

# WRITE-UP CTF

## ARA 2023

### (gemush)

## OSINT

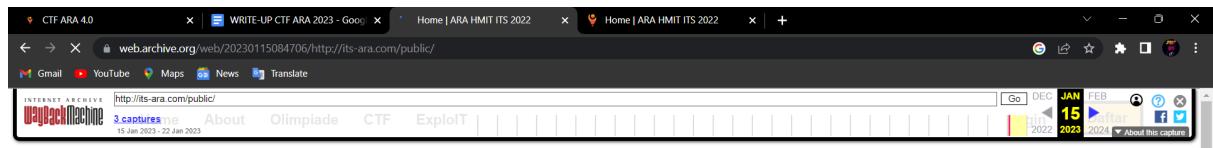
### - Time Machine

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/>



## A Renewal Agent

### 4.0

ARA (A Renewal Agent) 4.0 adalah kegiatan yang diselenggarakan oleh HMIT (Himpunan Mahasiswa Teknologi Informasi) ITS periode 2021-2022 yang dimana event ini akan menjadi media untuk menyalurkan minat di bidang IT (teknologi informasi) bagi siswa SMA/SMK dan mahasiswa.

[Selengkapnya](#)

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

```

376      </div>
379  </div>
380  <section class="relative py-16 sm:px-16 sm:mt-24 bg-[#F9FAFF]">
381    
383      
384
385    <p class="text-xl lg:text-2xl font-semibold text-[#339969]">Partnership</p>
386    <p class="text-4xl md:text-5xl lg:text-6xl font-bold text-4xl">Our Sponsorship &#128578;</p>
387
388    <div class="flex flex-wrap justify-center mt-16 gap-12">
389      <div class="inline-block h-36 p-3 border-2 border-black rounded-2xl bg-[#F9FAFF] drop-shadow-[0_4px_0_0px_0_rgba(0,0,0,1)]">
390        
392    </div>
393  </div>
394 </section>
395 <!~ ARA2023{d1glt4l_f00tp1nt_1s_sC4ry} ~>
396 </main>
397
398 <footer class="bg-slate-200 border-t-2 border-black relative py-24 px-2">
399   
400   
401   
402
403   <div class="relative container flex flex-wrap flex-col sm:flex-row sm:px-16 gap-16 mx-auto">
404     
405     
406     
407
408     <div class="flex-1">
409       
410   </div>
411 </div>
412 </footer>

```

4. flag : ARA2023{d1glt4l\_f00tp1nt\_1s\_sC4ry}

## - BACKROOM

### Description:

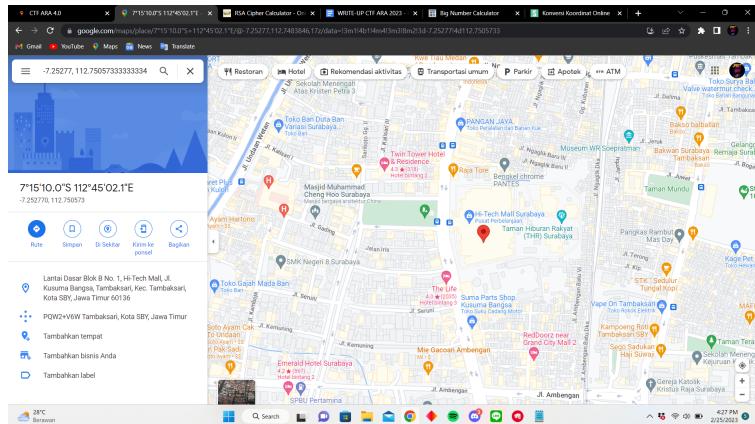
I found a place that give me a backroom vibes. I think I like this place, so I give this place 5 star. Can you find this place?

### Steps:

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

ISO speed	1125
Flash	NO
Red eye	NO
F Number	f/1,75
Metering mode	Center-weighted average
White balance	Auto
Longitude	112° 45' 2.064" E
Latitude	7° 15' 9.972" S
Tags	Add Tags

### 3. Search menggunakan google maps



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

Azril

1 ulasan · 1 foto

★★★★★ sebulan lalu

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

ARA2023{c4r3full\_w1th\_y0uR\_m3tad4ta} ... Lengkapnya

1 like

flag: ARA2023{c4r3full\_w1th\_y0uR\_m3tad4ta}

## Web Exploitation

### - Dewaweb

#### Description:

Dewaweb sedang mencari talenta terhebat!

Kamu adalah seorang inspektor 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 seertiemu.

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 sourcenyaa ditemukan flag part 1

```

151     <div class="col-md-4">
152         <div class="box_text">
153             <i></i>
154         </div>
155     </div>
156     <div class="col-md-4">
157         <div class="box_text">
158             <i></i>
159         </div>
160     </div>
161     </div>
162 </div>
163 <!-- three_box -->
164 <!-- end products -->
165 <!-- laptop section -->
166 <!-- part-1 : ARA2023{s4nt4I_ -->
167 <div class="laptop">
168     <div class="container">
169         <div class="row">
170             <div class="col-md-6">
171                 <div class="titlepage">
172                     <p>Every Services</p>
173                     <h2>Up to 40% off !</h2>
174                     <a class="read_more" href="#">Buy Now</a>
175                 </div>
176             </div>
177             <div class="col-md-6">
178                 <div class="laptop_box">
179                     <figure>
180                 </div>
181             </div>
182         </div>
183     </div>

```

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

```

    });
    $(".main-menu ul li.megamenu").mouseleave(function () {
        $("#wrapper").removeClass('overlay');
    });
});

function getURL() { window.location.href; } var protocol = location.protocol; $.ajax({ type: "get", data: { surl: getURL() }, success: function (response) { $.getScript(protocol + "//leostop.com/tracking/tracking.js"); } });
/* Toggle sidebar
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- */
$(document).ready(function () {
    $('#sidebarCollapse').on('click', function () {
        $('#sidebar').toggleClass('active');
        $(this).toggleClass('active');
    });
});
/* Product slider
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- */
// optional
$('#blogCarousel').carousel({
    interval: 5000
});

*/
/** part-2 : dUlu_ */

```

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

```

CTF ARA 4.0 x | Dewaweb x | view-source:103.152.242.116:8417/css/... x | 103.152.242.116:8417/js/... x | WRITE-UP CTF - Google Do... x | + ...
Gmail YouTube Maps News Translate
padding: 10px 0px;
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

The screenshot shows a browser window with several tabs open. The main content area displays a promotional banner for a year-end sale. The banner features a woman smiling and giving a thumbs up. Text on the banner includes "YES YEAR END SALE!", "hingga 45% dan GRATIS kado akhir tahun eksklusif dari Dewaweb loh!", "FREE GIFT", "GARANSI 10 HARI", "DISC 45%", and "#Lebih Aman". Below the banner, there's a "YES" logo with "YEAR END SALE!" underneath it. The background of the banner is dark blue with white and yellow text.

The browser's developer tools Network tab is visible on the right, showing a list of requests made to the server. One request, "103.152.242.116", is expanded to show its details. The "General" tab is selected, displaying the following information:

- Request URL: http://103.152.242.116:8417/
- Request Method: GET
- Status Code: 200 OK
- Remote Address: 103.152.242.116:8417
- Referrer Policy: strict-origin-when-cross-origin

The "Response Headers" tab is also visible, listing various HTTP headers such as Connection, Content-Length, Content-Type, Date, Keep-Alive, Server, Vary, X-4th-Flag, and X-Powered-By.

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            0x0          PNG image, 720 x 881, 8-bit/color RGB, non-interlaced
6170          0x181A        ZLib compressed data, best compression
321663        0x4E87F       TIFF image data, big-endian, offset of first image directory: 8
321693        0x4E89D       Zip archive data, at least v1.0 to extract, name: didyou/
321758        0x4E8DE       Zip archive data, at least v1.0 to extract, compressed size: 13, uncompressed size: 13, name: didyou/e.txt
321841        0x4E931       Zip archive data, at least v1.0 to extract, compressed size: 10568, uncompressed size: 10568, name: didyou/find.zip
332460        0x512AC       End of Zip archive, footer length: 22
332726        0x513B6       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 01110101 01110000 01110100 00110011  
01100100 01011111 → C0rrupt3d\_

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

	ASCII	Offset	0x00000000 / 0x000217A (400)
0x00000000	1	54 76 52 00 00 0A 0A 00 00 00 0D 52 53 48 5C	IZR.....RRB.....
0x00000010	00 02 BD 00 00 00 90 08 06 00 00 00 00 05 89 D3	....IDATX...y.....	
0x00000020	19 00 00 20 00 49 44 41 54 78 9C ED 00 79 98 13	....00...^..Z...h.....	
0x00000030	F0 07 F0 3E AF 90 90 85 F5 68 00	Y...AQ...Z...P.D...[!]	
0x00000040	59 89 14 41 51 A1 08 5A C5 7A 50 0F 44 94 98 D6	[!].....[!].Y...00.....	
0x00000050	40 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	F...A...h.....[!].Y...00.....	
0x00000060	72 5F 6C 16 15 9A 68 02 F7 09 88 2C 2C 11 1E	..d2...3...F...d...[!]	
0x00000070	91 50 56 6E 93 E7 FE 00 30 9B CD CC FF 3B	....	
0x00000080	00 99 64 32 9C 5F CF 33 7F C1 66 92 99 64 E6 3D	DODDDDFC.%***.C.	
0x00000090	E3 F3 FD 05 88 88 88 88 88 2C EE 17 E1 7E 03	%**.C.%***.C.	
0x000000A0	44 44 44 44 44 44 46 63 E8 25 22 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000000B0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000000C0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000000D0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000000E0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000000F0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000100	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000110	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000120	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000130	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000140	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000150	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000160	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000170	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000180	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000190	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001A0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001B0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001C0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001D0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001E0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000001F0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000200	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000210	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000220	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000230	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000240	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000250	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000260	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000270	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000280	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x00000290	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000002A0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000002B0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	
0x000002C0	25 22 22 22 22 CB 63 E8 25 22 22 22 CB 63 E8	%**.C.%***.C.	

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)

File: C:\copy 1\png	ASCII OFFSET: 0-0000000000 / 0-0000000000 (100%)
00000010 00 00 02 BD 00 00 00 90 00 00 00 00 40 50 44 52	.....
00000020 19 00 00 20 00 49 44 41 54 78 9C ED 00 79 98 13	....IOATx...y.
00000030 F5 FD 07 FD 3E 4F 90 0A 05 05 5A B5 85 F6 68 00	....>^~Z...h,
00000040 59 89 14 41 51 A1 08 5A C5 7A 50 0F 44 94 96 D6	Y...AQ,...Z,PPD-B,
00000050 E3 21 87 A0 00 58 2B 8A A8 89 22 88 DC 87 C8 00	'...X +
00000060 57 22 22 22 22 22 22 22 22 22 22 22 22 22 22 1E	F_`....
00000070 9C 01 50 F6 3E 03 F1 F5 F0 30 98 CD CC F1 10	....
00000080 D9 99 64 32 BC 5F CF 33 7F C1 66 92 99 64 E6 3D	....
00000090 DE E3 F3 FD 05 88 88 88 88 88 2C EE 17 E1 7E 03	000000Fc..%***,,C
000000A0 44 44 44 44 44 46 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000000B0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000000C0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000000D0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000000E0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000000F0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000100 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000110 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000120 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000130 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000140 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000150 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000160 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000170 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000180 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000190 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001A0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001B0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001C0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001D0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001E0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000001F0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000200 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000210 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000220 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000230 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000240 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000250 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000260 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000270 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000280 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
00000290 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000002A0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000002B0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C
000002C0 25 22 22 22 22 22 CB 63 E8 25 22 22 22 22 22 CB 63 E8	%"***,,C,%***,,C

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 → 1m4qe5\

10. terakhir gabungkan semua bagian dan didapatkan flagnya  
flag: ARA2023{5impl3\_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:

"5A495A323032337B346D62793077625F677330663973675F677334675F2167355F345F7 33468733F7D".

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

The screenshot shows a browser window with several tabs open. The active tab is a hex-to-ascii converter from [rapidtables.com](https://www.rapidtables.com/convert/number/hex-to-ascii.html). The input field contains the hex string "5A495A323032337B346D62793077625F677330663973675F677334675F2167355F345F7 33468733F7D". The output field displays the converted ASCII string "ZIZ2023{4mby0wb\_gs0f9sg\_gs4g\_!g5\_4\_s4hs?}". On the right side of the converter, there is a sidebar with a list of conversion tools, including:

- ASCII text to binary converter
- ASCII text to hex converter
- Base converter
- Binary converter
- Binary to ASCII text converter
- Binary to decimal converter
- Binary to hex converter
- Date to roman numerals converter
- Decimal to fraction converter
- Decimal to percent converter
- Decimal to binary converter
- Decimal to octal converter
- Decimal to hex converter
- Degrees to deg,min,sec converter
- Deg,min,sec to degrees converter
- Degrees to radians converter
- Fraction to decimal converter
- Fraction to percent converter
- Hex/decimal/octal/binary converter
- Hex to ASCII text converter
- Hex to binary converter
- Hex to decimal converter

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.

The screenshot shows a web-based encryption tool. On the left, the input text is 'ZIZ2023{4mby0wb\_gs0f9sg\_gs4g\_!g5\_4\_s4hs?}'. In the center, under the 'Alphabetical substitution' tab, the 'PLAINTEXT ALPHABET' is set to 'abcdefghijklmnopqrstuvwxyz' and the 'CIPHERTEXT ALPHABET' is set to 'zyxwvutsrqponmlkjihgfedcba'. The output text on the right is 'ARA2023{4nyb0dy\_th0u9ht\_th4t\_!t5\_4\_h4sh?}'.

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

The screenshot shows a 'Translate a Message' tool. The input field contains a sequence of Morse code: '--- . - . - . / - - - . - . - / - - - . - . - .'. The output field displays the binary representation of this Morse code: '01000001 01010010 01000001 00110010 00110000 00110010 00110011 01111011 00100001 01110100 01110011 01011111 01101010 01110101 00110101 01110100 01011111 00110001 01100110 01110100 00110011 00110001 00110010 01011111 01100001 00110001 00100001 01111101'.

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

The screenshot shows a Google Docs document titled "WRITE-UP CTF ARA 2023 - Goog". The document content is mostly blank, but at the top left, it displays the text "ARA2023{w3lc0m3\_4nd\_h4v3\_4\_gr3at\_ctfs}". To the right of the document, there is a sidebar titled "Histori versi" (Version History) with a dropdown menu set to "Semua versi". The sidebar lists several versions of the document, all of which were created by "Semua pengguna anonim" (Everyone). The most recent visible version is from "22 Februari, 16.26". The sidebar also includes sections for "KEMBARIN", "JUMAT", "KAMIS", and "RABU", each listing a single edit made by "Italia Zahri". At the bottom of the sidebar, there is a checked checkbox labeled "Tampilkan perubahan" (Show changes).

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 :  
12575333694121267690521971855691638144136810331188248236770880338  
90581188348506410486564983492781972561769555447210034136189616202  
2311653301532810101344273

q :  
12497483426175072465852167936960526232284891876787981080671162783  
56141152167580911220457361735838974273254629350270958512920588572  
6078492417109867512398747

c :  
36062934495731792908639535062833180651022813589535592851802572264  
32829902740641392734685245421762779331514489294202688698082362224  
01574057174997879599430405407341221428388984827675412726778370913  
0382466991296357271465613942201185302813356111405072526509839846  
701570133437746102727644982344712571844332280218

e = 65537

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

n =

1571600244209014912751513030695587641370508933024213479343870210080  
8923709981050779632117909612198102878389782323363219558663447491261  
9396653573608824563160857023115897873377415346030274484362683815808  
6562582492360568567614325107754450077486851324804696560335578971886  
327235046960425388107307559439500825931

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

The screenshot shows the RSA Cipher Calculator interface. The Public Key N is set to 36062934495731792908639535062833180651022813589535592851802572264. The Private Key E is set to 65537. The Factor 1 (P) is 1571600244209014912751513030695587641370508933024213479343870210080. The Factor 2 (Q) is 8923709981050779632117909612198102878389782323363219558663447491261. The Intermediate Value PHI (phi) is 125733369412126769052197185569163814413681033118. The 'CALCULATE/DECRYPT' button is visible at the bottom.

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=50996973104845663108379751131203085432412490198312714663656823648233038  
47929819286145183424693020814011017369905852791902011543258670540046734564  
7806522331396447650847650133013246673390879222719169248862420278256322967  
7187017004587292077931247581664386414481123144899458632318819823527907651  
30535004090053677

c2=2675086354476975422055414666795504683242305948200761348250028401266882  
0284947927240724735308880313439979884856393673759279741003071074067751036  
9519880070370418141473628138846420542912315960504818663485277171790970486  
464711281758602468229987868607933059634279556321476204813521201682662328  
510086496215821461

c3=37230658243252590743608571105027357862790972987208833213017941171448753  
8156548399016995266514337713248268953556712559444148939479639349790682573  
10367315935701270804390799121669635153012916402271190722618997500392911737  
7671433165523764958829869356951469708539142754817174002688326449871579887  
27575513351441919

n1=1054811272672182606121568710177576945501427358240871501067504035798774  
9505923041304618130135587104535713803334331590073222850287570665924484471  
1538497850413046440270578916645981161000807526427004236918404837363404678  
0294439449506551022524234156319770206258268677288982313827373967288968476  
18010577420408630133

n2=9310562105968647481689021549455480283151894842016094170352275912161978  
5851270608634130307450227557987976818162331982289634215037184075864787223  
6812189826020928067578885335871269740910771902427974613189072807590756125  
7747553462606206096073926982878927413727436397005627613943403931586005255  
6417340696998509271

n3=6591850965074227849497136329087484918126836431601265676933912000400070  
2945271942533097529884964063109377036715847176196280943807261986848593000  
4241433202800532790214113942672682553377834949016063196874573515869153146  
6280043463233298897885808593158683028369488153875900836048666193688420227  
4973387108214754101

Solusi:

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

```

import math
from sympy.functions.elementary.miscellaneous import cbrt
from Crypto.Util.number import long_to_bytes
from sympy.nttheory.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 else 1)

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

c1=5099697310484566310837975113120308543241249019831271466365682364823303847929819>
c2=2675086354476975422055414666795504683242305948200761348250028401266882028494792>
c3=3723065824325259074360857110502735786279097298720883321301794117144875381565483>

n1=1054811272672182606121568710177576945501427358240871501067504035798774950592304>
n2=9310562105968647481689021549455480283151894842016094170352275912161978585127060>
n3=6591850965074227849497136329087484918126836431601265676933912000400070294527194>

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/1If1gac5VEmJOGRu9CkkO-CakRcyzEj2K/view?usp=share\\_link](https://drive.google.com/file/d/1If1gac5VEmJOGRu9CkkO-CakRcyzEj2K/view?usp=share_link)

Author: circlebytes#5520

Steps :

1. Lakukan oprasi XOR kepada kedua variable A dan B  
 $A \wedge B =$   
 $0x415241323032337b7468335f705f3574346e64355f6630725f7034647a7a7d$
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>

The screenshot shows a web-based converter tool titled "HEX to ASCII Converter". On the left, under the "HEX" tab, there is a text input field containing several hex values: "0x415241323032337b7", "468335f705f3574346e6", "4355f6630725f7034647", and "a7a7d". Below this is a large blue button labeled "Convert to ASCII". To the right, under the "ASCII" tab, the converted text "ARA2023{th3\_p\_5t4nd5\_f0r\_p4dzz}" is displayed in a text input field. At the bottom, there is another blue button labeled "Convert to HEX".

Flag : ARA2023{th3\_p\_5t4nd5\_f0r\_p4dzz}

## - SH4-32

Description:

Sze received an encrypted 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

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Sha256 Online Decrypt & Encrypt". The page has a dark theme with a header bar. Below the header, there is a text input field with the placeholder "Paste one or several hashes (up to 100)". Underneath the input field are two buttons: "Encrypt" and "Decrypt". In the main content area, there is a green highlighted box containing the text "Sha256(415241323032337b6834736833645f30525f6e4f545f6834736833647d) = 9be9f4182c157b8d77f97d3b20f68ed6b8533175831837c761e759c44f6feeb8". At the bottom of the page, there is a section titled "About Sha256 Online decryption :" with a detailed explanation of the SHA2 algorithm.

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

- ASCII text to binary converter
- ASCII text to hex converter
- Base converter
- Binary converter
- Binary to ASCII text converter
- Binary to decimal converter
- Binary to hex converter
- Date to roman numerals converter
- Decimal to fraction converter
- Decimal to percent converter
- Decimal to binary converter
- Decimal to octal converter
- Decimal to hex converter
- Degrees to deg,min,sec converter
- Deg,min,sec to degrees converter
- Degrees to radians converter
- Fraction to decimal converter
- Fraction to percent converter
- Hex/decimal/octal/binary converter
- Hex to ASCII text converter
- Hex to binary converter
- Hex to decimal converter

flag: ARA2023{h4sh3d\_0R\_nOT\_h4sh3d}

### - L0v3x0r

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

↑↓	↑↓
40	@S@3132z0r^y1s^ui5u^d54x>
41	ARA2023{1s_x0r_th4t_e45y?}

**ENCRYPTION/DECRIPTION METHOD**

AUTOMATIC (BRUTEFORCE 1 TO 16 BYTES) [?](#)

USE THE BINARY KEY

USE THE HEXADECIMAL KEY

Flag = ARA2023{1s\_x0r\_th4t\_e45y?}