WRITEUP CTF WRECKIT4.0 2023

Tim : TehManis
Solver : 1. Ari
2. Ahmad
Waktu : Pukul 09:00 WIB - 21:00 WIB
Hari : Sabtu
Tanggal : 8 April 2023

Sekilas Tentang CTF WRECKIT4.0 2023

CTF adalah singkatan dari Capture The Flag yang dimana tugas utamanya mencari sebuah Flag / Bendera yang berada pada sebuah sistem komputer yang mempunyai sebuah keamanan, biasaya tingkat keamanan tergantung penyelenggaranya.

Dan CTF WRECKIT4.0 2023 ini adalah kali ke empat WRECKIT menyelenggarakan sebuah kompetisi CTF di seluruh Indonesia.

CTF atau Capture The Flag ini dibuat bertujuan untuk melatih, menguji, dan mengudate wawasan kita sebagai pentester agar lebih terampil dan selalu update dengan path atau bug terbaru.

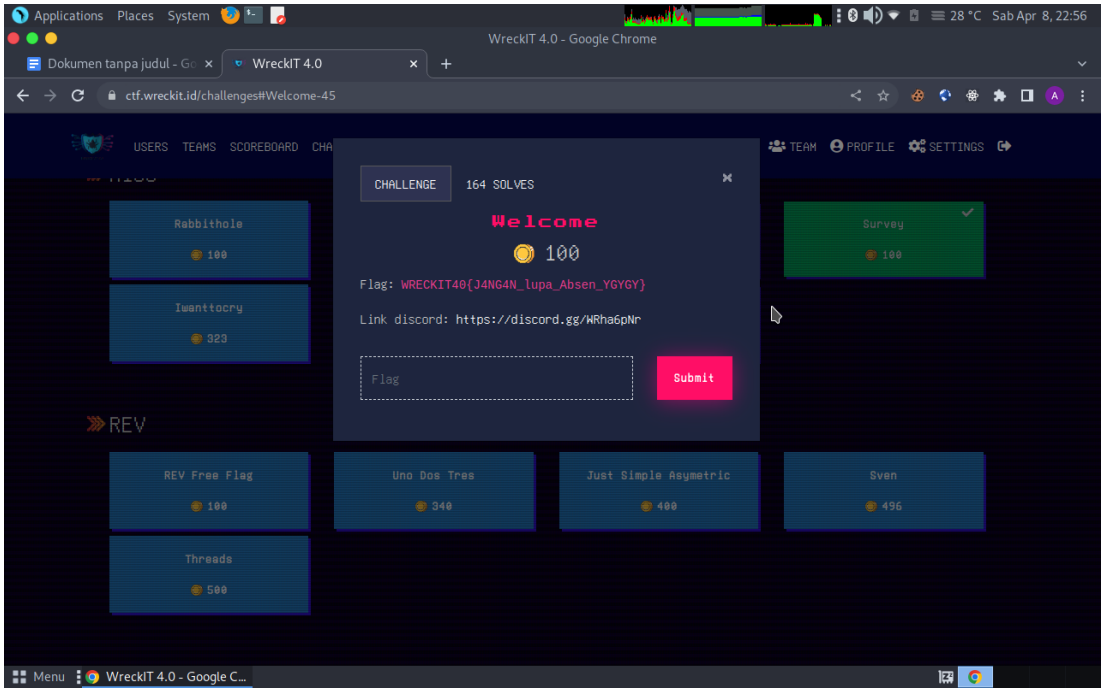
CTF WRECKIT4.0

Ada beberapa test yang diselenggarakan oleh WRECKIT4.0, Diantaranya dari Reverse Engineering, Web Exploitation, MISC, PWN, Forensic, dan Cryptography.

WRITEUP'S CTF WRECKIT4.0

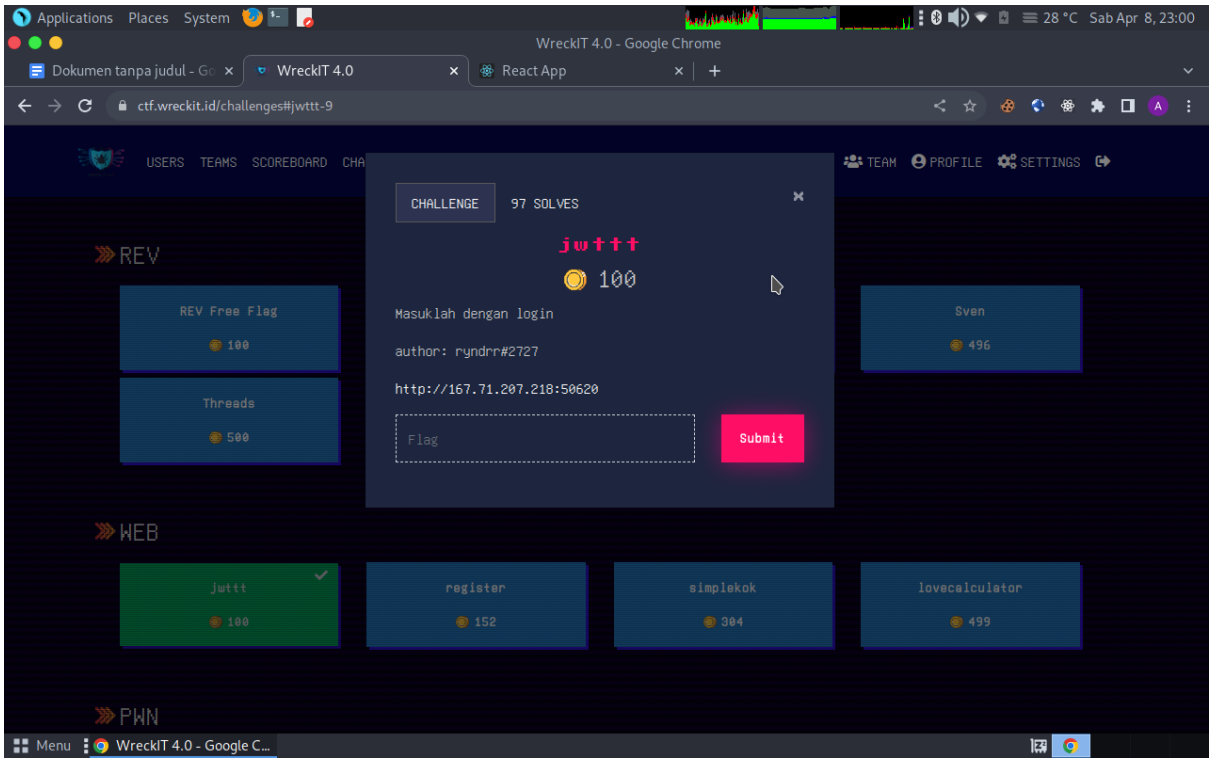
Kami telah mengikuti event CTF WRECKIT4.0 ini, dan ada beberapa soal soal yang dapat kami jawab, seperti berikut :

1. Welcome >> MISC
   Welcome ini adalah sambutan awal dari pihak WRECKIT4.0 dan langsung di berikan coin dan ditampilkan juga contoh Flag yang akan dicari pada soal berikutnya, berikut gambarnya :



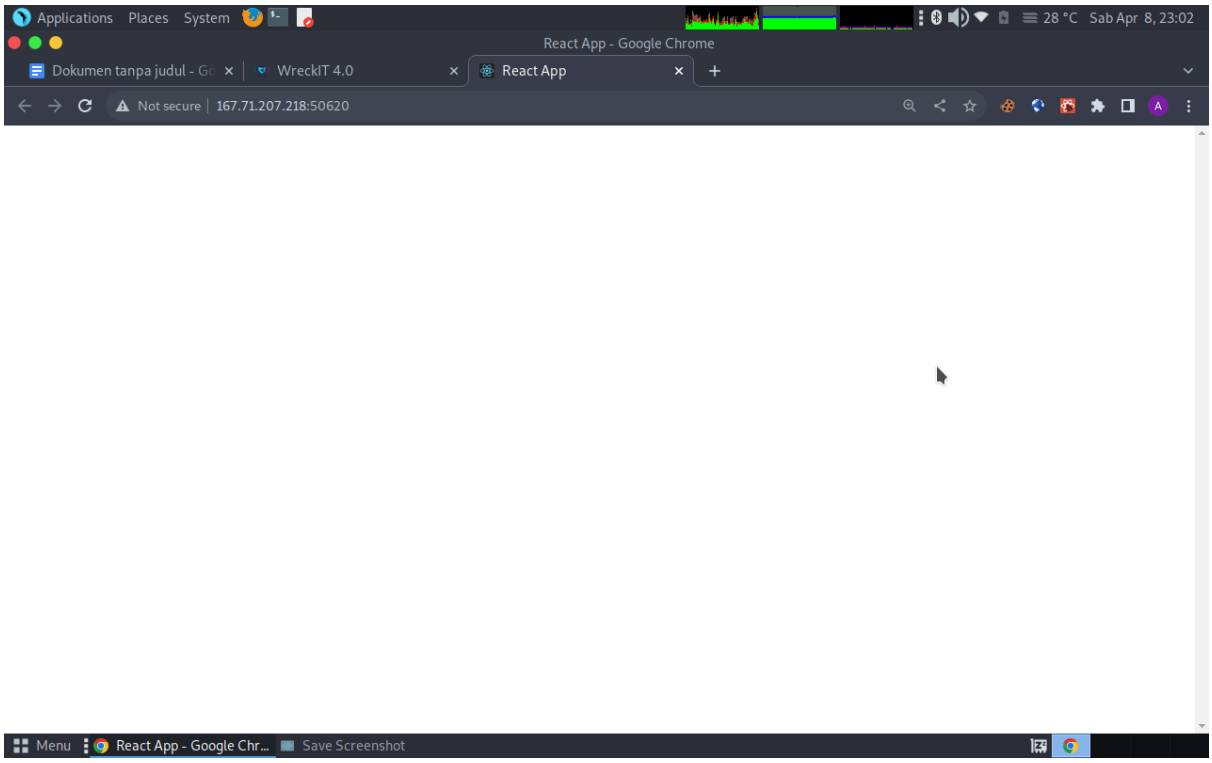
2. JWTT >> WEB EXPLOIT

JWTT adalah mencari dimana letak FLAG yang ada pada link, berikut gambarnya :

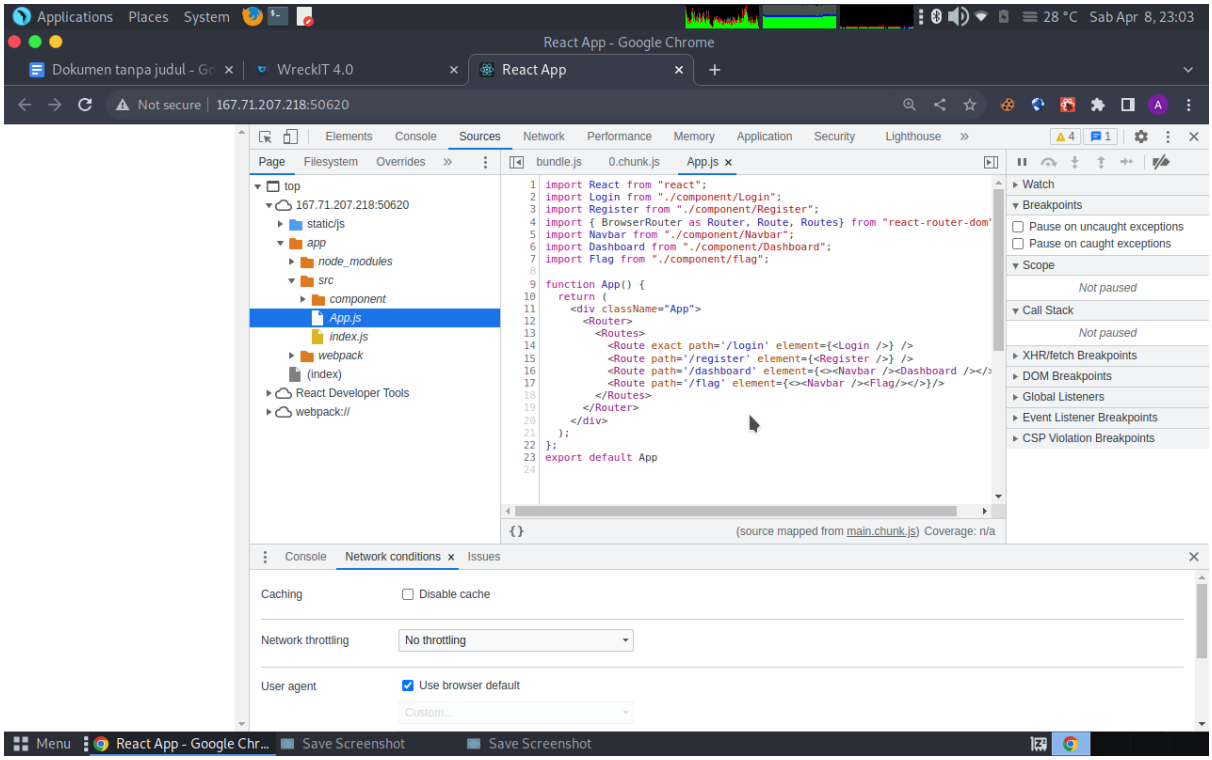


Berikut Untuk Cara Solvingnya :

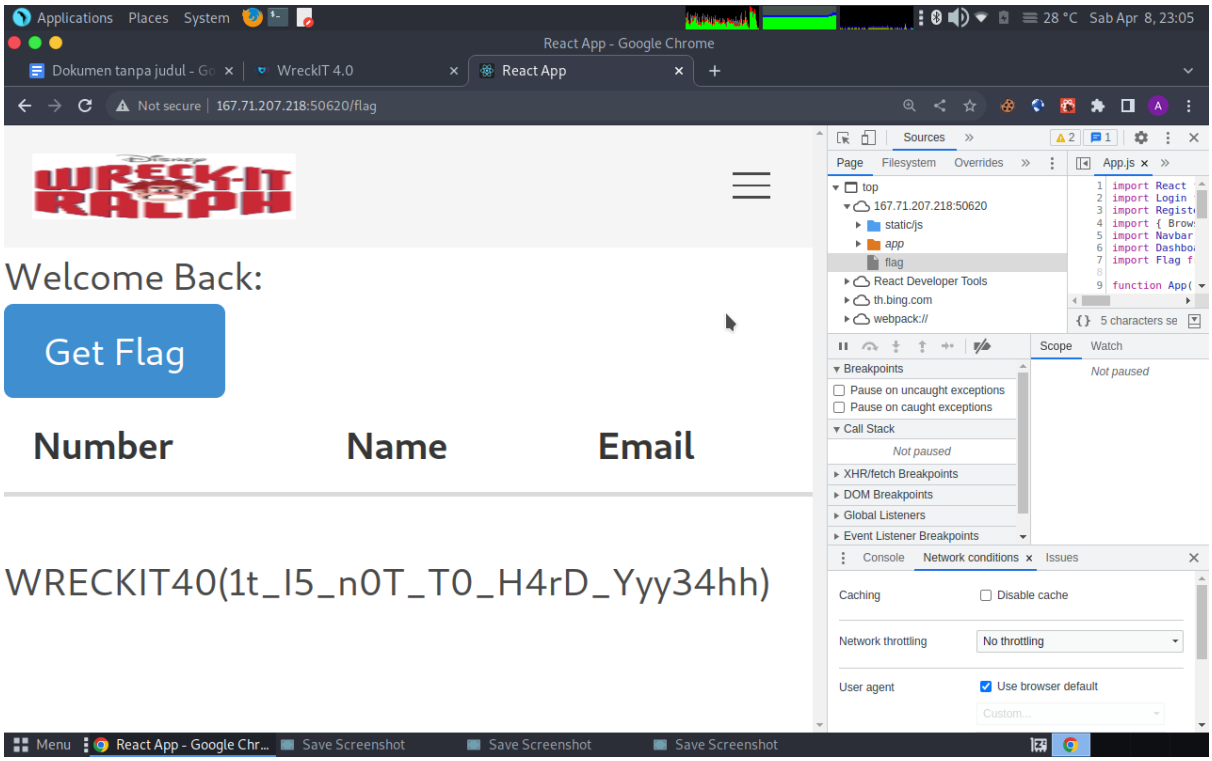
> Buka link tersebut, lalu akan muncul seperti gambar di bawah ini, blank tidak ada apa apa



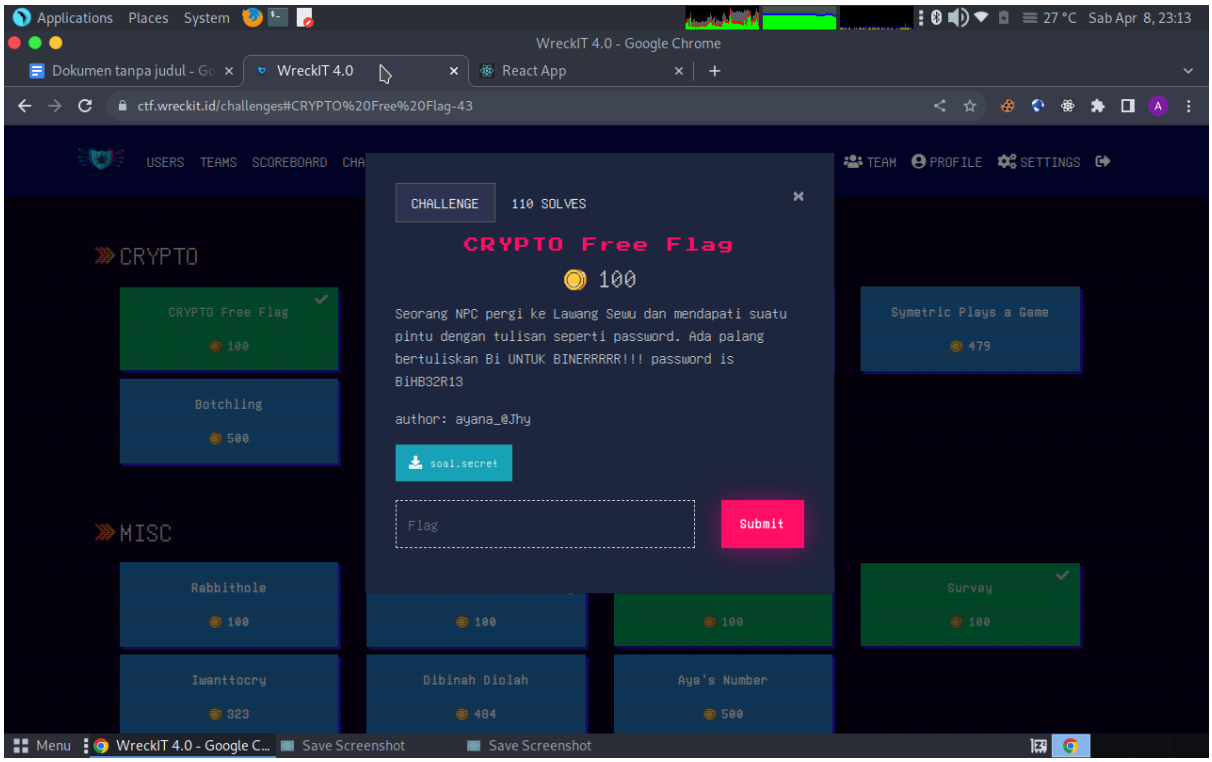
> Klik kanan >> Instpect element >> Sources, seperti gambar di bawah



> buka /flag pada browser tab baru, dan flag sudah ketemu seperti gambar di bawah,



3. Crypto Free Flag >> Cryptograpy
   Crypto Free Flag adalah sebuah soal yang dimana banyak sekali yang disembunyikan.

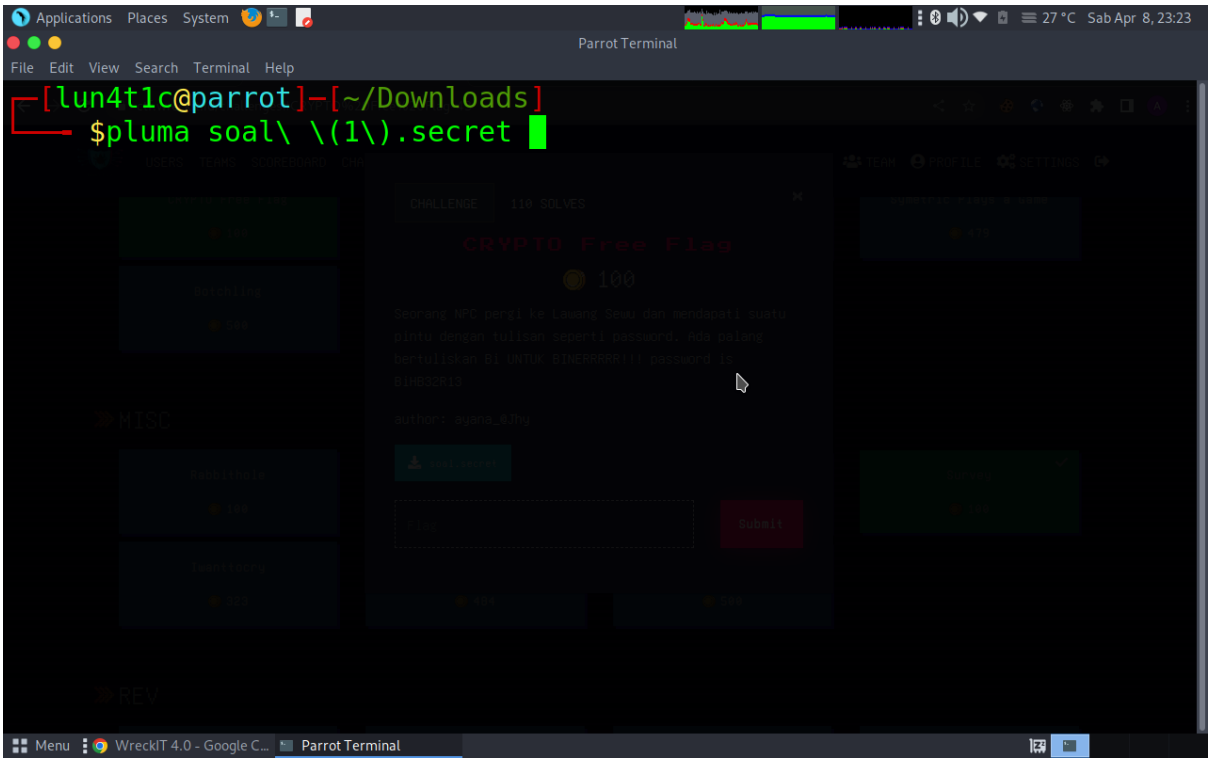


Tools :

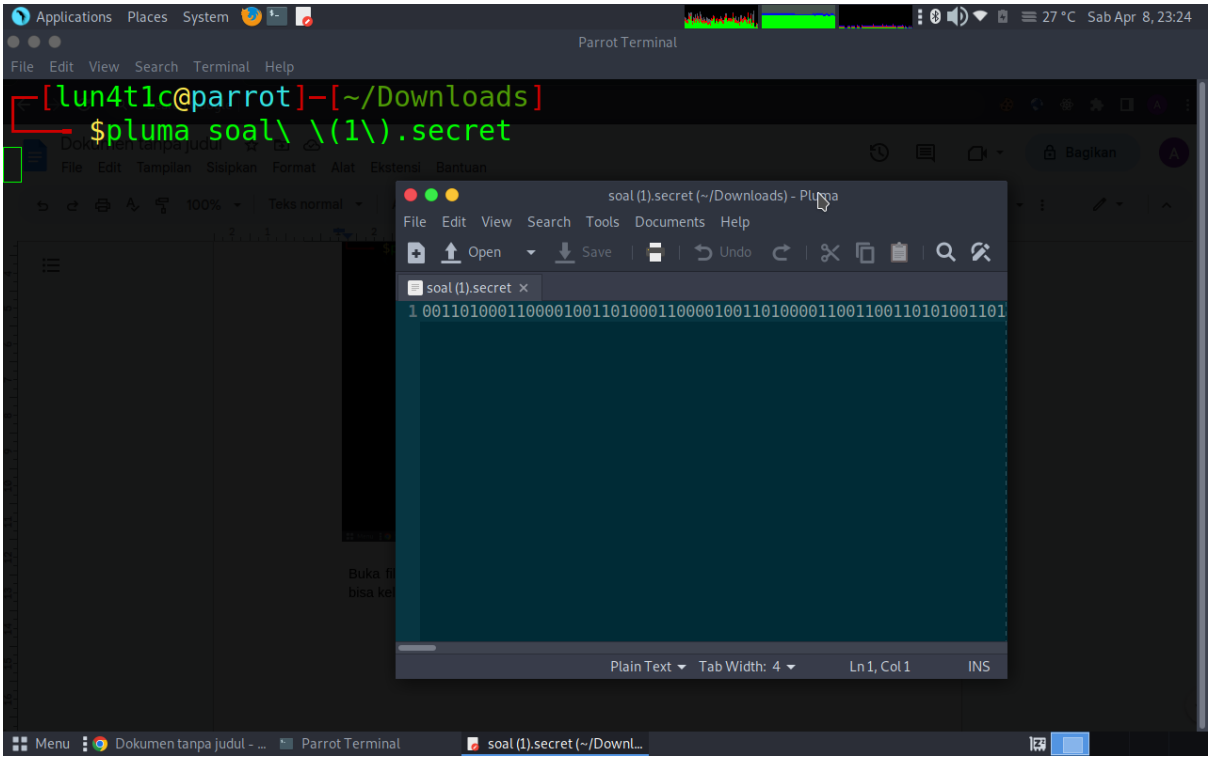
1. Multiple Hasing App, CyberChef
   Link : https://gchq.github.io/CyberChef/
2. Terminal
3.

Berikut Cara Untuk Solvingnya :

> Download file, setelah dibuka cobalah untuk membongkar file yang telah didown, berikut gambarnya



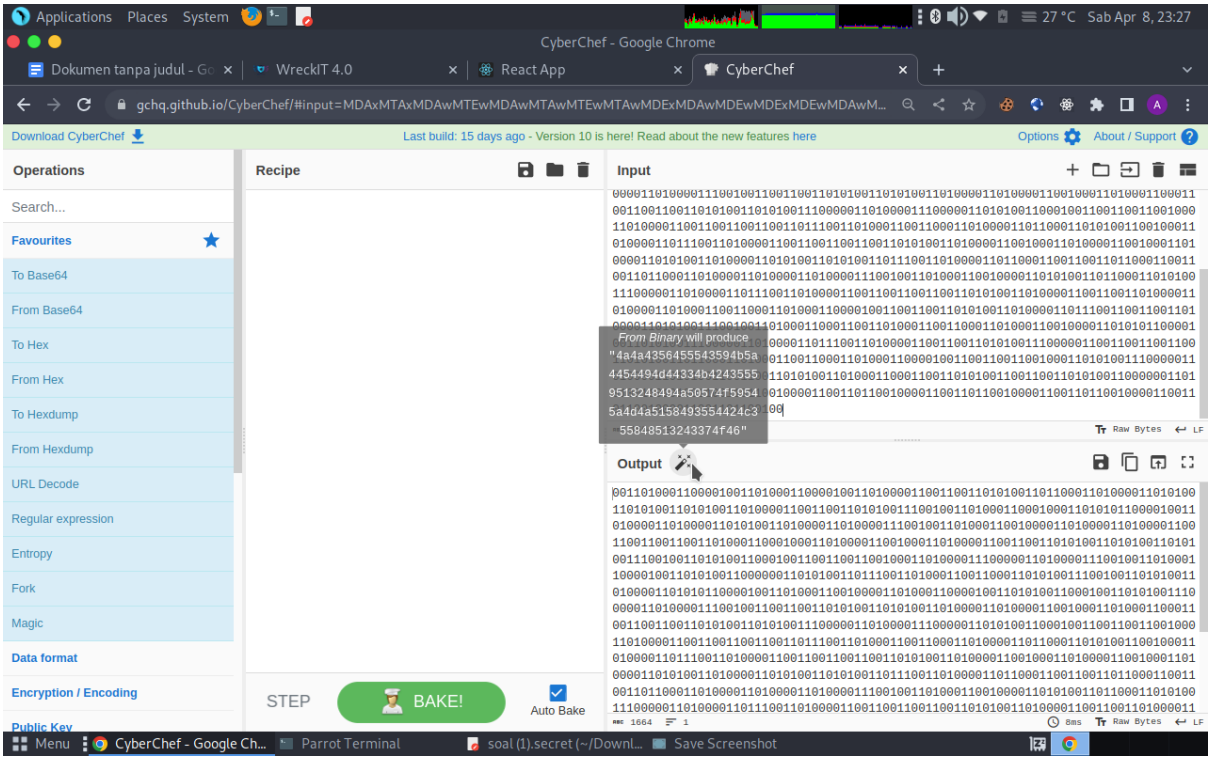
Buka file soal.secret, disini kami menggunakan aplikasi pluma agar rebih rapih dan bisa kelihatan semua, berikut gambarnya.



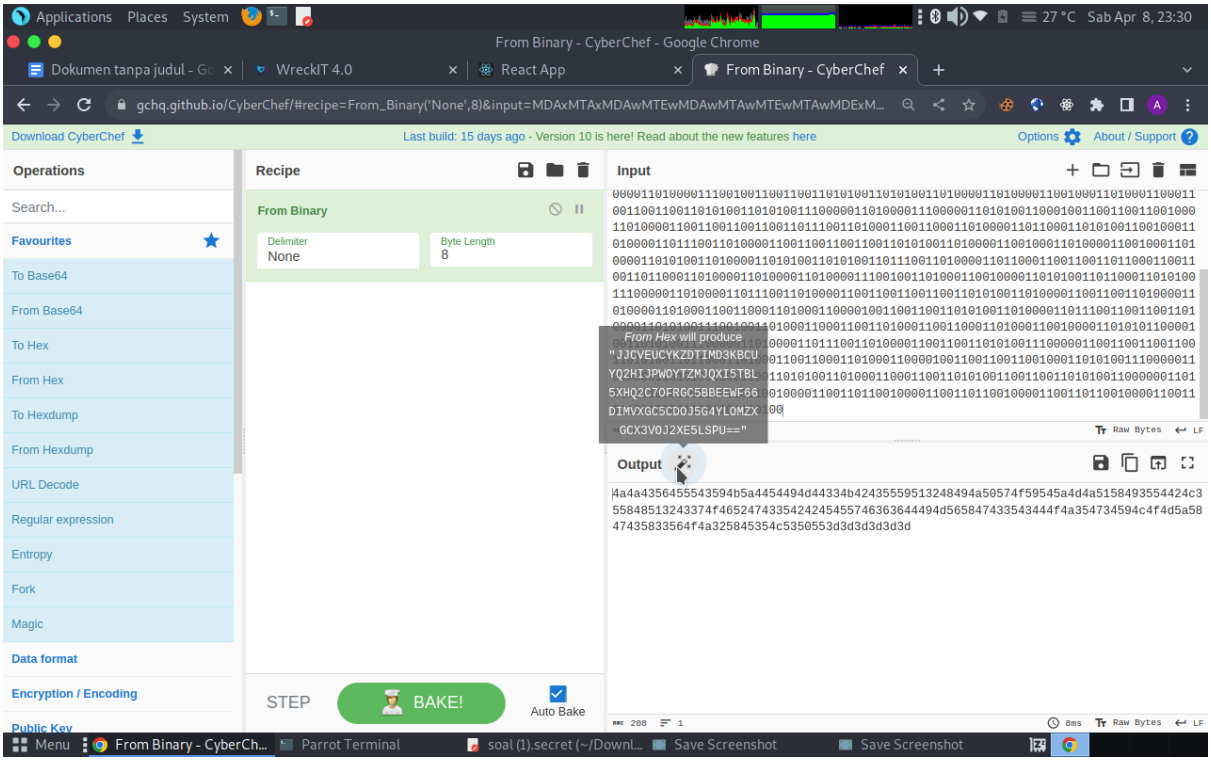
Selanjutnya copy binnary code yang muncul di pluma lalu masuk ke website yang sudah kami jabarkan di atas.

> Decrypt Binary to Text To Base32 To ROT13

Ini alasan kami kenapa menggunakan tools yang sudah kami tulis diatas, karena situs ini bisa langsung multiple decode, seperti gambar berikut,

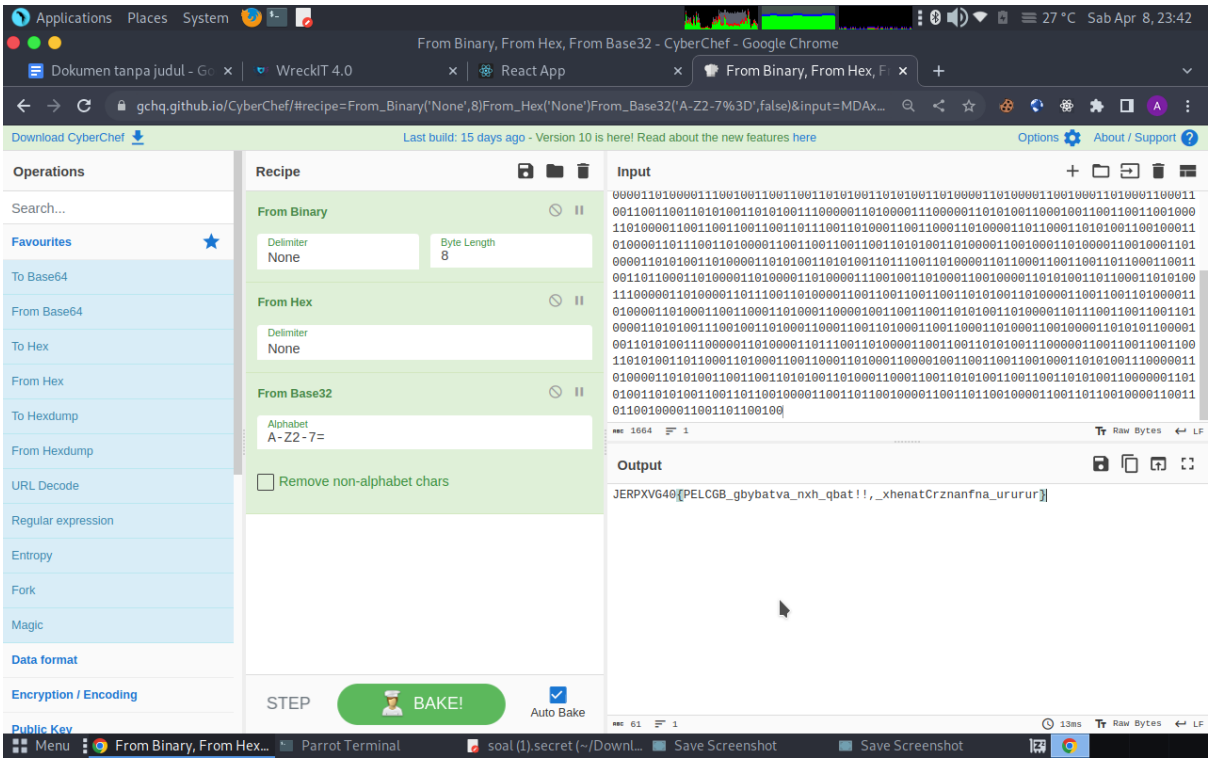


Dan pada tools diatas ini ada fitur yang cukup berguna untuk mengetahui identifier hash apa yang cocok utntuk memecah kode binari, Base32 rot13, dan.
Lalu klik pada tombool MAGIC, lalu akan muncul resultnya seperti ini



setelah tidak menemukan bug atau flagnya, selantutnya ialah untuk menentukan anda apakah sifatnya, seperti gabar di atas

Setelah itu lanjut saja sampai keluar nanti hasil decypt dari tools
>> Rubah dari BASE32 to ROT13
Dan langsung bertemu dengan dilenya



Ubah dari base32 ke text, maka ini yang anakan terjadi, dan, akan muncul seperti gambar di bawah