Old Portal

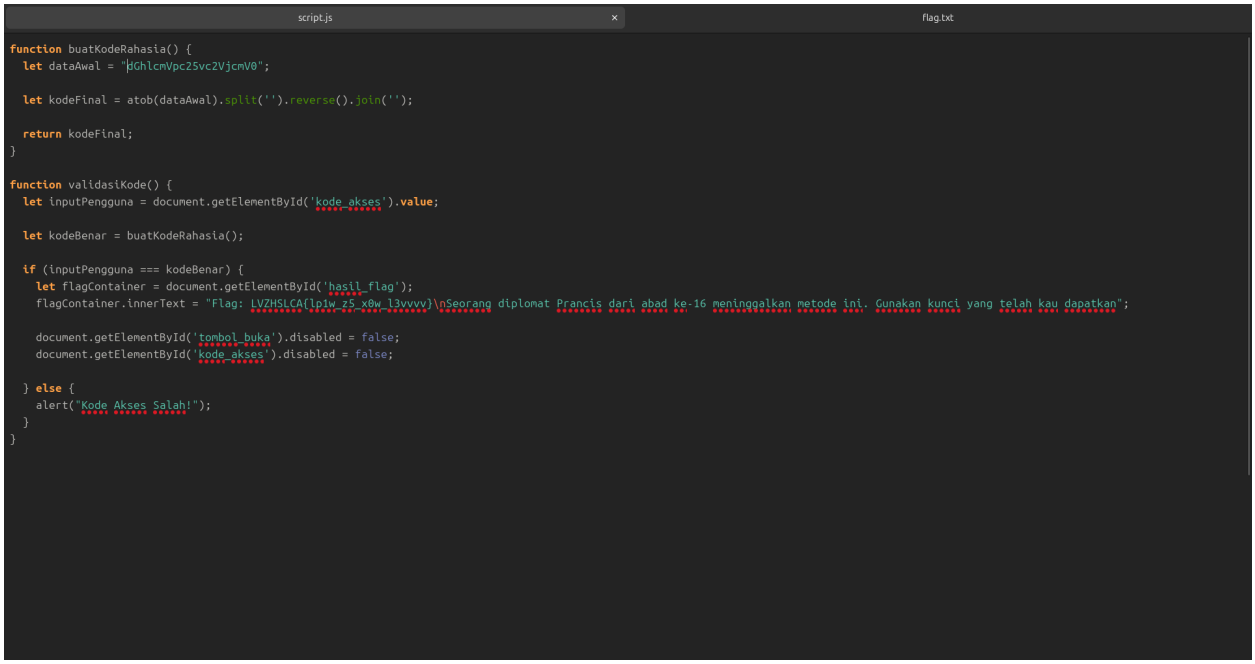
GejesGejes

Web Exploitan

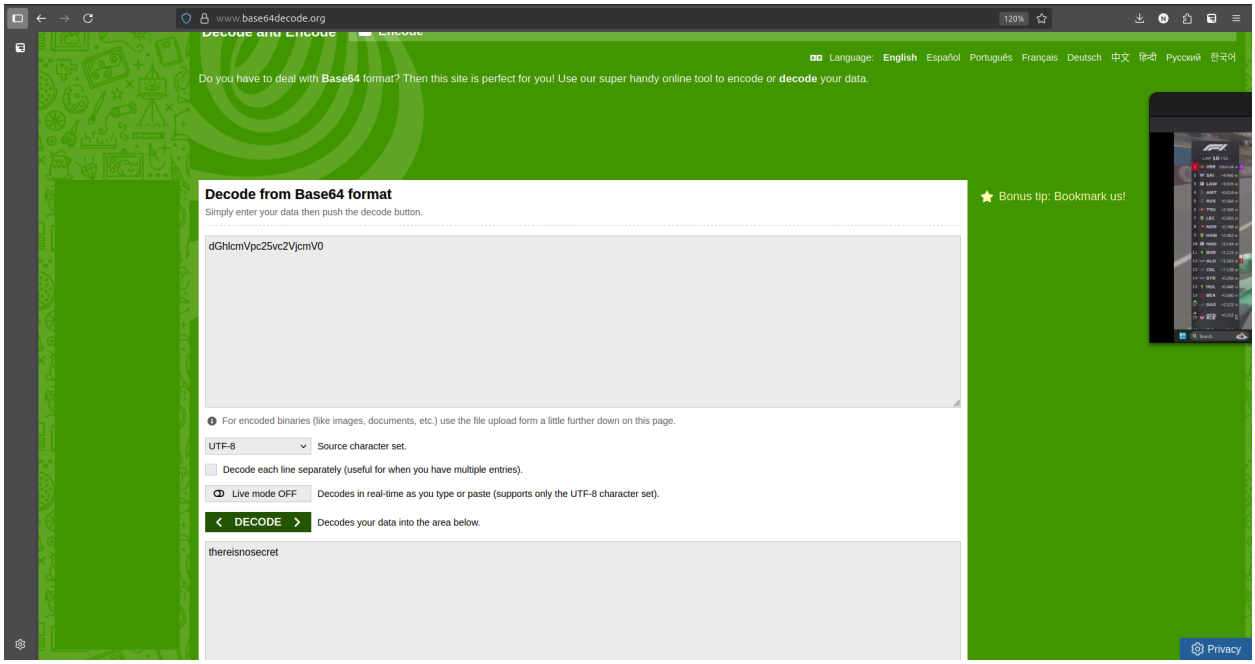
Write-up Penyelesaian

1. Diberikan `Portal.zip` , ketika di extract terdapat `index.html` dan `script.js`. File html sendiri berisi form yang harus diisi dengan suatu ‘kunci’.

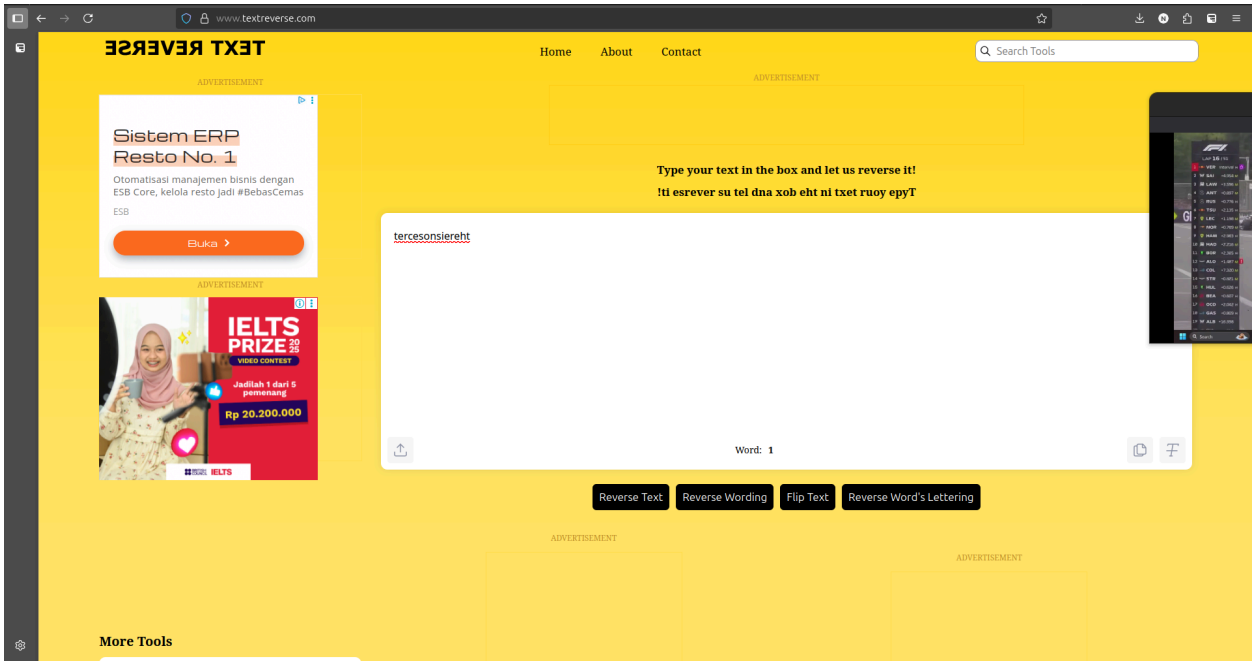
2. Saatnya melihat `script.js`. Terdapat fungsi buatKodeRahasia() yang terlihat sedikit mencurigakan dan mungkin mengandung kunci untuk Portal.



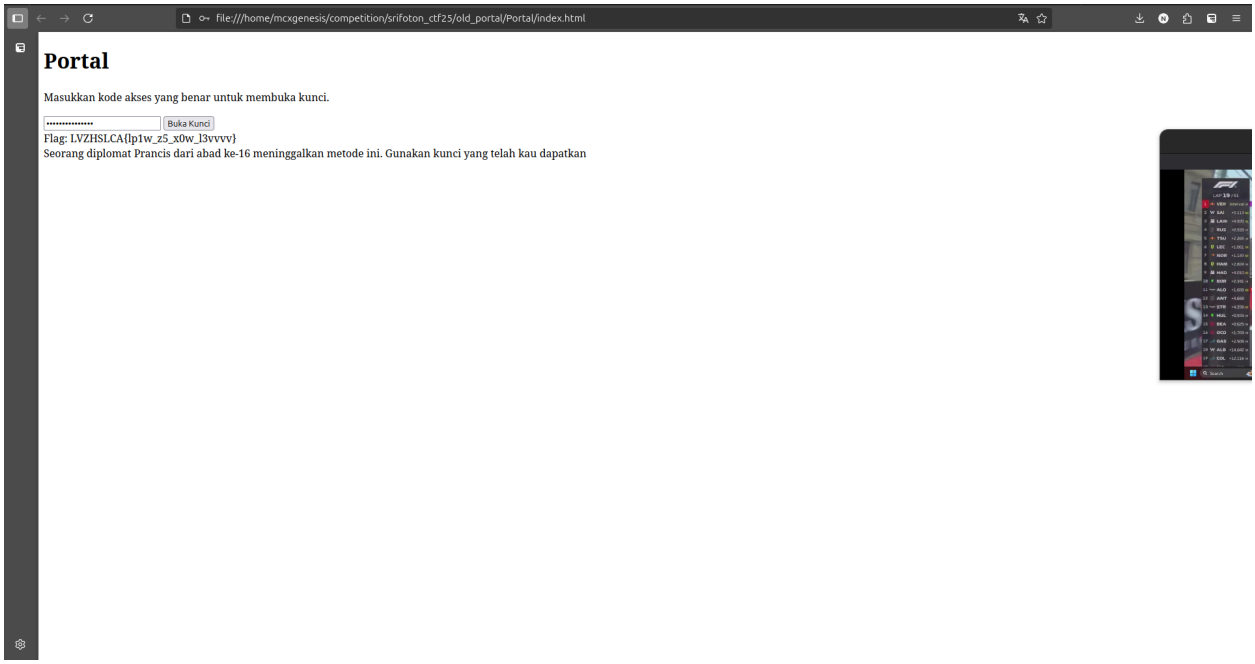
Tapi karena flagnya sudah terlihat (meski ter-encode) di file .js, saya bisa langsung fokus untuk memahami fungsi buatKodeRahasia() untuk memecahkan kunci encoding dari flag. Kunci rahasia yang beruapa ‘dataAwal’ diubah menjadi ‘kodeFinal’ dengan menggunakan atob, split, reverse, dan join. Yang perlu diperhatikan adalah atob() dan reverse(). Jadi data awal yang terenkripsi di reverse() kemudian di atob(). Fungsi atob() sendiri adalah fungsi untuk decode base64 pada teks. Sehingga, untuk kodeFinal adalah dataAwal yang telah di-encode base64 kemudian di reverse. Hal ini bisa dilakukan dengan menggunakan tools online.



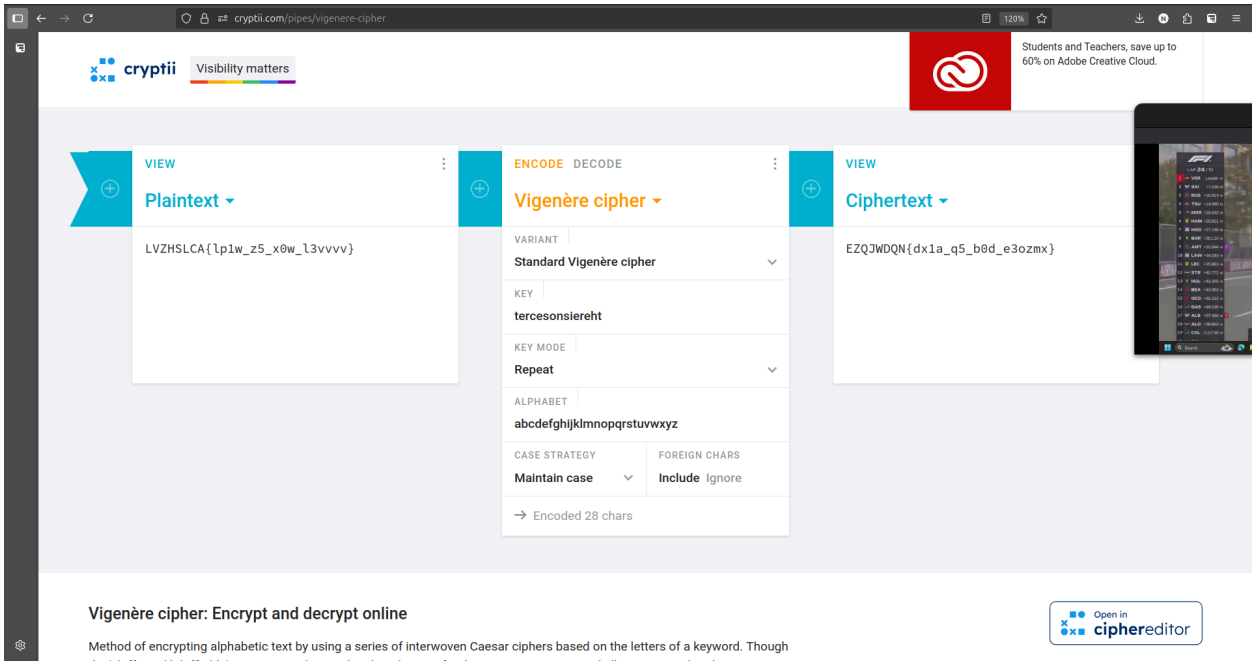
Didapatkan teks hasil decode: thereisnosecret



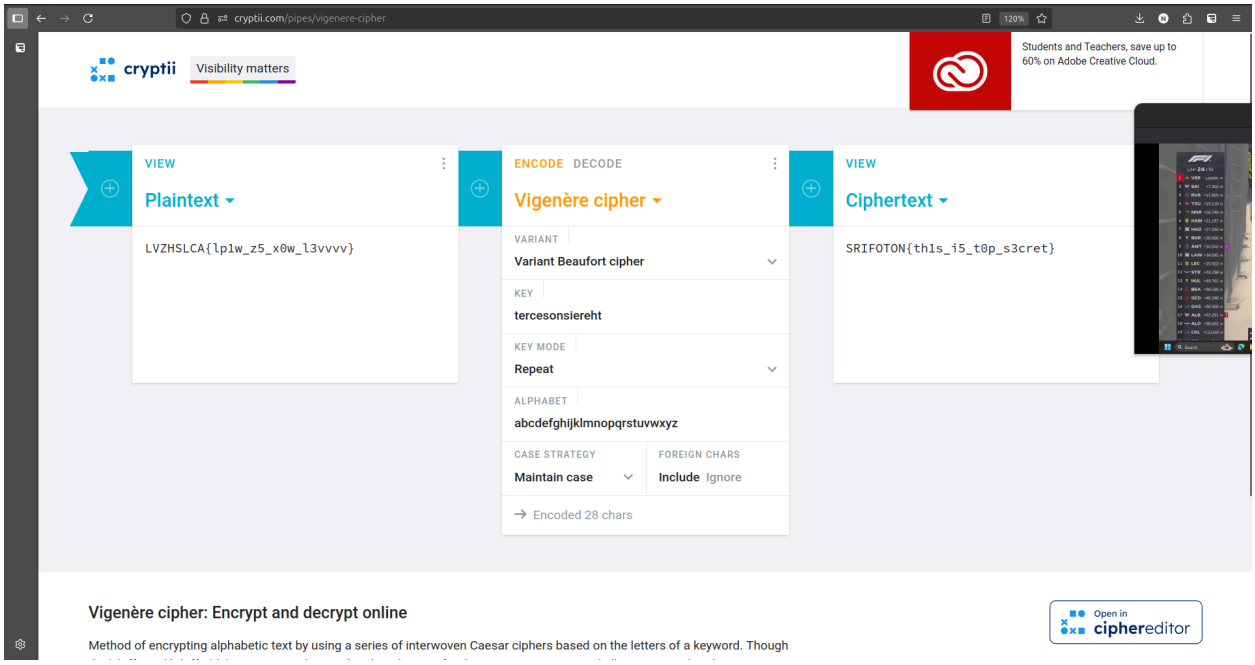
Didapatkan kunci: tercesonsiereht. Hal ini bisa dibuktikan dengan meng-submit key ke form html.



3. Didapatkan flag: LVZHSLCA{lp1w_z5_x0w_l3vvvv}. Didapatkan juga hint berupa ‘Seorang diplomat Prancis dari abad ke-16 meninggalkan metode ini. Gunakan kunci yang telah kau dapatkan’. Tidak lain tidak bukan ini adalah vigenere cipher. Tools online bisa digunakan untuk melakukan decode dengan vignere cipher. Kuncinya, kalau sesuai hint adalah ‘tercesonsiereht’.



Coba variannya diganti.



Flag: SRIFOTON{th1s_i5_t0p_s3cret}