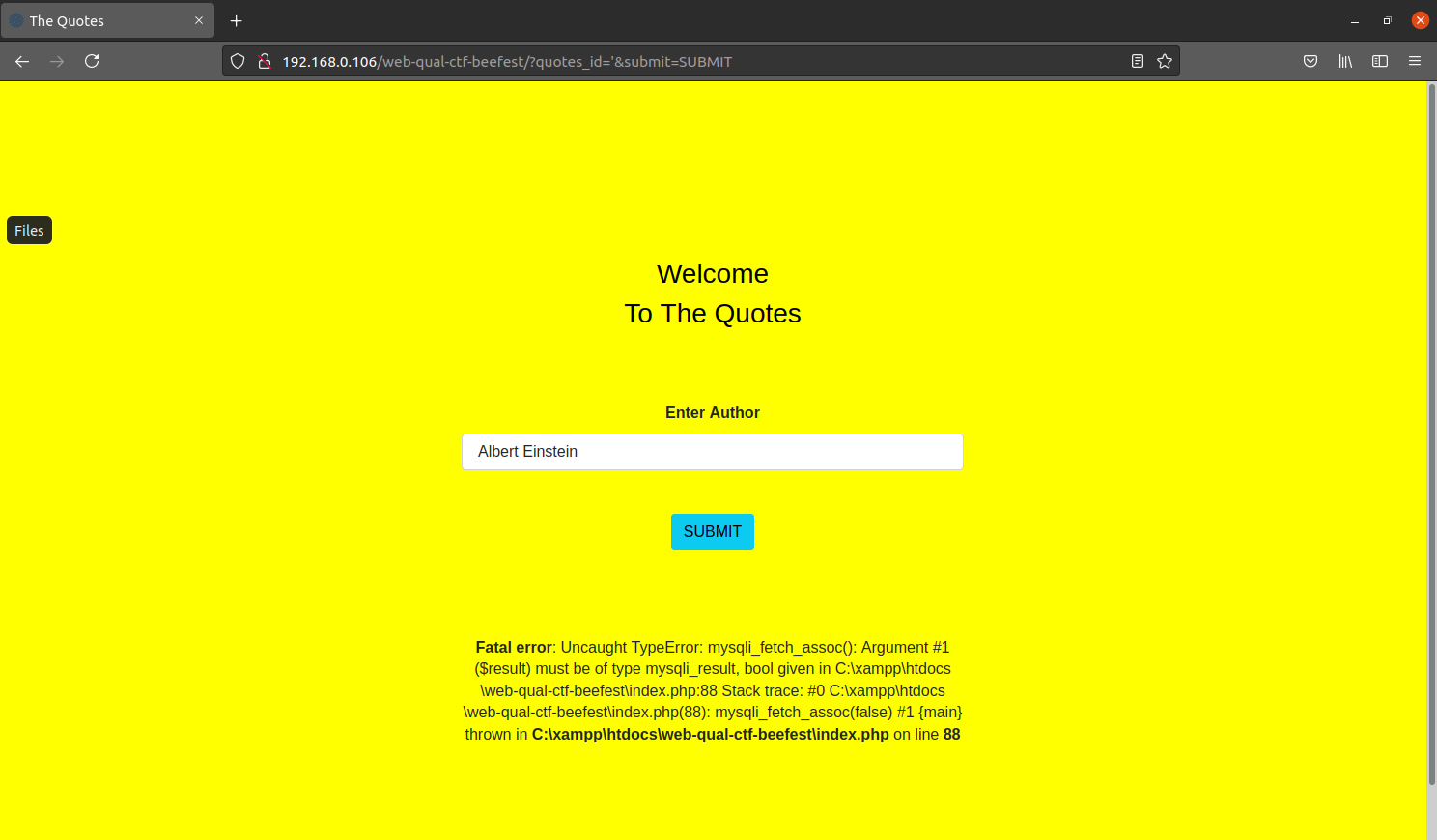
**The Quotes - Web**

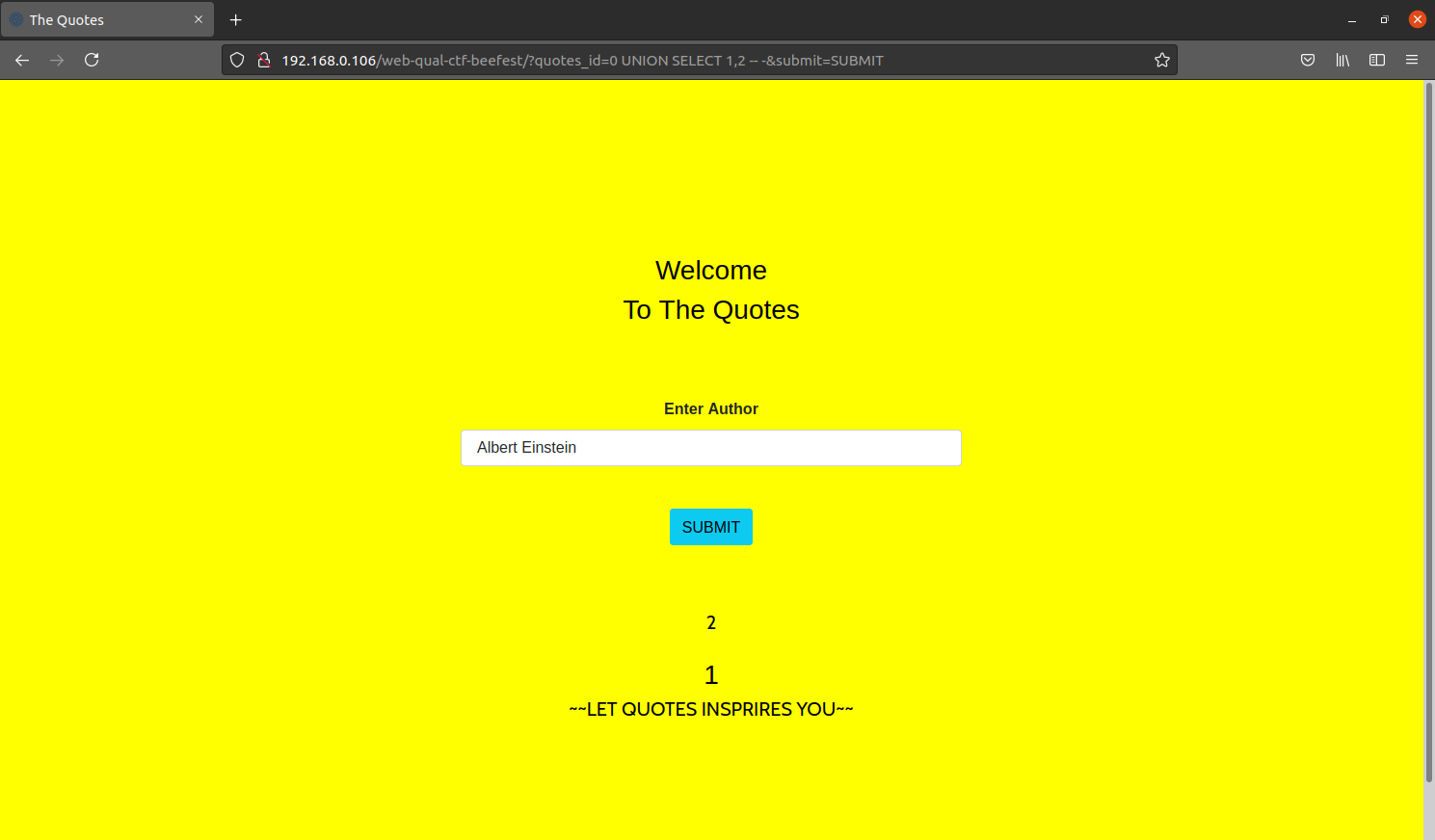
Ini merupakan soal Union-based SQL Injection biasa. Bagaimana kita dapat mengidentifikasi bahwa ini adalah soal SQL Injection? Pertama kita dapat memasukkan simbol berbahaya seperti single quotes (‘), pada parameter **quotes\_id**.



Bisa dilihat terhadap error pada website tersebut dengan error **mysqli\_fetch\_assoc()**. Ini memberikan kita sebuah clue bahwa ada koneksi menuju database pada parameter **quotes\_id**.

Dengan menggunakan payload UNION-based SQL injection biasa seperti:

**0 UNION SELECT 1,2 -- -**

****

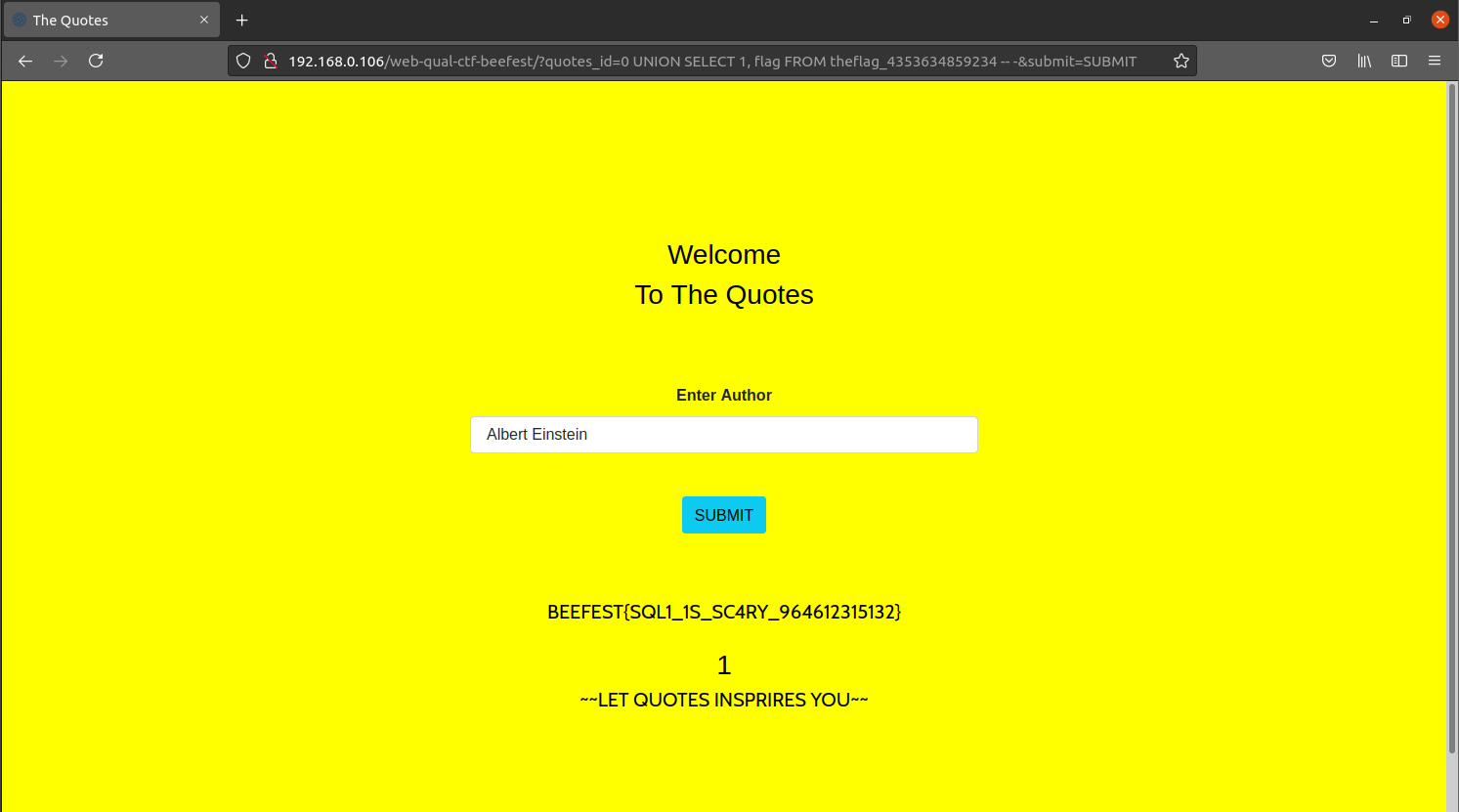
Kita dapat mengkonfirmasi bahwa ini adalah UNION-based SQL injection. Untuk mendapatkan flag kita hanya tinggal membaca nama tabel dan kolom flag di dalam database. Kita bisa melakukannya dengan payload sebagai berikut:

**0 UNION SELECT 0, group\_concat(table\_name, ‘:’, column\_name) FROM information\_schema.columns -- -**

****

Saya menggunakan ‘:’ untuk pemisah antara kolom dan tabel agar lebih mudah terbaca. Dari situ kita akan mendapatkan tabel bernama **theflag\_4353634859234** dengan kolom **flag**. Terakhir kita hanya perlu membacanya dengan command sebagai berikut:

**0 UNION SELECT 1, flag FROM theflag\_4353634859234 -- -**

****