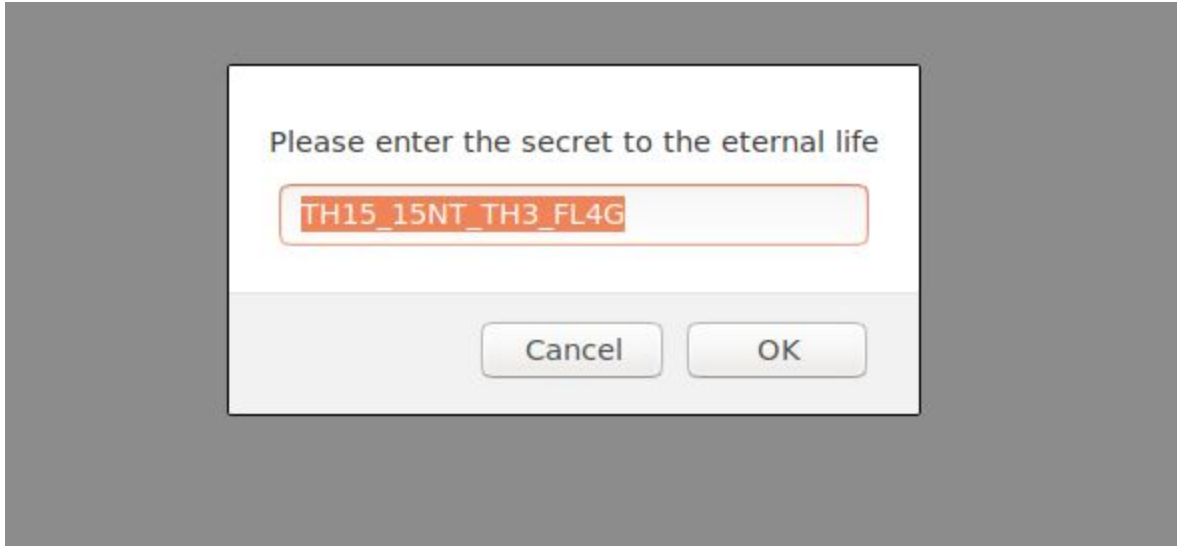


Webrev

Soal ini dibuat dengan tujuan sebagai tiebreaker (terdapat 2 soal lainnya).

Diberikan sebuah webpage di mana webpage meminta sebuah kata sandi. Jika diperhatikan, sudah terisi value yang kelihatan jelas seperti kata sandi tipuan.



Javascript yang diberikan cukup acak, sehingga perlu dirapikan “sedikit” agar mengerti codenya.

```
// "NDMSCRTH" or digits or '_'
if ([NDMSCRTH1234567890_].test(password)) {
  // password length = 0x15
  if (password.length == 0x15) {
    var i = 0x0;
    for (var j = 0x0; j < password.length; j++) {
      i += password.charCodeAt(j);
    }
    // sum of password must be 0x598
    if (i == 0x598) {
      i = 0x0;
      for (var j = 0x0; j < password.length; j++) {
        i ^= password.charCodeAt(j);
      }
      // xor of password's sum and password must be 0x26
      if (i == 0x26) {
        // way too much constraint...
        if (password.charAt(0xb) == 'T' && password.charAt(0x0) ==
            if (password.charAt(0x6) == password.charAt(0xd) && pa
            if (q(password.charAt(0x0)) && q(password.charAt(0
```

Soal seperti dapat di solve dengan cukup cepat menggunakan z3 solver. z3 merupakan SAT (satisfiability solver), di mana z3 ini digunakan untuk mengecek apakah kumpulan constraint yang sudah diberikan bersifat satisfiable (dapat terpenuhi) atau tidak. Selain untuk pengecekan

constraint, z3 dapat digunakan untuk mengecek model, yang artinya print apa yang menurut z3 memenuhi constraint.

Untuk lebih detail tentang contoh penggunaan z3, lihat ***solver.py***. Ketika solver di jalankan, muncul beberapa solusi. Ini merupakan password/flag, namun urutannya teracak-acak.

```
tempest@tempestuous: ~/projects/beefest/final/re/webrev master python solver.py
1ND0M13C15_T_3HS3_R3T
1ND0M13H15_T_3_S3CR3T
1ND0M13H15_T_3CS3_R3T
1ND0M13_15_TC3HS3_R3T
1ND0M13_15_TC3_S3HR3T
1ND0M13_15_T_3CS3HR3T
1ND0M13_15_T_3HS3CR3T
1ND0M13H15CT_3_S3_R3T
1ND0M13_15CT_3_S3HR3T
1ND0M13C15_T_3_S3HR3T
1ND0M13_15_TH3_S3CR3T
1ND0M13H15_TC3_S3_R3T
1ND0M13_15_TH3CS3_R3T
1ND0M13_15HTC3_S3_R3T
1ND0M13C15HT_3_S3_R3T
1ND0M13_15CTH3_S3_R3T
1ND0M13C15 TH3 S3 R3T
1ND0M13_15HT_3_S3CR3T
1ND0M13_15HT_3CS3_R3T
1ND0M13_15CT_3HS3_R3T
```

Terdapat satu yang cukup mendekati flag asli (karena kata-katanya cukup masuk akal dan tersusun rapi, kecuali satu huruf dan satu garisbawah).

Flag: ***BeeFest{1ND0M13_15_TH3_S3CR3T}***