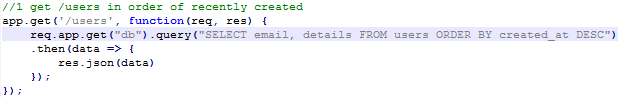
Daniel Moloney C15446648

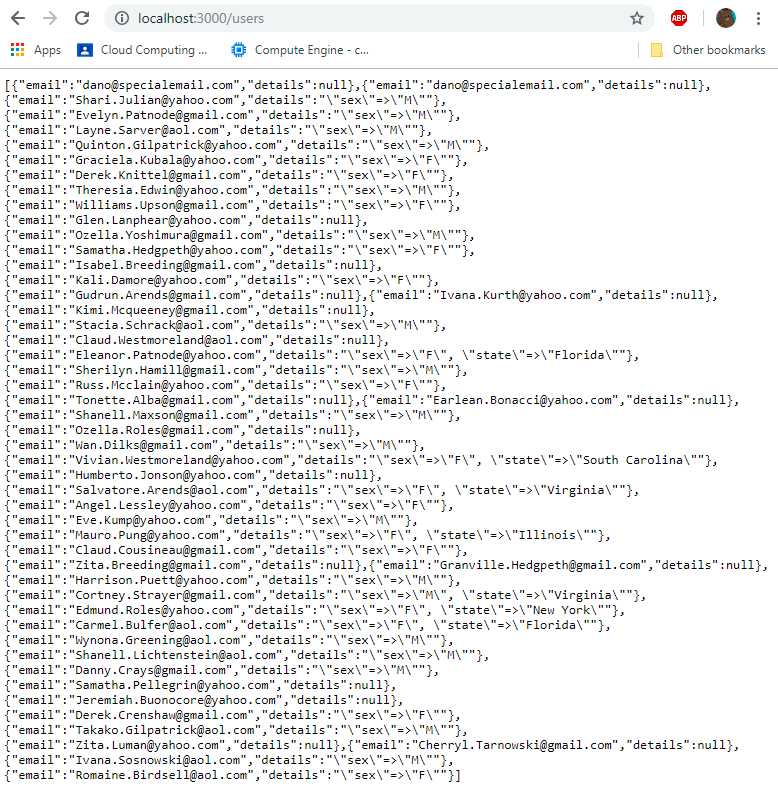
# Question 1:

1 GET /users

Code

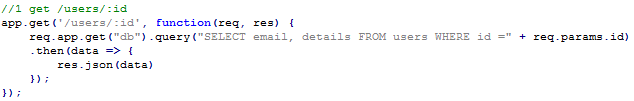


Output

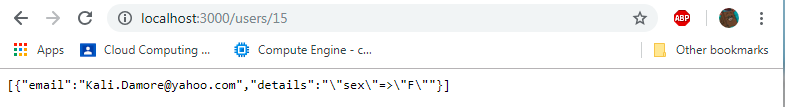


1 GET /users/:id

Code

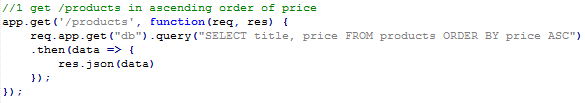


Output

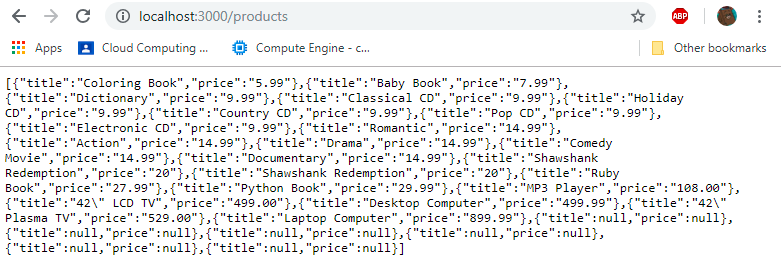


1 GET /products

Code

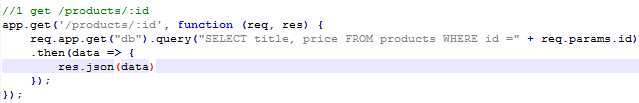


Output

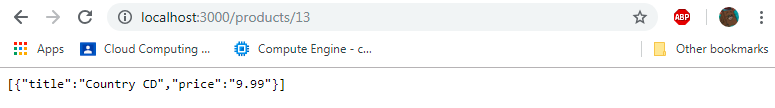


1 GET /products/:id

Code

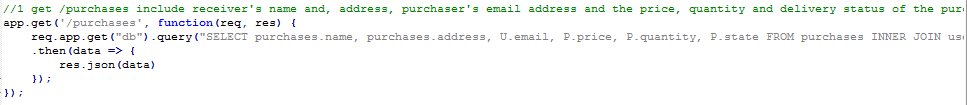


Output



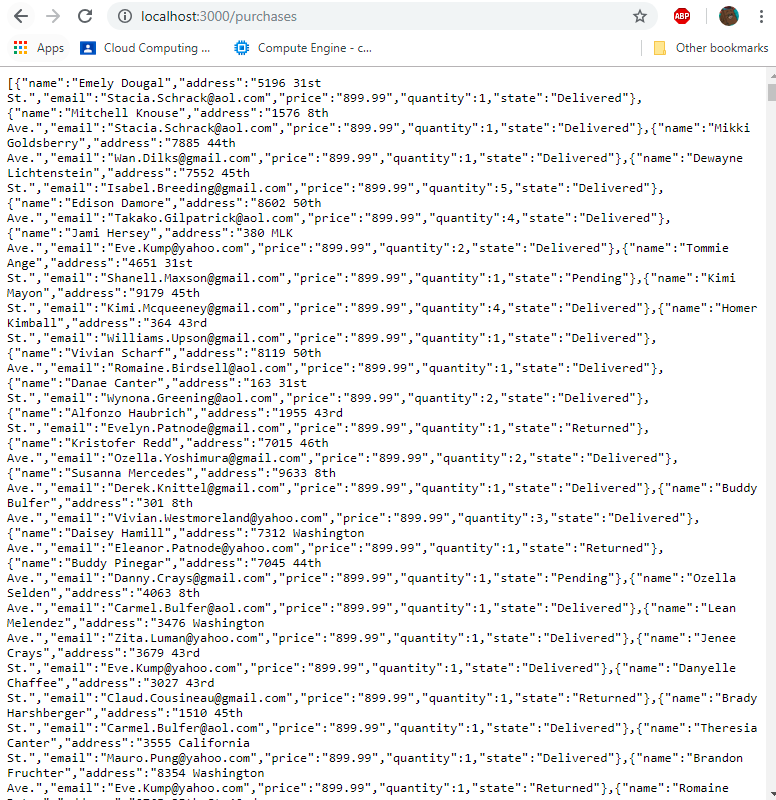
1 GET /purchases (uses joins etc)

Code





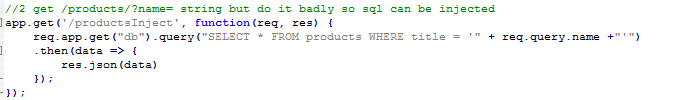
Output



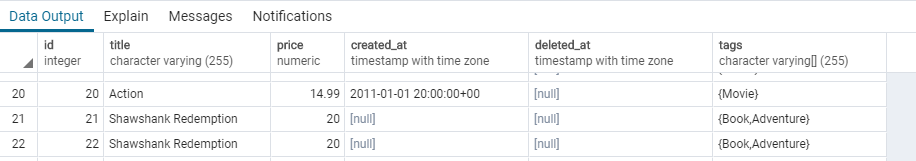
As you can see above, the output scrolls on and on (full query is loaded)

2 GET /products/?name sql injectable

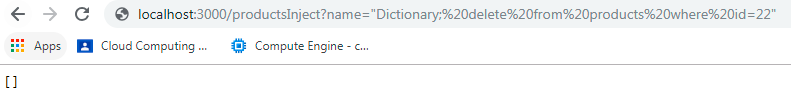
Code



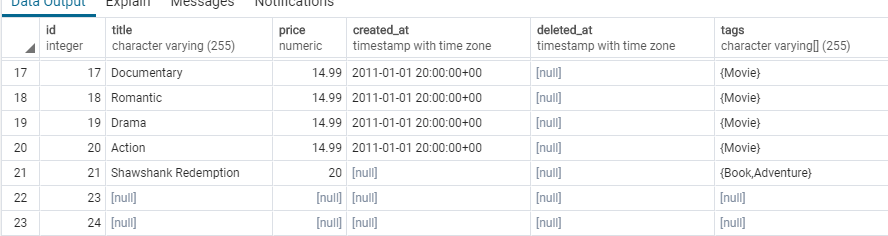
Before injection



Injection



Result of injection

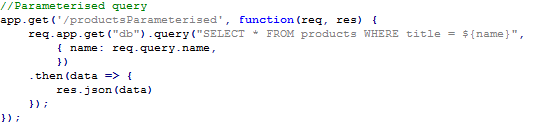


3 Solution to injections

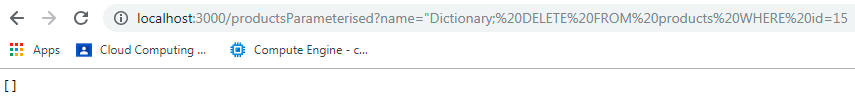
a)

parameterisation

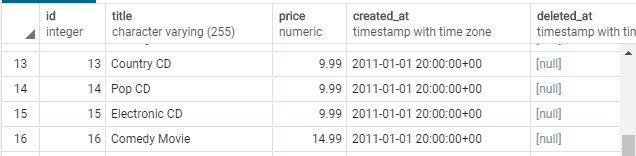
Code



Injection



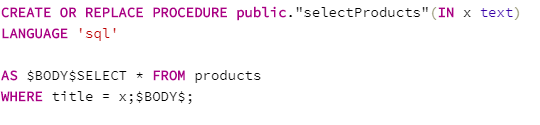
Result (no loss of product with id 15)



b)

stored procedure

Code



Similarly to parameterized approach, output showed injection failed (same id used)

