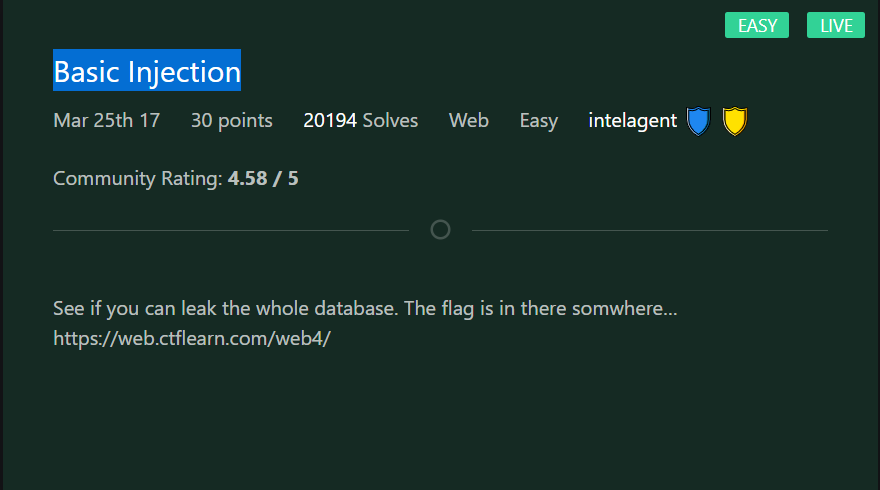
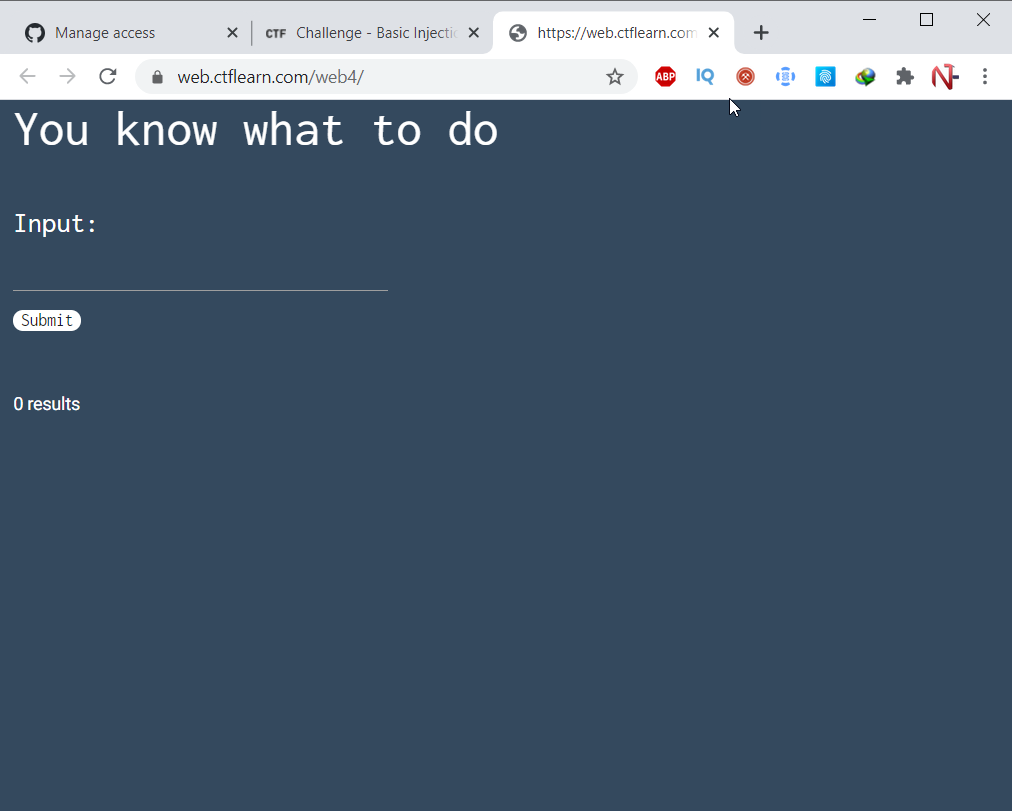
Soal

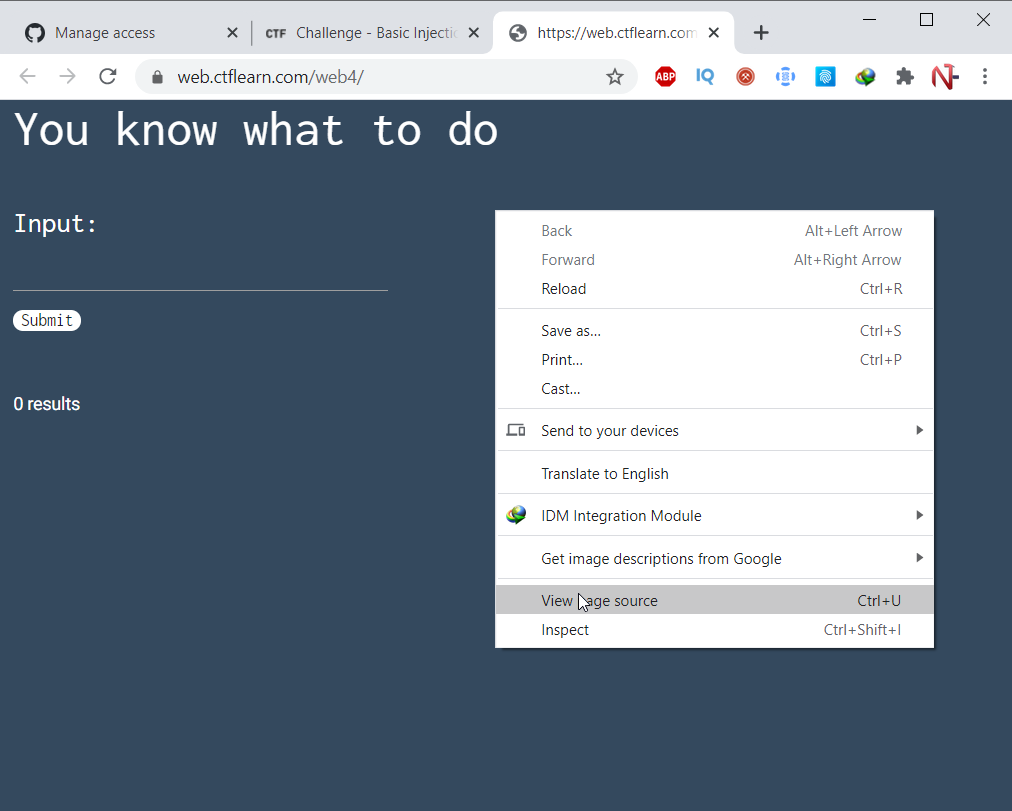


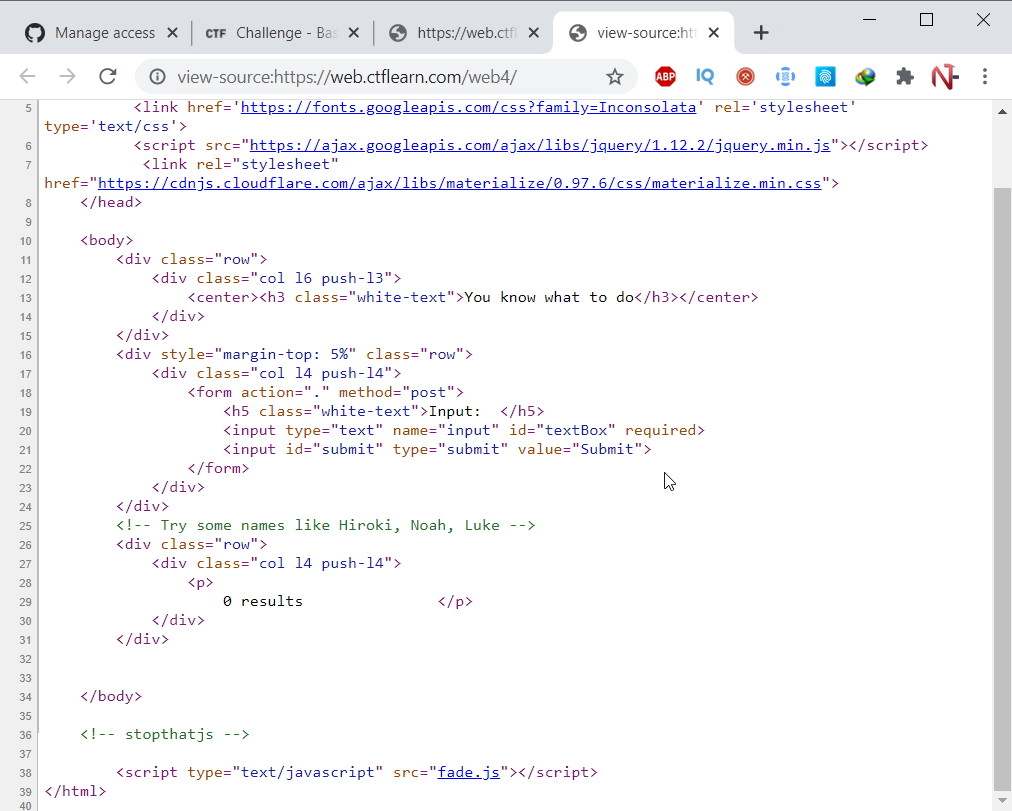
Penjelasan.

Dalam soal terdapat sebuah link ke website <https://web.ctflearn.com/web4/>. Setelah link tersebut dibuka terdapat sebuah textedit untuk memasukan nama

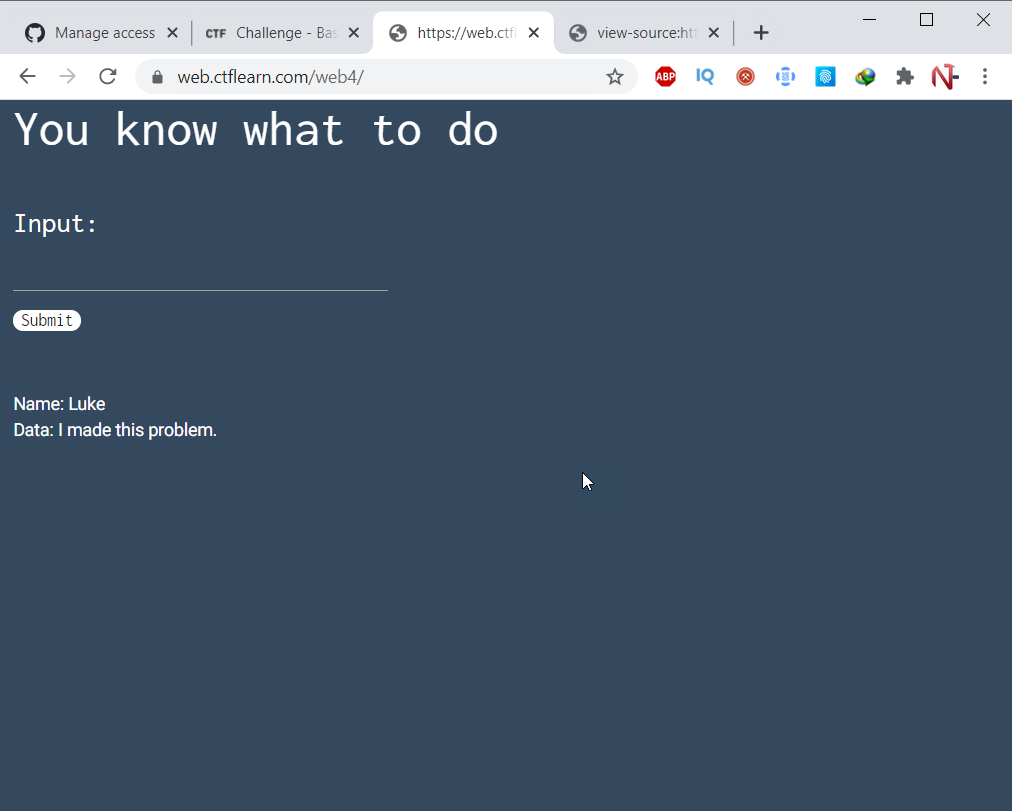


Klick kanan pada browser dan pilih View Page Source, maka akan ditampilkan kode sumber HTML dari halaman tersebut

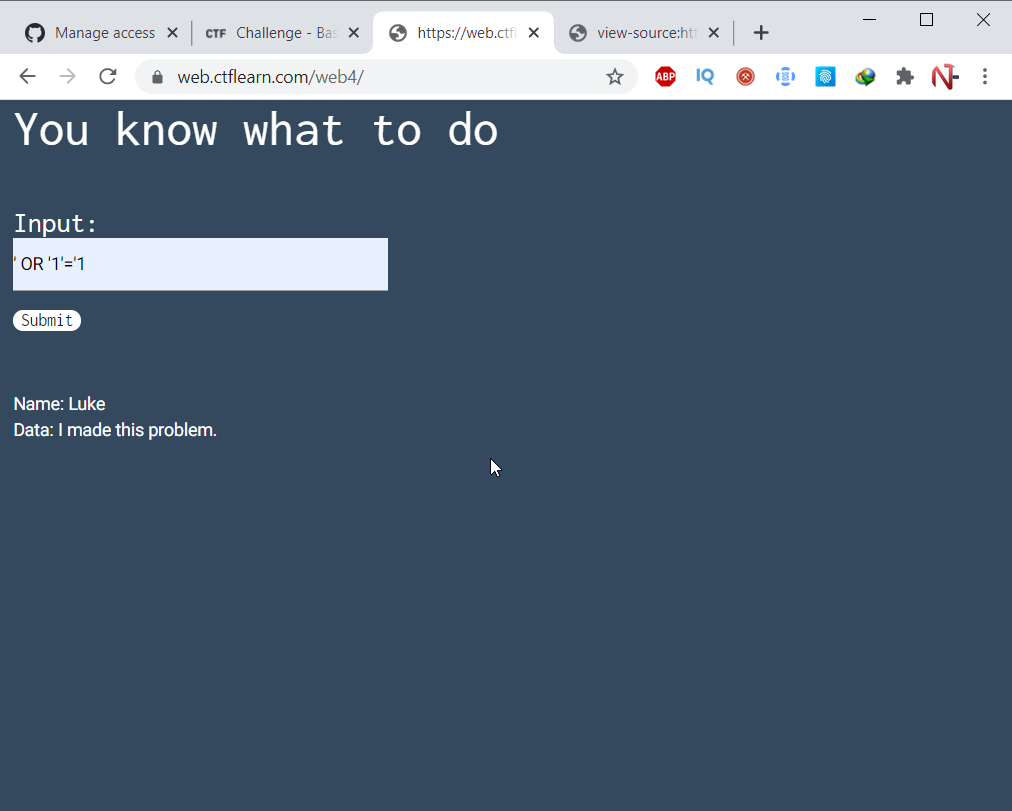




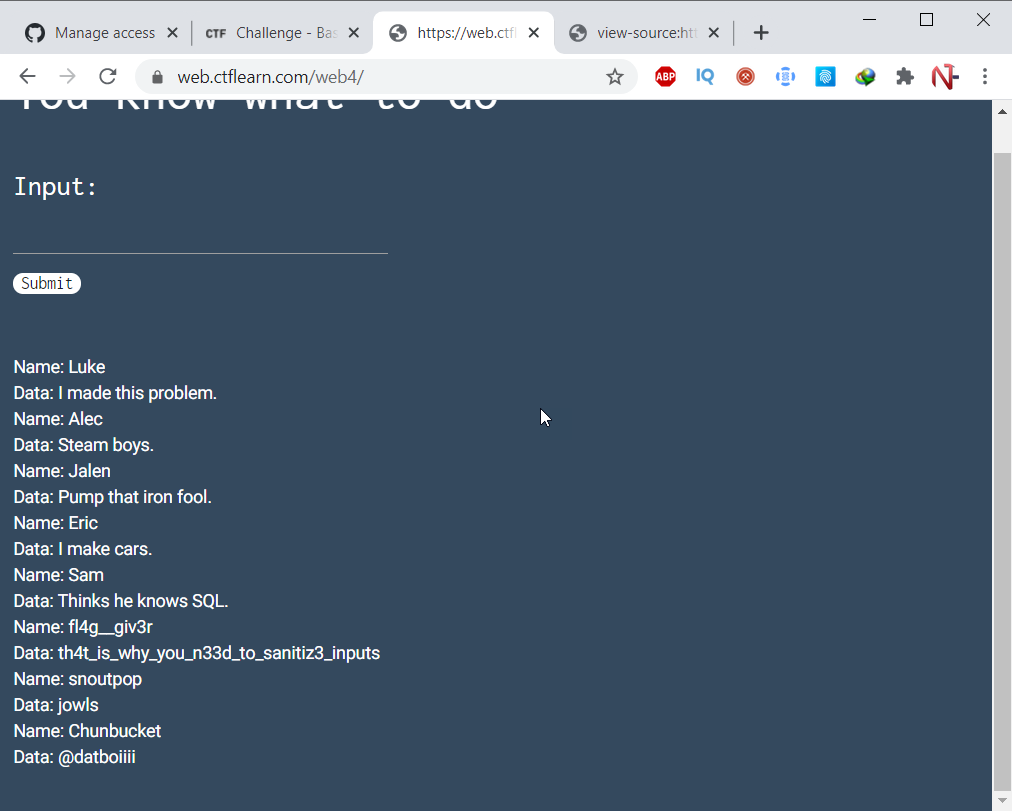
Ketika kita memasukan string Luke akan keluar data sebagai berikut



Kita berasumsi bahwa pada database akan terdapat field Nama dan Data. Dengan asumsi tersebut maka kita bisa mengira-ira sebenarnya bagaimana query di dalam aplikasi yang kemungkinan adalah **SELECT Name, Data FROM Users WHERE Name=’Luke’.** Dengan asumsi dari query pada program maka kita bisa melakukan inject query ‘ OR ‘1’=’1 yang nantinya akan terbentu sebuah query **SELECT Name, Data FROM Users WHERE Name=’Luke’ OR ‘1’=’1’**, dengan query hasil injeksi maka database akan menampilkan semua data di dalam Table Users. Maka kita akan menginput string ‘ OR ‘1’=’1 kedalam form.



Dan hasilnya adalah



Dan kita mendapatkan th4t\_is\_why\_you\_n33d\_to\_sanitiz3\_inputs sebagai flag nya