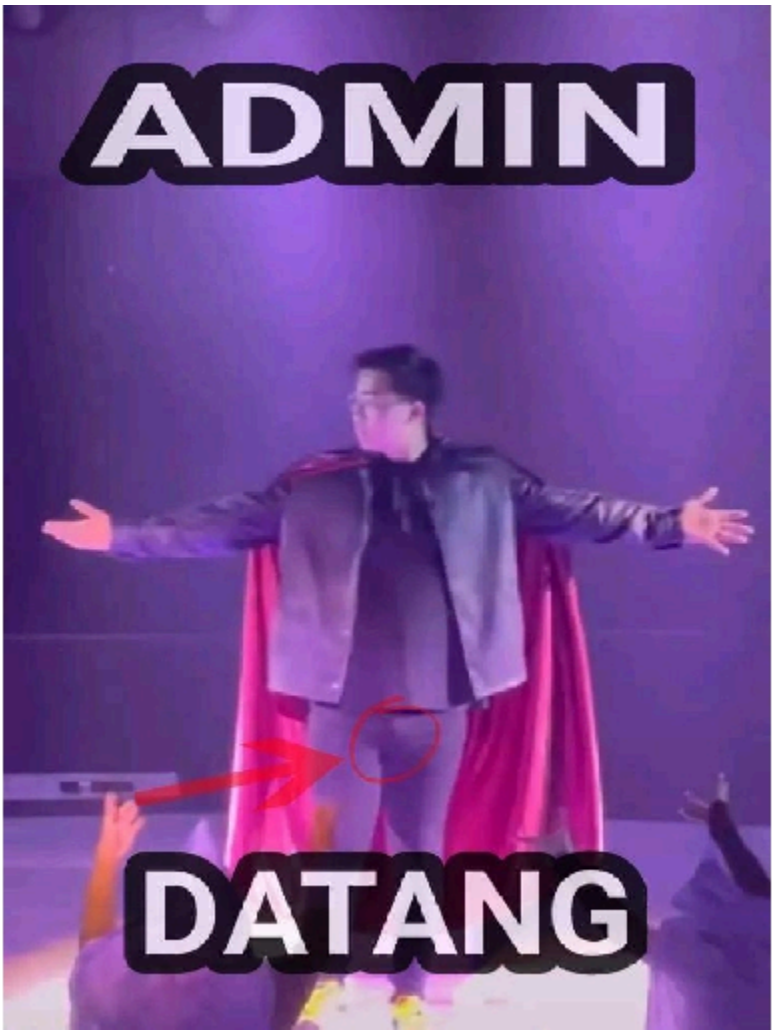
Write-Up COSMOS 2024



By Imagine Losing😎

Muhammad Abi Abdillah (245150701111027) - zenCipher
Muhammad Dhika Ferdiansyah (245150700111046) - Ghoti_Kisruf
Ahmad Muflih Azhari (245150701111030) - arigatogojaimas

DAFTAR ISI

[web]

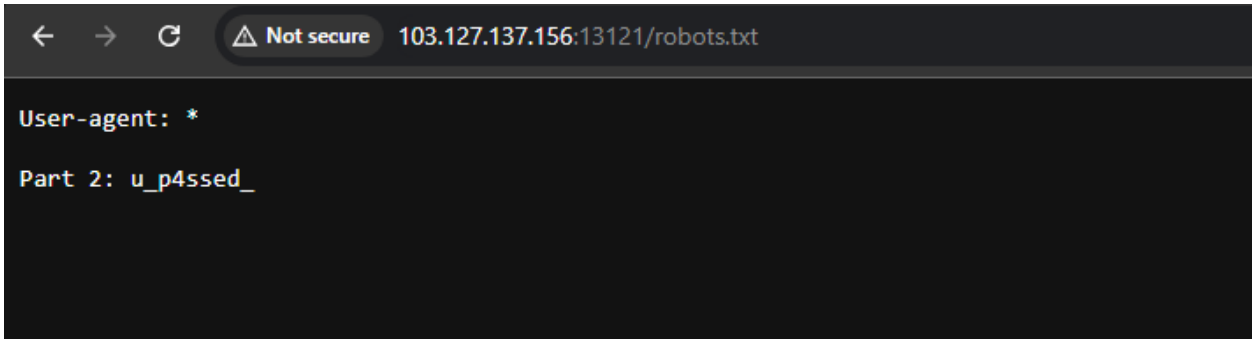
1. Sanity check

Sanity check
Author : anakmamah

Sebuah ***Robot*** telah membagi flag menjadi beberapa bagian, bisakah anda menolong saya untuk mengumpulkan semua bagian flag?

http://103.127.137.156:13121

Pada challenge ini, kami masuk ke sebuah website yang diberikan. Pada description challenge, kata "Robot" seperti ditegaskan. Maka, kami langsung mencoba masuk ke **/robots.txt**.



Ternyata flag yang akan dicari terpisah-pisah menjadi beberapa bagian. Pada page **robots.txt** terdapat potongan kedua. Selanjutnya kami coba mengeksplor *source code* yang ada pada web. Kita mulai dari **style.css**. Di line paling bawah kita mendapatkan potongan pertamanya.

Kemudian, kami cek script bernama **app.js**. Pada script ini, terdapat function pada suatu tombol untuk membuka file bernama **secret.html**. Ketika dibuka, kami mendapat potongan terakhir flag.

Congratulation, you find all the flag's parts

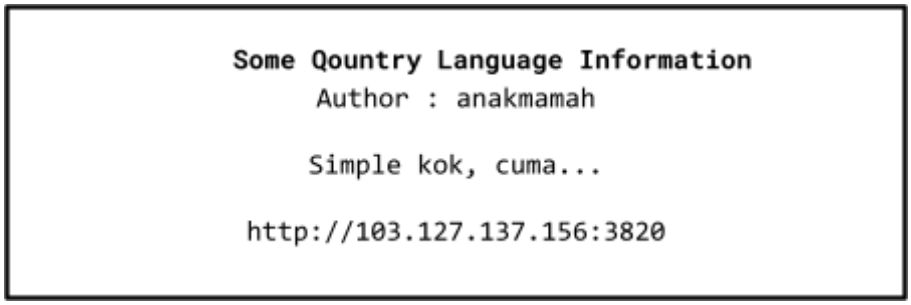
here's your last part: _ch3ck}

Dont forget to combine all the parts 👍

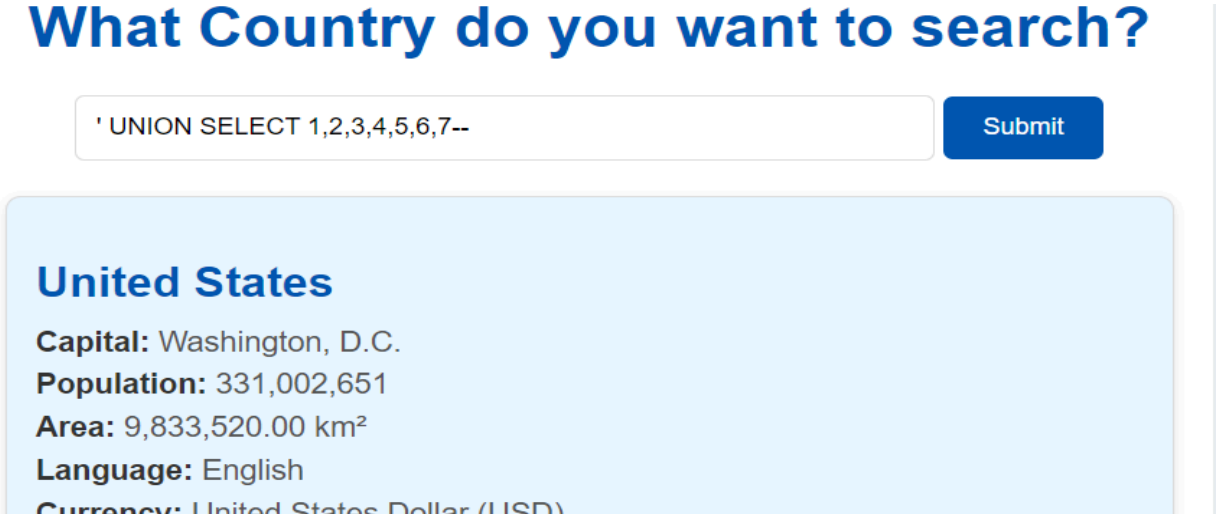
Tapi, terdapat satu file javascript lagi pada *source code*, yaitu **part3.js**. Sepertinya kode yang ada di script tersebut adalah brainfuck js. Langsung saja kita gunakan online tools. Setelah script aneh itu dimasukkan, maka kita mendapatkan part ketiga dari flag.

Flag: COSMOS24{c0ngr4ts_u_p4ssed_th3_s4n1ty_ch3ck}

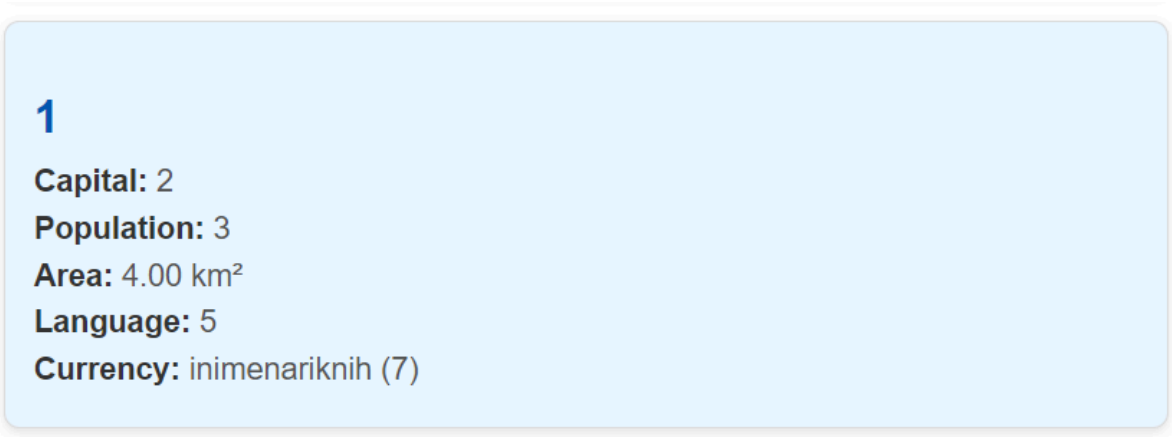
2. Some Qountry Language Information



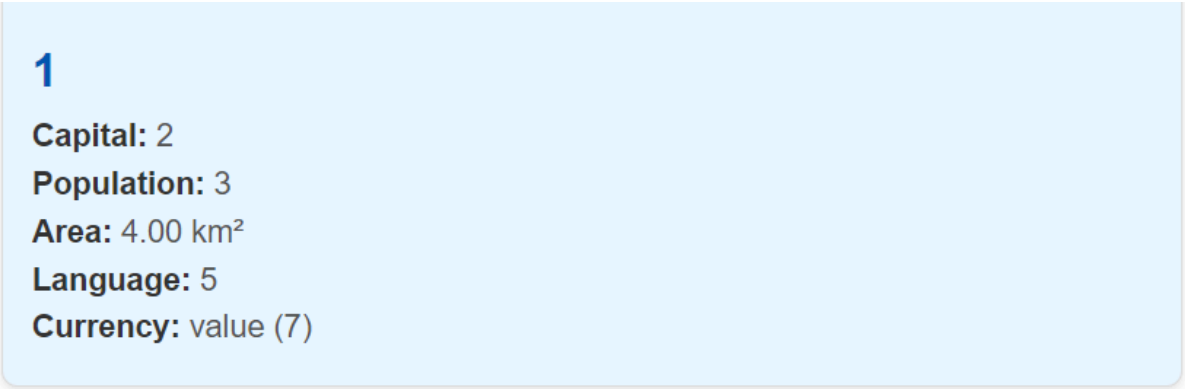
Pada challenge ini, website meminta kita untuk menginput sebuah strings dan berdasarkan judul dari challenge kami berpikir bahwa challenge ini berupa SQL Injection challenge. Dengan melakukan test dengan injection payload “' UNION SELECT 1,2,3,4,5,6,7-- ”



Dengan ini kita dapat melakukan injection dengan tanpa filter. Kita dapat check nama table pada database website dengan injection ' UNION SELECT 1, 2, 3, 4, 5, table_name, 7 FROM information_schema.tables --

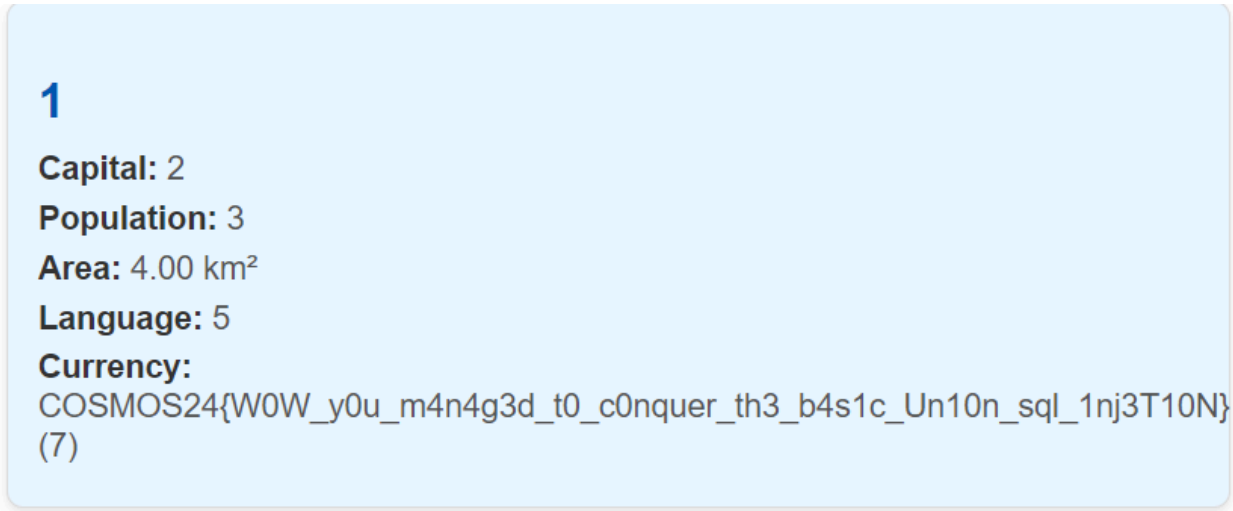


Terdapat table dengan nama yang menarik perhatian. Untuk check isi dari table ini dapat dengan meng-input injection “' UNION SELECT 1, 2, 3, 4, 5, column_name, 7 FROM information_schema.columns WHERE table_name = 'inimenariknih' -- ”



Imagine Losing😎

Nah ada table menarik lagi ni bernama value, kita dapat melihat lagi isi dari table ini dengan injection “' UNION SELECT 1, 2, 3, 4, 5, value, 7 FROM inimenariknih -- ”



Flag:COSMOS24{W0W_y0u_m4n4g3d_t0_c0nquer_th3_b4s1c_Un10n_sql_1nj3T10N}

[foren]

1. Mr. Vige

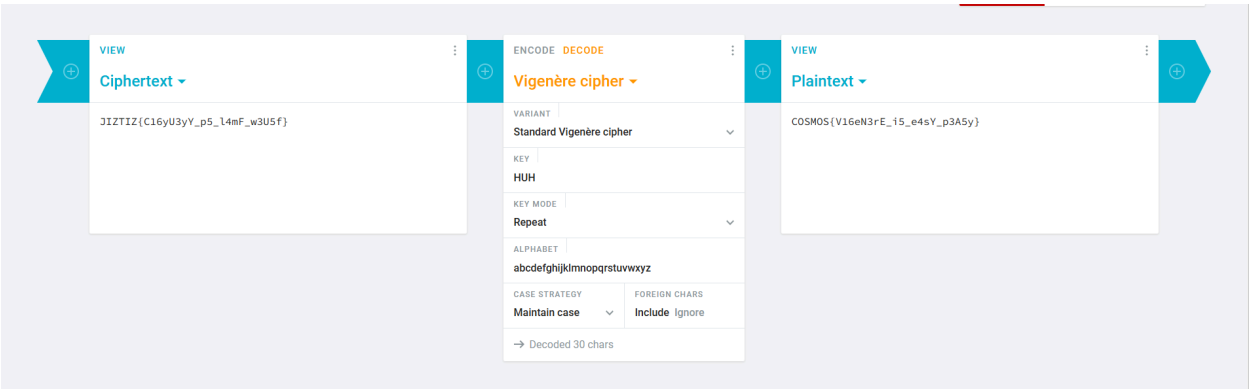
Mr.Vige
Author : Maet

HUH who tf is Mr.Vige??

Di chall ini, kami diberikan sebuah file berformat **.jpeg**. Setelah kami coba untuk cek metadata file dengan exiftool, kami mendapat sebuah comment dengan **Vigenere cipher** yang kemudian kami sadari itu adalah *fake flag* (awas admin aku tandain 😡).

```
┌──(shizukana㉿LAPTOP-BJKHV1O6)-[~/cosmos]
└─$ exiftool table.jpeg
ExifTool Version Number         : 12.76
File Name                       : table.jpeg
Directory                       : .
File Size                       : 21 kB
File Modification Date/Time     : 2024:11:15 09:49:13+07:00
File Access Date/Time           : 2024:11:15 09:49:13+07:00
File Inode Change Date/Time     : 2024:11:15 09:49:13+07:00
File Permissions                : -rwxr-xr-x
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Exif Byte Order                 : Big-endian (Motorola, MM)
XP Comment                      : JIZTIZ{C16yU3yY_p5_U0n_Ao4n_3H5f}
Padding                         : (Binary data 268 bytes, use -b option to extract)
Image Width                     : 213
Image Height                    : 236
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 213x236
Megapixels                      : 0.050
```

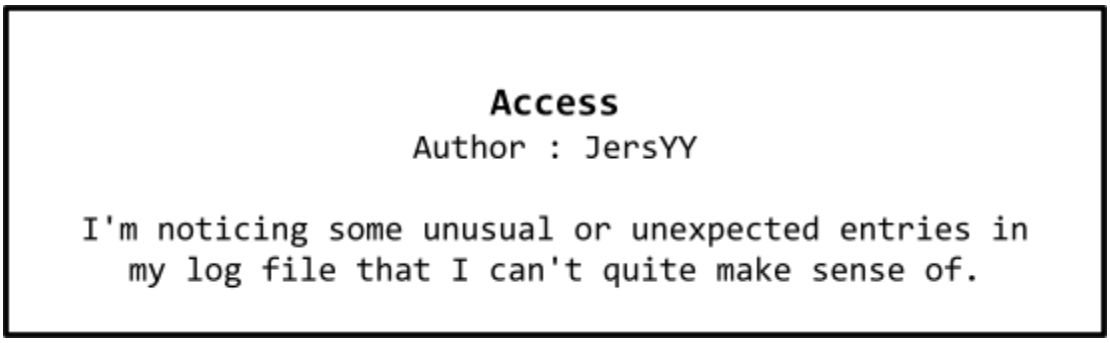
Akhirnya kami coba cek steganograph yang mungkin saja ada di **table.jpeg**. Benar saja isinya diekstrak ke “Mr.Vige.txt”. Langsung saja kita buka. Kami mendapat vigenere cipher lagi. `JIZTIZ{C16yU3yY_p5_l4mF_w3U5f}`. Key yang akan kami gunakan adalah “*HUH*” karena sepertinya itu kode dari deskripsi chall.



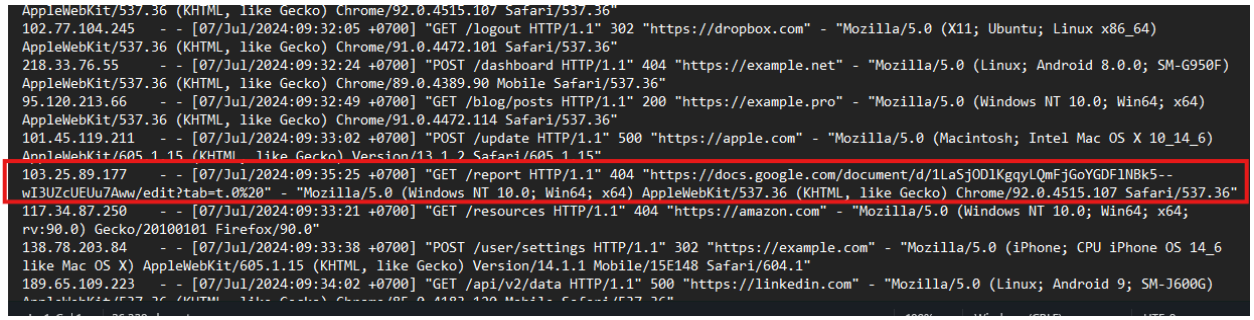
Hell yeahh!!

Flag: COSMOS{V16eN3rE_i5_e4sY_p3A5y}

2. Access



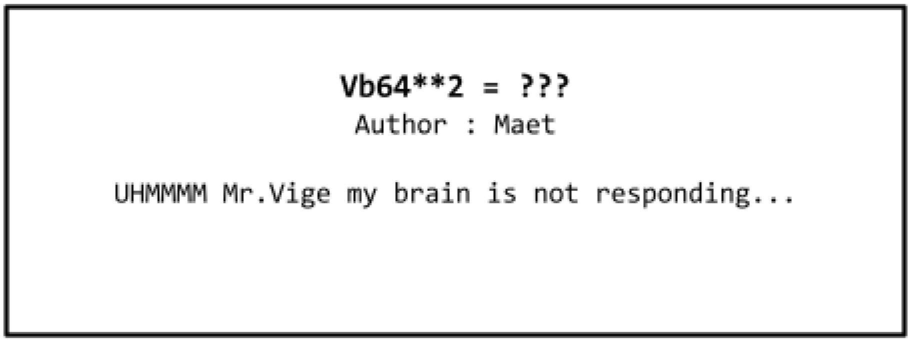
Kami diberikan sebuah file log yang berisi log suatu web. Di sana terdapat banyak website-website baik dari method GET ataupun POST. Jika dilihat lebih **teliti**, ada satu log yang mengarah ke ***docs.google.com***. Setelah dibuka web itu, maka akan didapatkan flag-nya. Yuhuuu!



Flag: COSMOS24{ITs_34Sy_1f_U_an4LyZE_it_W3ll!!!}

[crypto]

1. **Vb64**2 = ???**

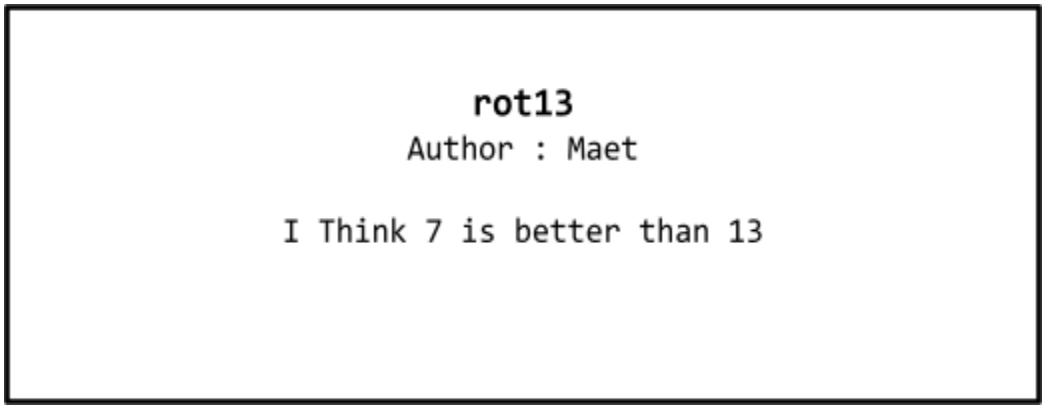


Pada chall ini, diberikan suatu text file yang sepertinya di-encrypt menggunakan **base64**. Setelah di-decrypt ternyata masih berbentuk **base64**. Kemudian kami mendapatkan sebuah text yang kurang jelas apa maknanya. Setelah mencari berbagai referensi, ternyata ini adalah **brainfuck text**.

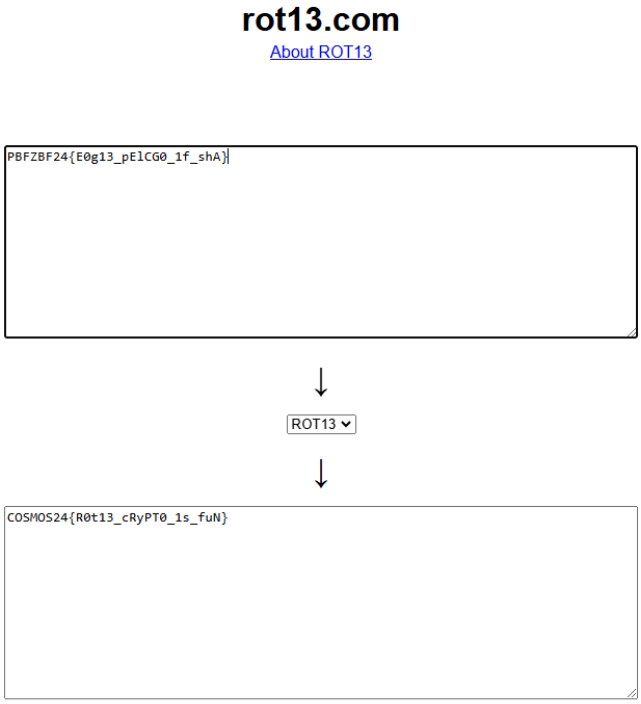
Kami menggunakan online tools ini untuk decrypt teks brainfuck. Ternyata flag masih di-encrypt menggunakan **vigenere cipher**. Boom, akhirnya kami dapatkan flagnya dengan menggunakan Key *"UHMMM"*.

Flag: COSMOS{bR41n_fUck_1s_n0T_tH4t_h4rD_r16Ht}

2. Rot13



Jelas sekali chall kali ini memiliki flag yang dienkripsi menggunakan **rot13**. Lamgsung kita coba dengan online tools [rot13.com](rot13.com).



Mudah saja

Flag: COSMOS24{R0t13_cRyPT0_1s_fuN}

3. Diffie and Hellman

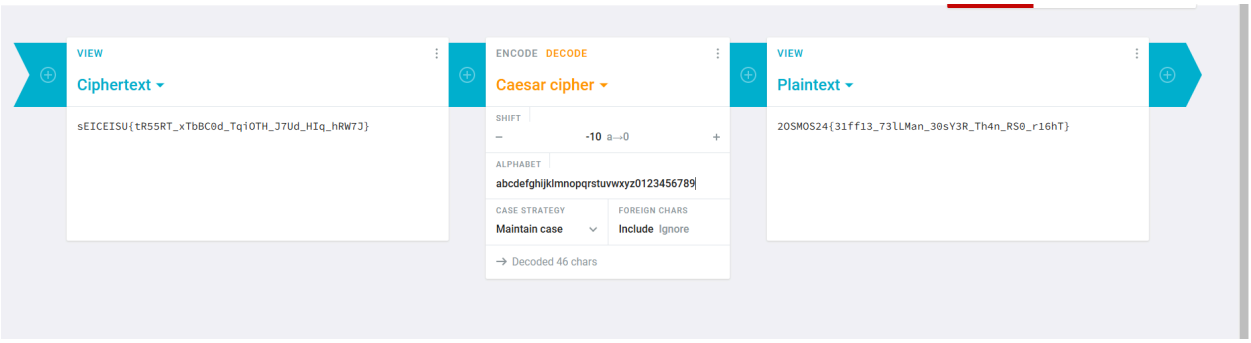
Diffie and Hellman
Author : Maet

Diffie?? Hellman?? who are they?

Di chall ini, diberikan sebuah file python yang berisi variabel **p, g, a, b**. Setelah mempelajari sekilas tentang **Diffie-Hellman** key exchange, ternyata ciphertext dienkripsi menggunakan sistem itu. Selanjutnya, kami menggunakan [Diffie-Hellman calculator] untuk mendapatkan key atau kuncinya.

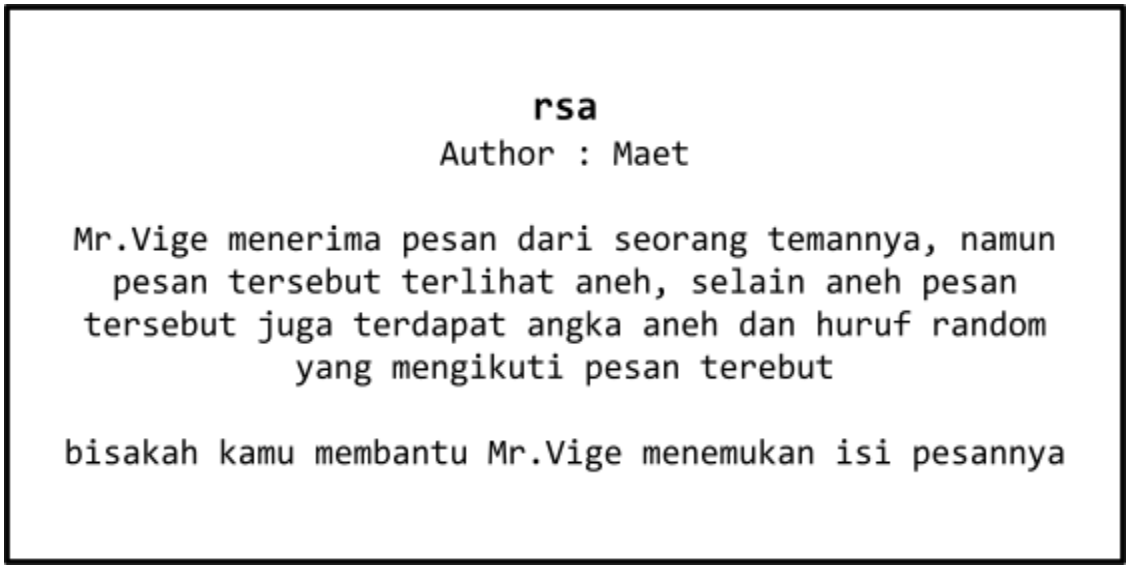
```
Diffie-Hellman
    P = 59
    G = 47
priv. 🔑 a = 19
priv. 🔑 b = 47
pub. 🔑 A = 55
pub. 🔑 B = 39
secret 🔑 (a,b) = 10
10
```

Key yang didapat adalah **10**. Selanjutnya, kami mencoba dekripsi ciphertext dengan **caesar cipher.** Alphabetnya kami tambahkan 0123456789 karena pada script python demikian.



2OSMOS24{31ff13_73lLMan_30sY3R_Th4n_RS0_r16hT}
Karena hasilnya sepertinya belum sempurna, akhirnya kami modifikasi. Seharusnya "2" di awal adalah "C", berarti untuk mendapatkan flag yang sempurna, bagian yang janggal seperti "RS0", "30sY3R", dll harus digeser 10.
Flag: COSMOS24{D1ff13_H3lLMan_3AsY3R_Th4n_RSA_r16hT}

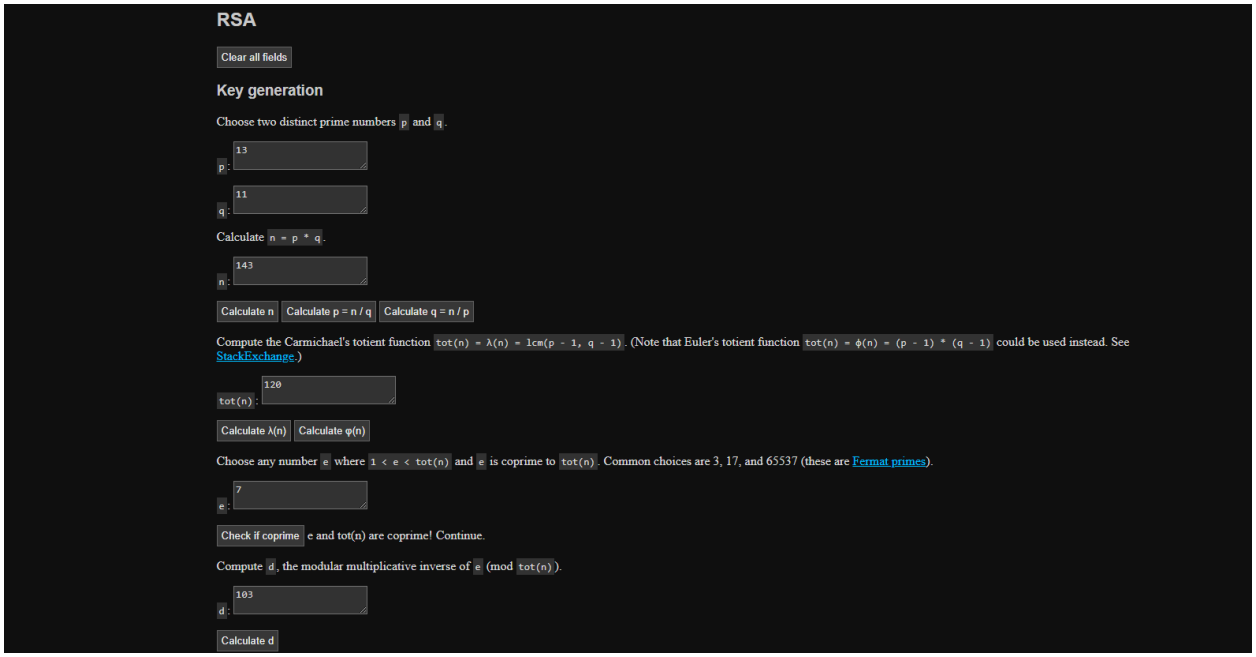
4. rsa



Di chall ini, kami mendapatkan file python yang berisi **ciphertext, nilai p, e dan q**. Selanjutnya kami mencoba kalkulasi dengan beberapa script untuk decrypt ciphertext. Dari semua script yang kami coba, hampir semuanya memberikan output `CMAW15WFuNWi5n'TW1@`. Sepertinya bukan ini isi flagnya.

Akhirnya, kami coba dengan online tools seperti rapidtables dan onlinetools. Dari sana, kami ubah ciphertext menjadi decimal number. Setelah dicoba kalkulasi dengan **p, q, d, e** dan **n** yang kami dapat melalui rsa calculator, outputnya tetap saja sama, `CMAW15WFuNWi5n'TW1`.

P = 13
Q = 11
D = 103
E = 143
N = 7



Saat waktu pengerjaan tinggal 10 menit, akhirnya kami memutuskan untuk konversi ciphertext secara manual satu-per-satu. Dapat dilihat dari tabel ASCII di bawah. *Tcih, online tools tak bisa diandalkan*

00 000 NUL	20 032	40 064 @	60 096 `	80 128 Ç	A0 160 á	C0 192 └	E0 224 α
01 001 ☺	21 033 !	41 065 A	61 097 a	81 129 ü	A1 161 í	C1 193 ┴	E1 225 ß
02 002 ☻	22 034 "	42 066 B	62 098 b	82 130 é	A2 162 ó	C2 194 ┬	E2 226 Γ
03 003 ♥	23 035 #	43 067 C	63 099 c	83 131 â	A3 163 ú	C3 195 ├	E3 227 π
04 004 ♦	24 036 $	44 068 D	64 100 d	84 132 ä	A4 164 ñ	C4 196 ─	E4 228 Σ
05 005 ♣	25 037 %	45 069 E	65 101 e	85 133 à	A5 165 Ñ	C5 197 ┼	E5 229 σ
06 006 ♠	26 038 &	46 070 F	66 102 f	86 134 å	A6 166 ª	C6 198 ╞	E6 230 µ
07 007 BEL	27 039 '	47 071 G	67 103 g	87 135 ç	A7 167 º	C7 199 ╟	E7 231 τ
08 008 BS	28 040 (	48 072 H	68 104 h	88 136 ê	A8 168 ¿	C8 200 ╚	E8 232 Φ
09 009 VT	29 041)	49 073 I	69 105 i	89 137 ë	A9 169 ⌐	C9 201 ╔	E9 233 Θ
0A 010 LF	2A 042 *	4A 074 J	6A 106 j	8A 138 è	AA 170 ¬	CA 202 ╩	EA 234 Ω
0B 011 ♂	2B 043 +	4B 075 K	6B 107 k	8B 139 ï	AB 171 ½	CB 203 ╦	EB 235 δ
0C 012 ♀	2C 044 ,	4C 076 L	6C 108 l	8C 140 î	AC 172 ¼	CC 204 ╠	EC 236 ∞
0D 013 CR	2D 045 -	4D 077 M	6D 109 m	8D 141 ì	AD 173 ¡	CD 205 ═	ED 237 φ
0E 014 ♫	2E 046 .	4E 078 N	6E 110 n	8E 142 Ä	AE 174 «	CE 206 ╬	EE 238 ∈
0F 015 ☼	2F 047 /	4F 079 O	6F 111 o	8F 143 Å	AF 175 »	CF 207 ╧	EF 239 ∩
10 016 ►	30 048 0	50 080 P	70 112 p	90 144 É	B0 176 ▒	D0 208 ╨	F0 240 ≡
11 017 ◄	31 049 1	51 081 Q	71 113 q	91 145 æ	B1 177 ▓	D1 209 ╤	F1 241 ±
12 018 ↕	32 050 2	52 082 R	72 114 r	92 146 Æ	B2 178 ▓	D2 210 ╥	F2 242 ≥
13 019 ‼	33 051 3	53 083 S	73 115 s	93 147 ô	B3 179 ▓	D3 211 ╙	F3 243 ≤
14 020 ¶	34 052 4	54 084 T	74 116 t	94 148 ö	B4 180 ┤	D4 212 ╘	F4 244 ⌠
15 021 §	35 053 5	55 085 U	75 117 u	95 149 ò	B5 181 ╡	D5 213 ╒	F5 245 ⌡
16 022 ▬	36 054 6	56 086 V	76 118 v	96 150 û	B6 182 ╢	D6 214 ╓	F6 246 ÷
17 023 ↨	37 055 7	57 087 W	77 119 w	97 151 ù	B7 183 ╖	D7 215 ╫	F7 247 ≈
18 024 ↑	38 056 8	58 088 X	78 120 x	98 152 ÿ	B8 184 ╕	D8 216 ╪	F8 248 °
19 025 ↓	39 057 9	59 089 Y	79 121 y	99 153 Ö	B9 185 ╣	D9 217 ┘	F9 249 ∙
1A 026 EOF	3A 058 :	5A 090 Z	7A 122 z	9A 154 Ü	BA 186 ║	DA 218 ┌	FA 250 ·
1B 027 ←	3B 059 ;	5B 091 [	7B 123 {	9B 155 ¢	BB 187 ╗	DB 219 █	FB 251 √
1C 028 ∟	3C 060 <	5C 092 \	7C 124 |	9C 156 £	BC 188 ╝	DC 220 ▄	FC 252 ⁿ
1D 029 ↔	3D 061 =	5D 093]	7D 125 }	9D 157 ¥	BD 189 ╜	DD 221 ▌	FD 253 ²
1E 030 ▲	3E 062 >	5E 094 ^	7E 126 ~	9E 158 ₧	BE 190 ╛	DE 222 ▐	FE 254 ■
1F 031 ▼	3F 063 ?	5F 095 _	7F 127 ⌂	9F 159 ƒ	BF 191 ┐	DF 223 ▀	FF 255

Damn, benar saja. Simbol "◄" dibaca oleh online tools dan script sebagai "9668". Setelah mengulang konversi & kalkulasi secara manual lagi, dapatlah sebuah output CMA_15_FuN_i5n'T_1} loh sepertinya sudah mendekati. Kami coba ubah-ubah beberapa percobaan. Pertama-tama, seharusnya "CMA" adalah "RSA". Lalu, seharusnya setelah angka "1" di akhir ada "T" agar isi flag menjadi "RSA is fun isn't it". Dicoba

modifikasi mulai dari “T” dan “t” dan modifikasi “COSMOS{“ atau “COSMOS24{“.
Akhirnya, flag yang **correct** didapat.

Flag: COSMOS{RSA_15_FuN_i5n'T_1t}