

WRITE UP ARA-ITS 2023

~ by Heker 1MISSU ~



TEAMS :

IndianaJones

BayzLightyear

UkiyoAgusta

CTF COMPETITION: *EXIST

ASENG:

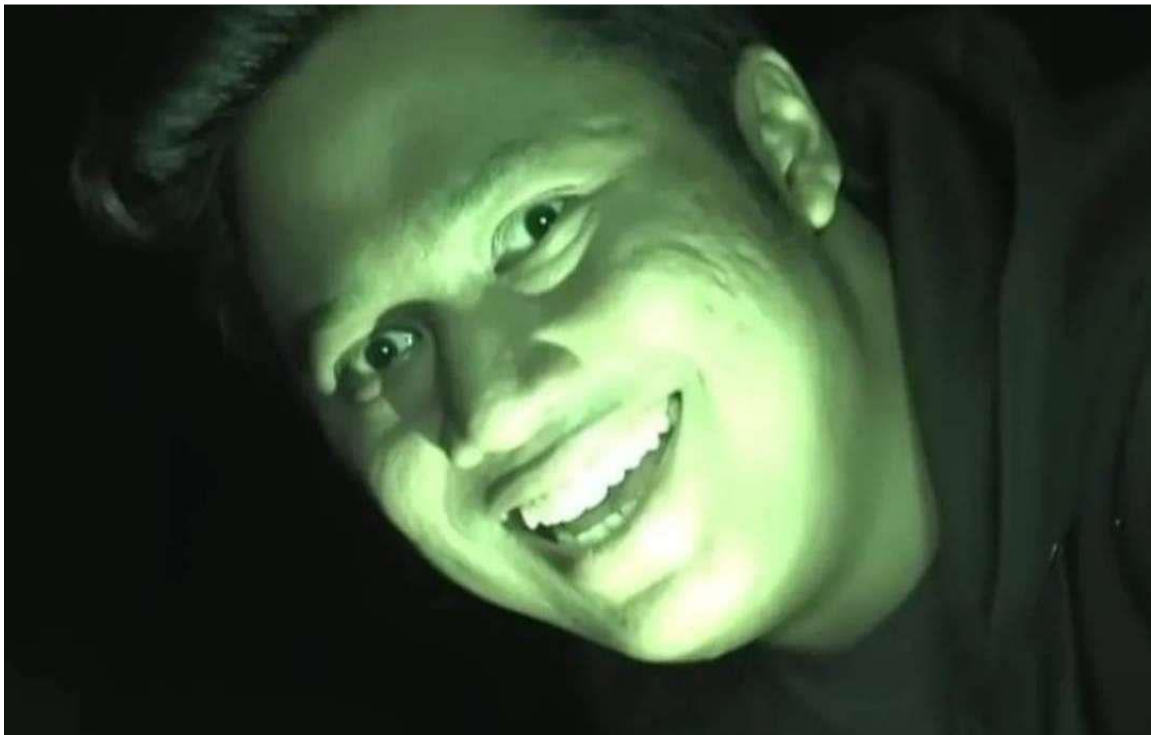


TABLE OF CONTENTS

FORENSIC4

Thinker4

Leakages5

CYRPTOGRAPHY7

One Time Password (?)7

Secrets Behind a Letter7

L0v32x0r8

SH4-329

WEB EXPLOITATION10

Dewaweb10

REVERSE ENGINEERING12

Vidner's Rhapsody12

MISCELLANEOUS13

in-sanity check13

@B4SH15

D0ts N D4sh3s16

Truth17

OSINT18

Time Machine18

Backroom18

Hey detective, can you help me20

FORENSIC

Thinker

Challenge

61 Solves

×

Thinker
100

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

[Attachments](#)

Author: Zangetsu#2398

Flag

Submit

Jadi pada chall ini, diberikan sebuah gambar. Seperti biasa kita cek dengan command file, exiftool, strings, binwalk dll dlu sebagai langkah awal. Setelah di binwalk ternyata di dalam gambar tersebut terdapat banyak file zip. Lalu saya mencoba mengekstrak filenya, didalamnya terdapat file zip lagi, unzip lagi, ada pecahan flag yang di encode ke base64 dan file zip lagi, unzip lagi dan didapat pecahan flag dalam bentuk hex dan lagi lagi ada file zip, unzip lagi dan ada pecahan flag dalam bentuk biner dan file zip lagi, di unzip lagi sampai AKHIRNYA ada file png yang headernya rusak, jadi kami mencoba memperbaiki 16 bytes pertama di headernya dan berhasil. Ternyata gambarnya berisi pecahan flag terakhir dalam bentuk ascii decimal

Flag: ARA2023{5!mpl3_C0rrupt3d_lm4ge5}


```

</nav>
<main class="login-form">
  <div class="container">
    <div class="row justify-content-center">
      <div class="col-md-12">
        <ul class="list-group">
          <li class="list-group-item disabled">Files</li>

          <li class="list-group-item">
            <a href="/download/b8624a72-d1d1-49b0-a50f-b841c7d6280a">lV0cwIGf</a>
          </li>

          <li class="list-group-item">
            <a href="/download/7d7f54c1-1a14-418c-83b1-6c0bace67454">pPPCaJnQ</a>
          </li>

          <li class="list-group-item">
            <a href="/download/8a64aa05-fe92-4b8d-b954-85b87fd9b912">nXZawYYW</a>
          </li>

          <li class="list-group-item">
            <a href="/download/de6fd541-97b6-4eab-b348-e0651bf2aebc">KVYsFEDX</a>
          </li>

          <li class="list-group-item">
            <a href="/download/94453c70-87d3-47c7-a0e1-b699f2cfd46f">Tdfekaav</a>
          </li>

        </ul>
      </div>
    </div>
  </div>

```

nah jadi nama file yang ada di list tersebut ditentukan dari hasil query yang ada pada gambar sebelumnya. Dan nama file ini akan di reflect ke user karena merupakan bagian dari laman html, dari sinilah si attacker mengetahui apakah karakter yang dicari sesuai apa tidak. Jadi Hal selanjutnya yang kita lakukan tinggal memetakan saja karakter yang dicari dengan hasil querynya yang berada pada list file. Disini kami memetakan setiap karakter yang didapat melalui querynya. Karena di dalam querynya terdapat char ke berapa yang coba untuk di retrieve. jadi tinggal disusun berdasarkan query tersebut dan didapatlah flagnya

Flag: ARA2023{r3visitIng_4wkward_sqlite_Injection_4210f9e471}

CYRPTOGRAPHY

One Time Password (?)

Challenge 90 Solves x

One Time Password (?)

100

bwoah, some innovative challenges

File :
https://drive.google.com/file/d/1lflgac5VEmJOGRu9CkkO-CakRcyzEj2K/view?usp=share_link

Author: circlebytes#5520

Flag Submit

Di chall ini diberikan file .txt yang berisi hex yang diidentifikasi dengan A, B, dan XOR. Awalnya kami pikir untuk mendapatkan flag tersebut kami perlu melakukan kalkulasi XOR blablabla, ternyata cukup dengan mengonversi hex yang diidentifikasi dengan XOR dan kemudian akan mendapatkan flag yang dicari-cari.

Flag : ARA2023{th3_p_5t4nd5_f0r_p4dzz}

Secrets Behind a Letter

Challenge 67 Solves x

Secrets Behind a Letter

100

Melon and Edith went to an 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](#)

Author: L e n s#1048

Flag Submit

p:
1257533369412126769052197185569163814413681033118824823677088033890581188

```
3485064104865649834927819725617695554472100341361896162022311653301532810
101344273
q:
1249748342617507246585216793696052623228489187678798108067116278356141152
1675809112204573617358389742732546293502709585129205885726078492417109867
512398747
c:
3606293449573179290863953506283318065102281358953559285180257226432829902
7406413927346852454217627793315144892942026886980823622240157405717499787
9599430405407341221428388984827675412726778370913038246699129635727146561
3942201185302813355611140507252650983984670157013343774610272764498234471
2571844332280218
e = 65537
```

Kalau dilihat-lihat, ini, mah, namanya RSA (Rivest-Shamir-Adleman), Masbro. Bisa pakai rumus dan kode python berikut:

```
import gmpy2
p = 1257533369412126769052197185569163814413681033118824823677088033890581188
3485064104865649834927819725617695554472100341361896162022311653301532810
101344273
q = 1249748342617507246585216793696052623228489187678798108067116278356141152
1675809112204573617358389742732546293502709585129205885726078492417109867
512398747
c = 3606293449573179290863953506283318065102281358953559285180257226432829902
7406413927346852454217627793315144892942026886980823622240157405717499787
9599430405407341221428388984827675412726778370913038246699129635727146561
3942201185302813355611140507252650983984670157013343774610272764498234471
2571844332280218
e = 65537
n = p*q
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
m = pow(c, d, n)
print("Hasile, Masbro: ", m)
```

Setelah dapat hasilnya, tinggal convert dari long to bytes saja, Masbro.

Flag: ARA2023{1t_turn5_Out_to_b3_an_rsa}

L0v32x0r

Challenge

56 Solves

×

L0v32x0r

100

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

Flag

Submit

Jadi karena ini soal xor dan hanya diberi satu data, saya asumsikan chall ini brute xor, jadi karena format flagnya ARA2023, saya coba men xor 3 karakter pertama ke 3 hex value pertama pada data, ternyata kuncinya 0x41, jadi tinggal di xor aja dapet deh flagnya

Flag: ARA2023{1s_x0r_th4t_e45y?}

SH4-32

Challenge

54 Solves

×

SH4-32

100

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](#)

Author: L e n s#1048

Flag

Submit

Mirip dengan chall 'One Time Password (?)', kami berpikir terlalu rumit padahal flagnya terdapat pada Dictionary.txt yang merupakan attachment pada chall ini. Pada Dictionary.txt terdapat satu string yang berbeda dengan string lainnya karena berupa hex. Jadi cukup dengan mengonversi hex string tersebut kami dapat menemukan flag yang dicari-cari.

Flag : ARA2023{h4sh3d_0R_nOT_h4sh3d}

WEB EXPLOITATION

Dewaweb

Challenge

77 Solves

×

Dewaweb

100

Dewaweb sedang mencari talenta terbaik!

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/>

Author: Oxazr#4883

Flag

Submit

Chall ini sebenarnya persis dengan chall saat Warm Up, namun bedanya ini di web dewaweb. Jadi part pertama flag ada pada comment source html.

part-1 : ARA2023{s4nt4I_

part kedua berada pada source js di file custom.js

part-2 : dUlu_

part ketiga berada pada source css di file style.css

part-3 : g4k_

part terakhir berada pada header response http

X-4th-Flag: s1h?XD}

Flag : ARA2023{s4nt4I_dUlu_g4k_s1h?XD}

REVERSE ENGINEERING

Vidner's Rhapsody

Challenge

36 Solves

×

Vidner's Rhapsody

304

Once I was going to send you the program, but do me a favor by retrieving the real output of the program from this generated JSON program tree. Can you?

[Attachments](#)

Author: aseng#2055

Flag

Submit

Di chall ini, terdapat attachment berupa file .json yang berisi hasil parsing dari suatu kode program. Setelah melakukan analisa, kami mencoba menyusun program ulang berdasarkan file .json tersebut. Dan akhirnya tersusun kode program sebagai berikut :

```
function mystenc(berserk, guts) {
    var s = [],
        j = 0,
        x,
        res = "";
    for (var i = 0; i < 256; i++) {
        s[i] = i;
    }
    for (i = 0; i < 256; i++) {
        j = (j + s[i] + berserk.charCodeAt(i % berserk.length)) % 256;
        x = s[i];
        s[i] = s[j];
        s[j] = x;
    }
    i = 0;
    j = 0;
    for (var y = 0; y < guts.length; y++) {
        i = (i + 1) % 256;
        j = (j + s[i]) % 256;
```

```

        x = s[i];
        s[i] = s[j];
        s[j] = x;
        res += String.fromCharCode(guts[y] ^ s[(s[i] + s[j]) % 256]);
    }
    console.log(res);
}

var berserk = "achenk";
var strenk = [244, 56, 117, 247, 61, 16, 3, 64, 107, 57, 131, 13, 137, 113,
214, 238, 178, 199, 4, 115, 235, 139, 201, 22, 164, 132, 175];
mystenc(berserk, strenk);

```

Flag : ARA2023{j4vAST_l!ke_8483l_t0wer_lol}

MISCELLANEOUS

in-sanity check

Challenge
74 Solves

in-sanity check
100

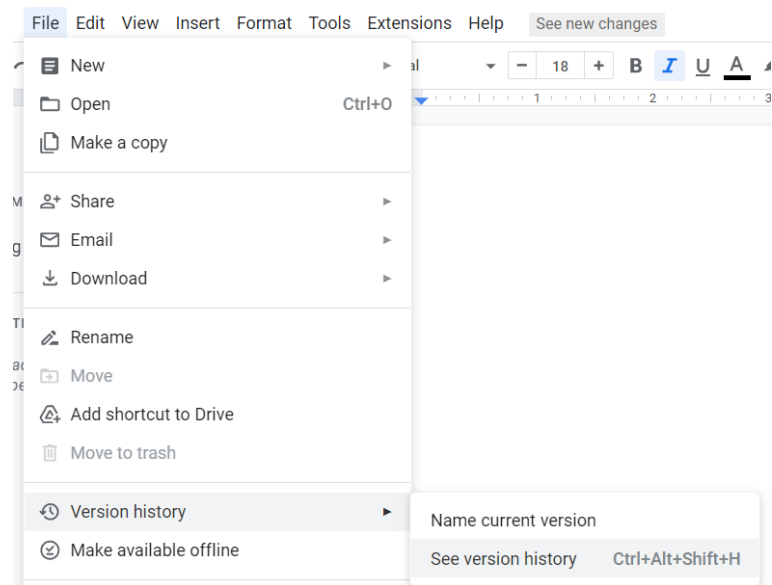
Even the flag for sanity check is gone?

[Attachments](#)

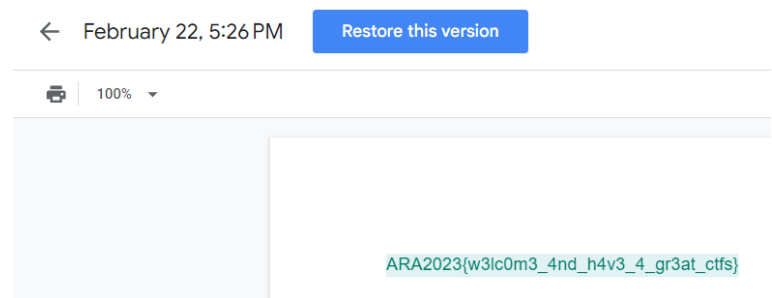
Author: circlebytes#5520

Flag
Submit

Kami dapat file Google Docs yang bisa diakses dan diedit oleh siapa pun, jadi kami berinisiatif mencoba untuk cek history dari file tersebut.



Kami coba untuk mengecek version history paling pertama dan akhirnya menemukan flag yang dicari-cari.



Flag : ARA2023{w3lc0m3_4nd_h4v3_4_gr3at_ctfs}

@B4SH

Challenge

80 Solves

×

@B4SH

100

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.

Author: L e n s#1048

Flag

Submit

Pada deskripsi chall tersebut terdapat hex code yang jika didecode akan menghasilkan string ZIZ2023{4mby0wb_gs0f9sg_gs4g_!g5_4_s4hs?}. Sesuai title dari chall ini yaitu @B4SH atau atbash, jadi kami mencoba untuk melakukan decode dengan menggunakan algoritma atbash.

Flag : ARA2023{4nyb0dy_th0u9ht_th4t_!t5_4_h4sh?}

D0ts N D4sh3s

Challenge

87 Solves

×

D0ts N D4sh3s

100

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-Gl0Uk2lcamH2/view?usp=sharing>

Author: L e n s#1048

Flag

Submit

Diberikan file .txt yang berisi rangkaian sandi morse. Kami mencoba menerjemahkan sandi tersebut menggunakan morse code translator online yaitu <https://morsecode.world/international/translator.html> dan menghasilkan susunan bilangan biner. Susunan bilangan biner tersebut dapat dikonversi dan akan menghasilkan flag yang dicari-cari.

Flag : ARA2023{!ts_ju5t_4_m0rs3_aft312_al!}

Challenge

45 Solves

X

Truth

191

Kuronushi traveled far away from his country to learn something about himself. He never sure about his identity. Untill One day, he met a sage who gave him a book of truth. The sage said " To understand about yourself,Erase the title and find the Bigger case"

Submit the flag on this format ARA2023{} Separate the sentences with _

Attachments

Author: Zangetsu#2398

Flag

Submit

Pada Chall kali ini diberikan file pdf yang memiliki password, dan karena tidak diberi password kami mencoba brute dengan john the ripper menggunakan password list. Pertama kami membuat hash khusus untuk john dengan menggunakan pdf2john lalu disimpan pada file dengan nama hash

[illegible]

setelah itu tinggal di brute hash tersebut dengan john the ripper menggunakan wordlist. Didapat passnya subarukun

```
Proceeding with wordlist:./JohnTheRipper/run/password.lst
Enabling duplicate candidate password suppressor
subarukun          (Truth.pdf)
1q 0:00:00:33 DONE 2/3 (2023-02-26 22:01) 0.03023q/s 53267p/s 53267c/s 53267C/s babyj90..vin
```

Unlock pdfnya, sesuai clue kita cari huruf kapitalnya saja dan buang judulnya. kami mency copy textnya ke file.txt agar mudah dibaca oleh script untuk mengambil huruf besarnya saja, berikut script singkat yang kami gunakan

```
1 #!/usr/bin/env python3
2 ct = open("tes.txt", "r").read()
3 flag = ""
4 for char in ct:
5     if (char.isupper()):
6         flag += char
7 print(flag)
```

Jalankan scriptnya, dan didapat huruf besarnya, pisahkan tiap kata, dan tambah format flag

Flag: ARA2023{SOUNDS_LIKE_FANDAGO}

OSINT

Time Machine

Challenge

82 Solves

×

Time Machine

100

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

Author: 0xazr#4883

Flag

Submit

Pada chall ini kita hanya tinggal mengunjungi website official ara pada tanggal yang sudah ditentukan menggunakan wayback machine lalu view page source untuk mendapatkan flag

```
</div>
</section>
<!-- ARA2023{d1gIt4l_f00tpr1nt_1s_sC4ry} -->
</main>
```

Flag: ARA2023{d1gIt4l_f00tpr1nt_1s_sC4ry}

Backroom

Challenge

73 Solves

×

Backroom

100

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?

[Attachment](#)

Author: 0xazr#4883

Flag

Submit

Kami menggunakan exiftool terhadap gambar tersebut, lalu menemukan sebuah koordinat -7.252769, 112.750573. Langsung saja mencari di maps dan mendapati bahwa tempat tersebut adalah Hi-Tech Mall Surabaya. Lalu menemukan review ini



Azril
1 ulasan

★★★★★ sebulan lalu

Very nice place, especially the last floor, its so quiet.

ARA2023{c4r3full_w1th_y0uR_m3tad4ta}

(Diterjemahkan oleh Google)

Tempat yang sangat bagus, terutama lantai terakhir,
sangat sepi.

ARA2023{c4r3full_w1th_y0uR_m3tad4ta}

Flag: ARA2023{c4r3full_w1th_y0uR_m3tad4ta}

Hey detective, can you help me

Challenge

35 Solves

×

Hey detective, can you help me

316

Ada seorang cosplayer dari China yang sangat aktif bersosial media, dia kadang memposting foto cosplaynya di facebook dan instagram. Dia pernah berkuliah di universitas ternama di China, suatu saat dia dan temannya berkunjung pada toko boneka untuk membeli sebuah boneka, tidak lupa dia juga berfoto dengan sebuah maskot di sana. Lalu selanjutnya dia mampir ke sebuah toko buku untuk membeli buku, sebagai seseorang yang update sosial media dia juga mengambil sebuah foto di toko buku tersebut dengan pose terduduk. Ohh iya dia juga pernah berfoto bareng atau collab dengan cosplayer asal China dengan nama 'Sakura'.

[Attachment](#)

Author: Abdierry#9836

⬇️ Instruction...

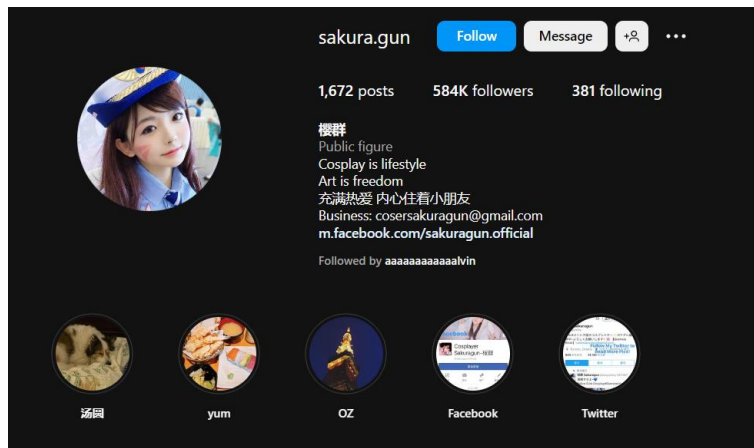
Flag

Submit

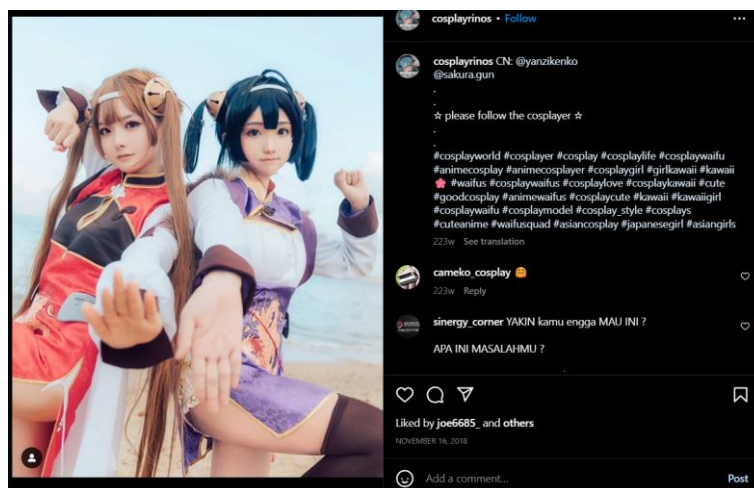
Pertama, diberikan sebuah video yang awalnya kami kira ini adalah video Sakura karena dia adalah klu satu-satunya yang kami miliki.



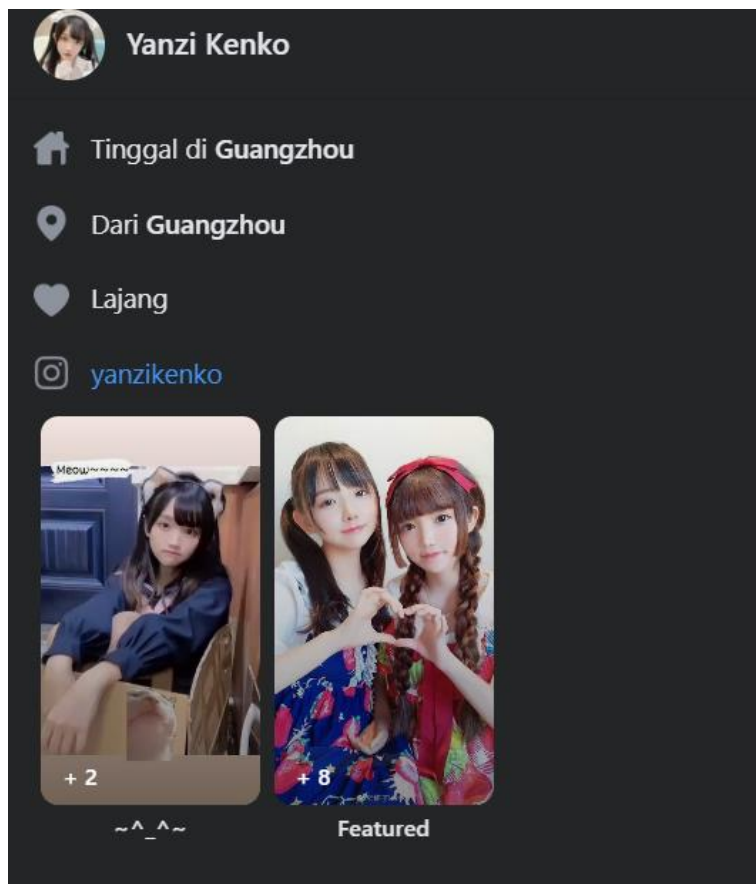
Lalu, kami mencoba mencari akun instagram seorang cosplayer asal Negeri Tirai Bambu yang bernama Sakura ini. Ujungnya, kami menemukan pengguna akun instagram @sakura.gun karena kemiripannya dengan gadis yang terdapat di video tersebut.



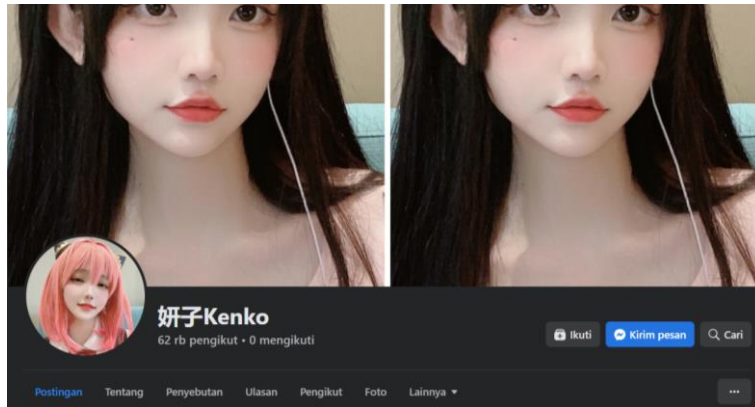
Kami pencari beberapa postingan yang mungkin bisa menjadi identitas si cosplayer yang dikatakan. Sampai akhirnya kami menemukan postingan ini di bagian tag.



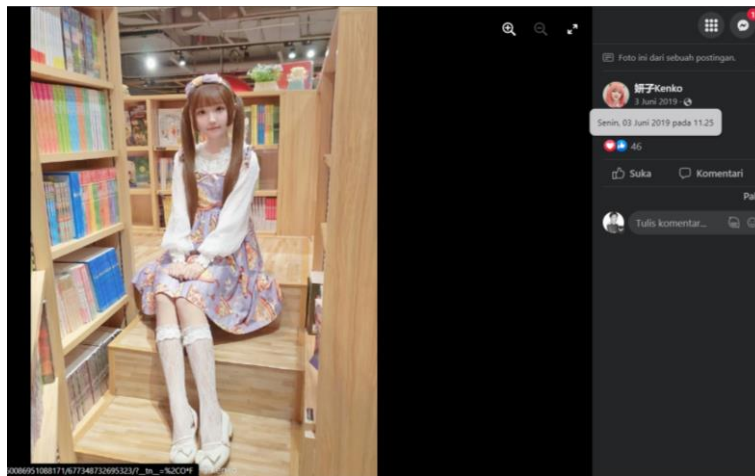
Anggota kami menganggap orang tersebut adalah pengguna dengan akun @yanzikenko karena memiliki kemiripan dengan @sakura.gun dan gadis di video. Lalu kami “menyelam” sedalam mungkin di beberapa sosial media miliknya. Sampai kami menemukan sebuah klu yang menarik pada akun yang satu ini.



Yap ..., benar sekali, video yang sama. Pernah belajar di Beijing Normal University (BNU), begitulah yang terisi di profilnya. Dan juga, lihat, akun facebook itu langsung terhubung dengan instagramnya. Tapi, akun tersebut hanya memiliki sedikit foto, jadi kami mencari lagi berbagai akun lain miliknya di facebook. Hingga akhirnya kami menemukan akun dengan lebih banyak foto.



Dan tebak, kami menemukan apa? Lebih banyak informasi.



Karena ARA CTF berlokasi di ITS, jadi kamu gunakan GMT+7, yaitun 10:25.



Yo Lalu kami menggeser lebih ke atas lagi



Kami menemukan bahwa maskot tersebut bernama Molly. Lalu, kami mencari ID akunnya, awalnya kami menggunakan ID facebook, tapi sepertinya lebih relevan menggunakan ID instagram dengan menggunakan <https://followersgratis.web.id/cek-user-id-instagram/>. Dan didapat id @yanzikenko adalah 44793134117. Akhirnya flag sudah terkumpul.

Flag: ARA2023{44793134117_BNU_Molly_3Juni2019-10:25_Y0u4r3ThE0s1nTm45t3R}