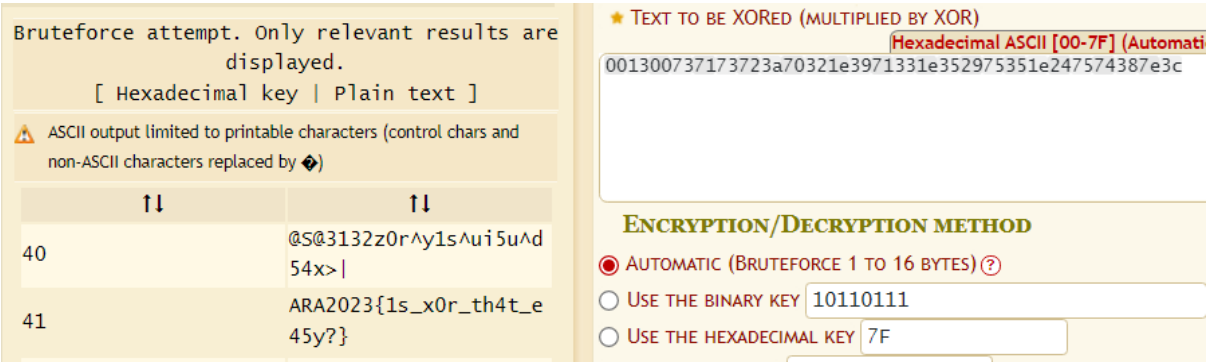
Vonny and Zee were having a treasure hunt game until they realized that one of the clues was a not alike the other clues as it has a random text written on the clue.

The clue was "001300737173723a70321e3971331e352975351e247574387e3c".

Help them to find what the hidden clue means!

Author: L e n s#1048

Solusi: mendecrypt clue yang sudah diberikan dengan xor.
Karena saya belum tahu banget script yang pas untuk chall ini maka saya menggunakan online tools



Flag = ARA2023{1s_x0r_th4t_e45y?}