

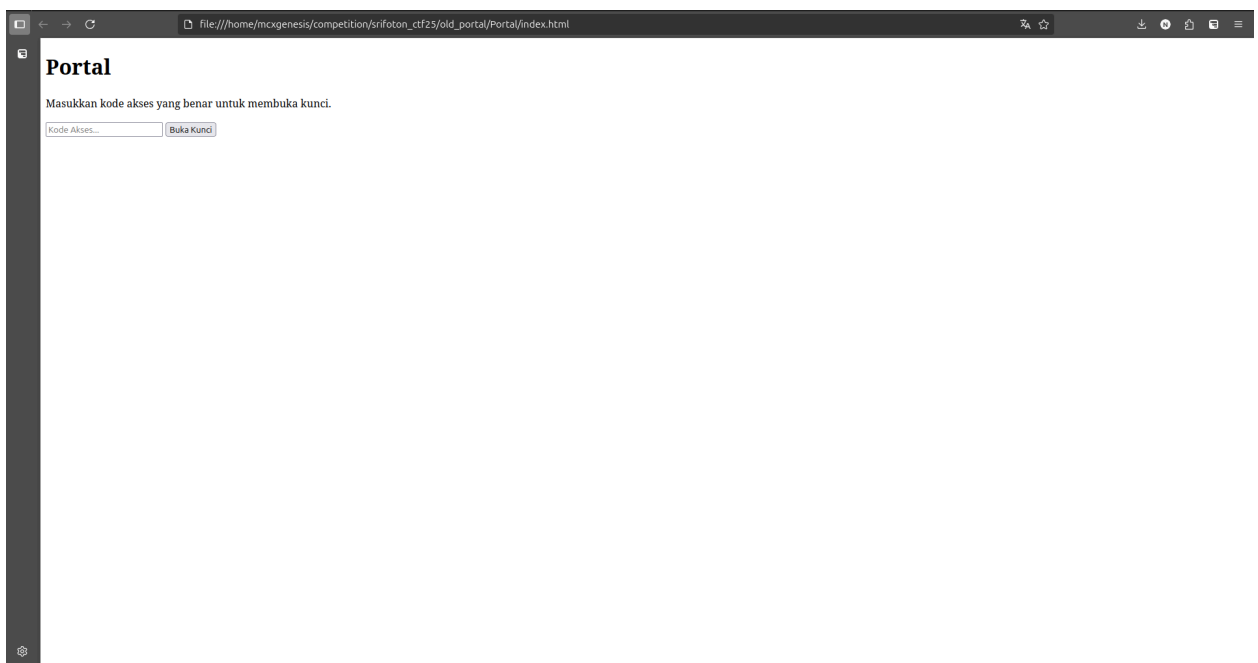
Old Portal

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.

```
script.js x flag.txt

function buatKodeRahasia() {
  let dataAwal = 'bGh1cmVpc25vc2VjcmV0';

  let kodeFinal = atob(dataAwal).split('').reverse().join('');

  return kodeFinal;
}

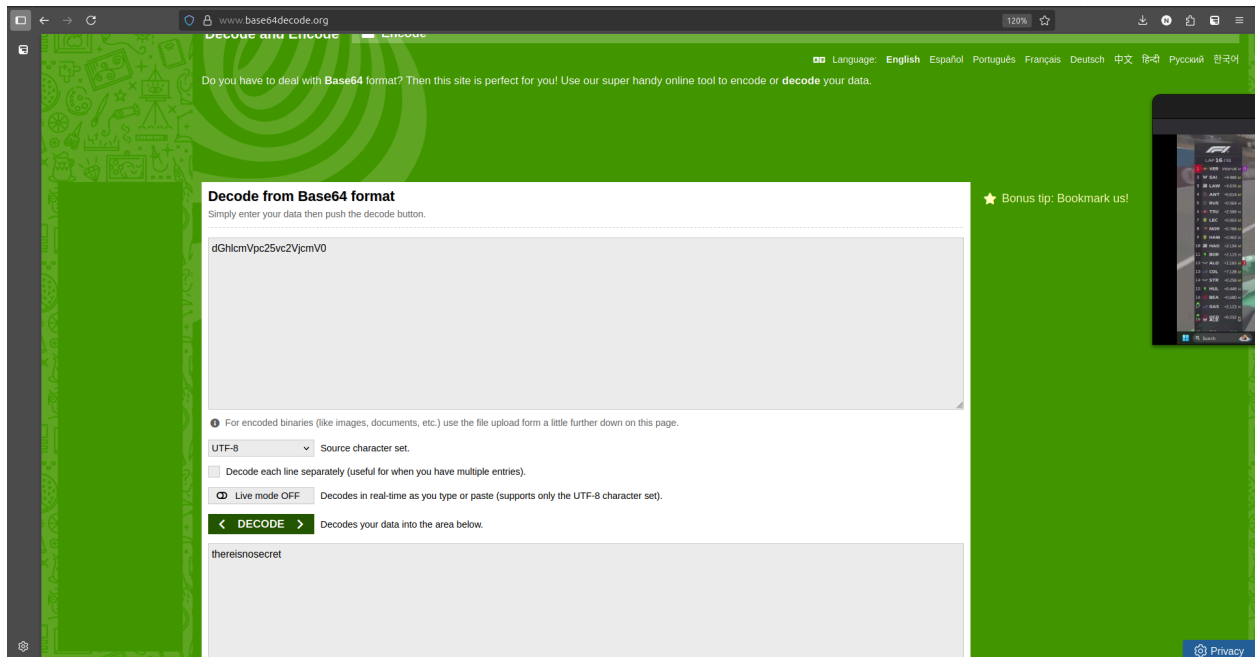
function validasiKode() {
  let inputPengguna = document.getElementById('kode_akses').value;

  let kodeBenar = buatKodeRahasia();

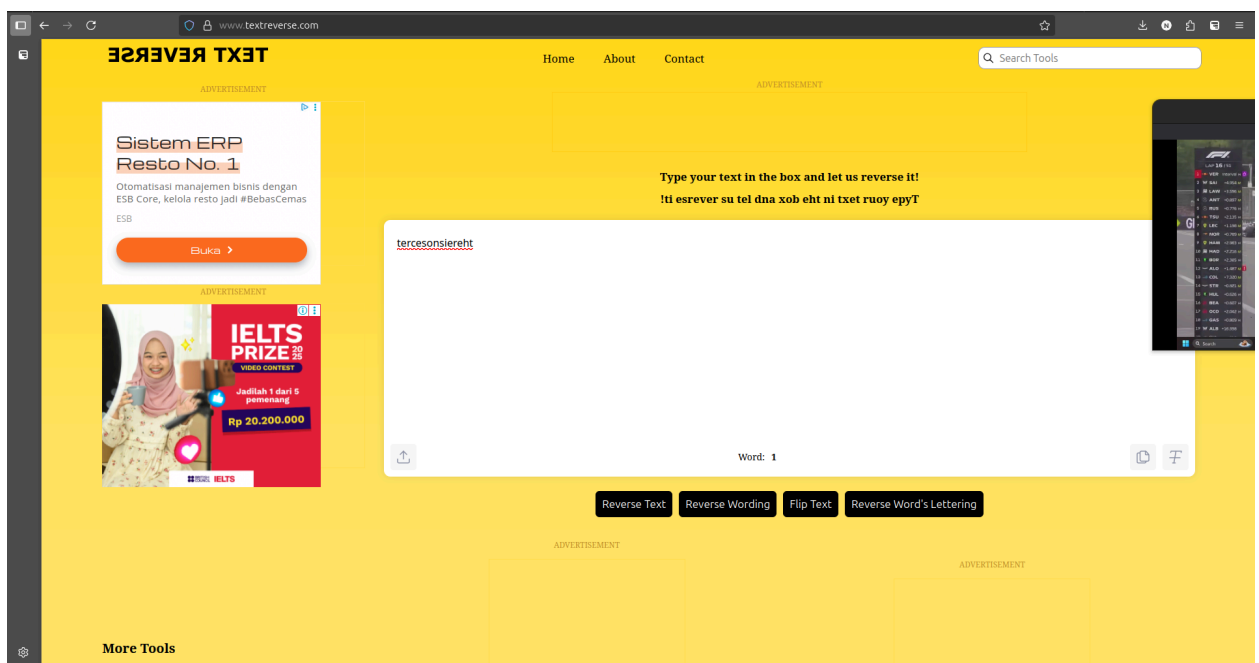
  if (inputPengguna === kodeBenar) {
    let flagContainer = document.getElementById('hasil_flag');
    flagContainer.innerText = "Flag: LVZHSICA[plw 75 x0w l3vvvv]\nSeorang diplomat Prancis dari abad ke-16 meninggalkan metode ini. Gunakan kunci yang telah kau dapatkan";

    document.getElementById('tombol_buka').disabled = false;
    document.getElementById('kode_akses').disabled = false;
  } else {
    alert("Kode Akses Salah!");
  }
}
```

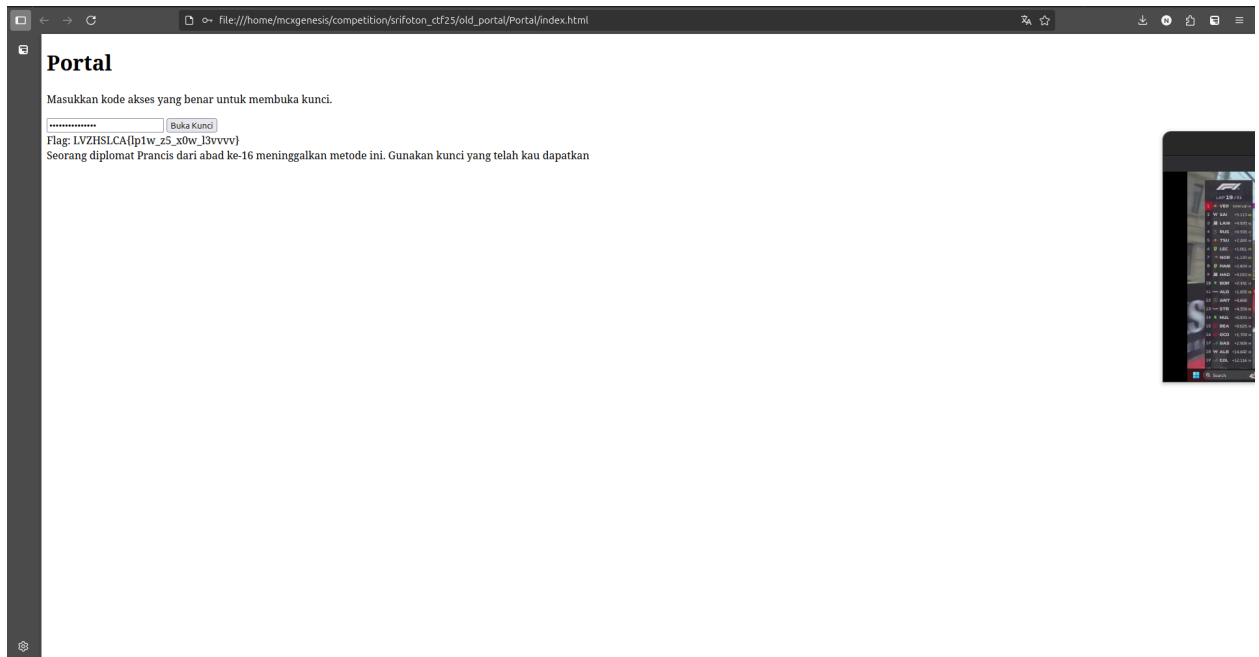
Tapi karena flagnya sudah terlihat (meski ter-encode) di file .js, saya bisa langsung fokus untuk memahami fungsi buatKodeRahasia() untuk memecahkan kunci encoding dari flag. Kunci rahasia yang berupa 'dataAwal' diubah menjadi 'kodeFinal' dengan menggunakan atob, split, reverse, dan join. Yang perlu 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.



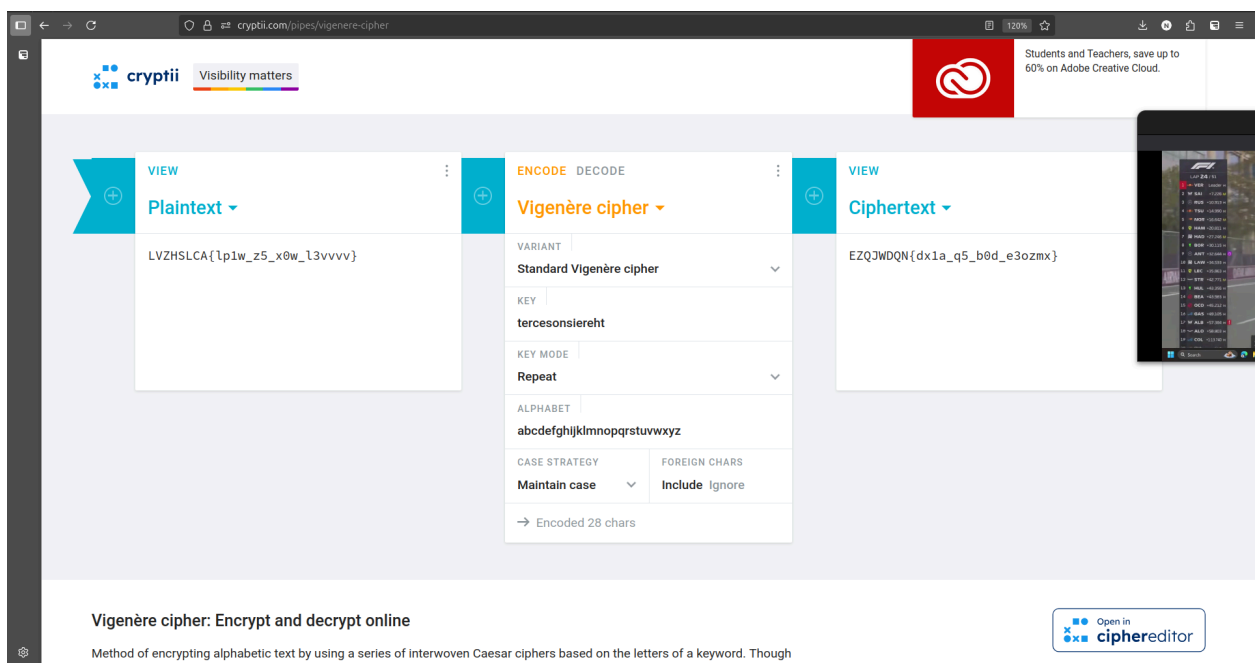
Didapatkan teks hasil decode: thereisnosecret



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



- 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 vigenere cipher. Kuncinya, kalau sesuai hint adalah ‘tercesonsiereht’.



Coba variannya diganti.

cryptii Visibility matters

Students and Teachers, save up to 60% on Adobe Creative Cloud.

VIEW

Plaintext ▾

LVZHSICA{lp1w_z5_x0w_l3vvvv}

ENCODE DECODE

Vigenère cipher ▾

VARIANT

Variant Beaufort cipher ▾

KEY

tercesonsiereht

KEY MODE

Repeat ▾

ALPHABET

abcdefghijklmnopqrstuvwxyz

CASE STRATEGY

Maintain case ▾

FOREIGN CHARS

Include Ignore

→ Encoded 28 chars

VIEW

Ciphertext ▾

SRIFOTON{th1s_i5_t0p_s3cret}

Vigenère cipher: Encrypt and decrypt online

Method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword. Though

Open in ciphereditor

Flag: SRIFOTON{th1s_i5_t0p_s3cret}