

**Enterprise**

**Application**

**Development**

**Max Macdonald**

**C15740661**

School of Computing

Technological University for Dublin

**Lab 1**

**DT228/4**

**Declaration A**

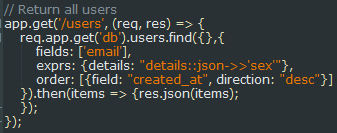
I hereby certify that this report which I now submit for assessment to the School of Computing, Dublin Institute of Technology as part of the stated module is entirely my own

work and has not been submitted for assessment for any academic purpose other than in

fulfilment for the stated above.

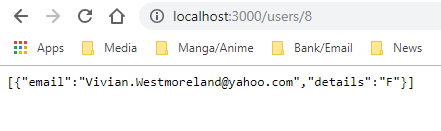
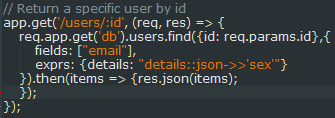
1)

GET /users

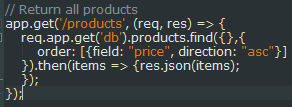


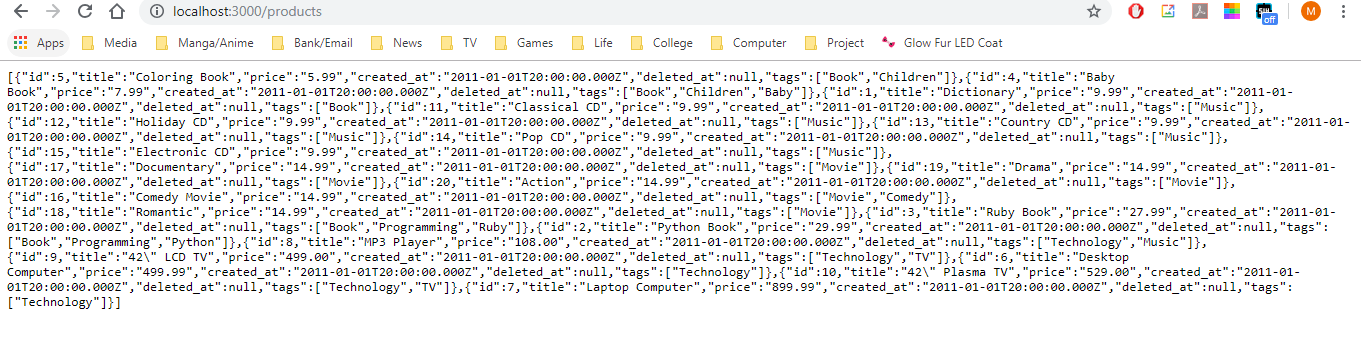


GET /users/:id

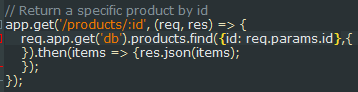


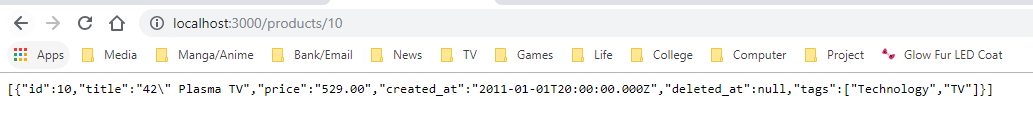
GET /products



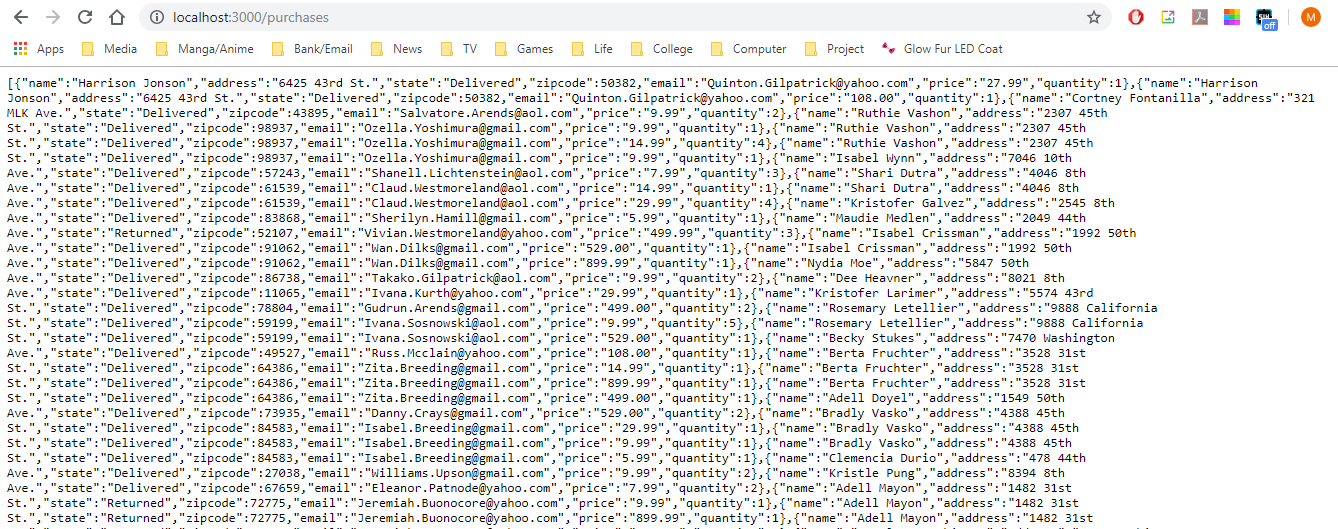
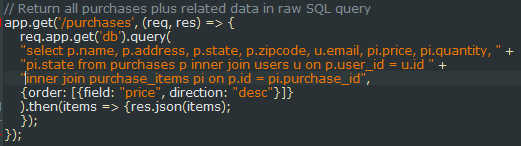


GET /products/:id



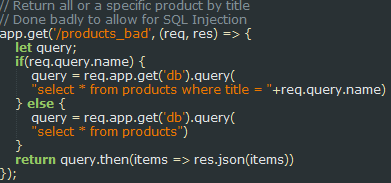


GET /purchases



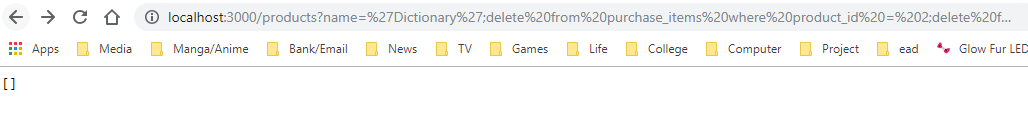
2)

GET /products[?name= *string* ] (Badly to allow SQL injection)

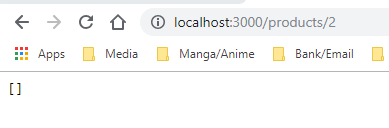


Will be susceptible to SQL injection of the form:

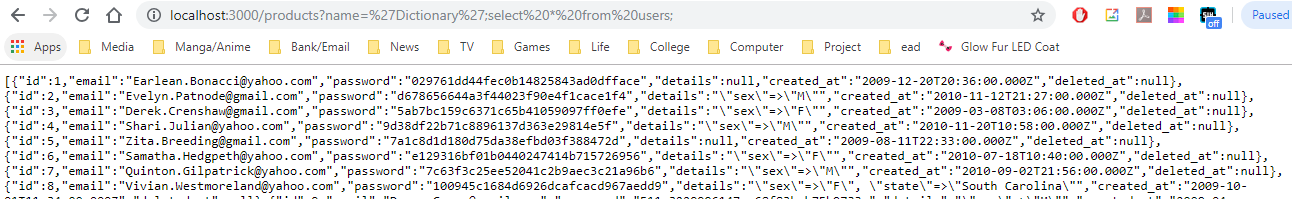
?name='Dictionary';delete from purchase\_items where product\_id = 2;delete from products where id = 2;



And then to show product with id has been deleted:

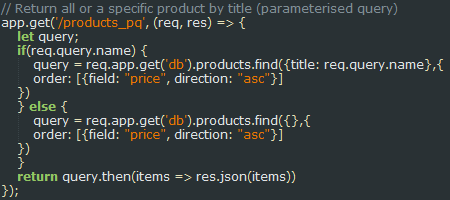


Better output to prove it works using: ?name='Dictionary';select \* from users;



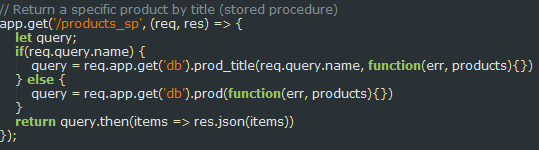
3) i)

Parameterised query:



ii)

Stored procedure using SQL:



With db/prod\_title.sql containing:

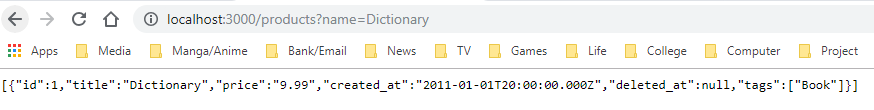


And db/prod.sql containing:

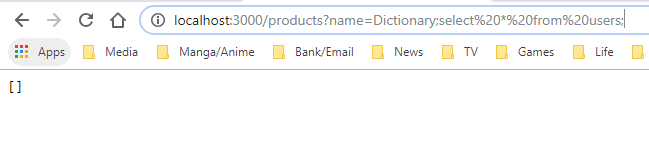


Outputs are the same for (i) & (ii)

Working:



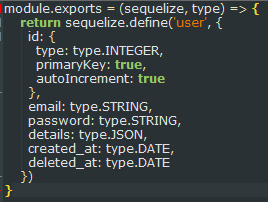
Showing immunity to SQL injection:



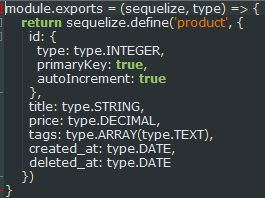
4)

Sequalize migrations for the pgguide sample database:

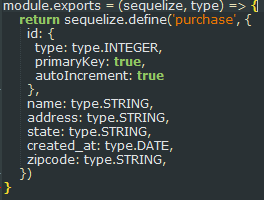
User:



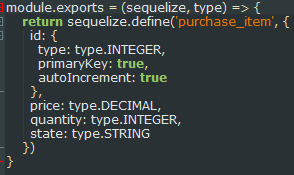
Product:



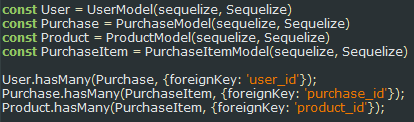
Purchase:



Purchase\_Item:



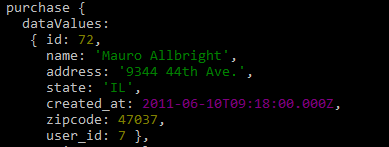
Appropriate associations and referential integrity:



Basic query to show working:

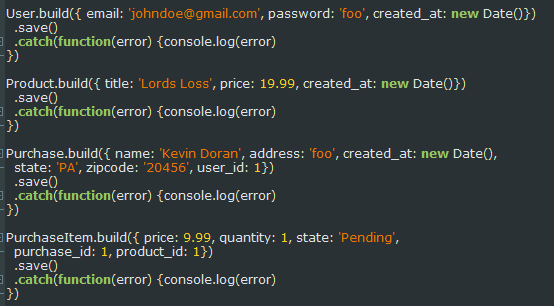


Console output example:

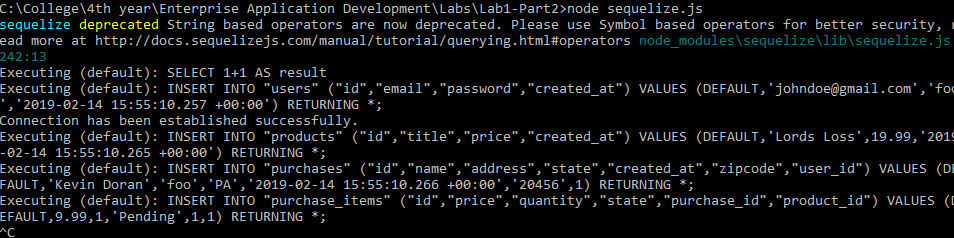


5)

Additional test data for all the models:

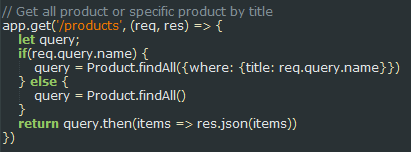


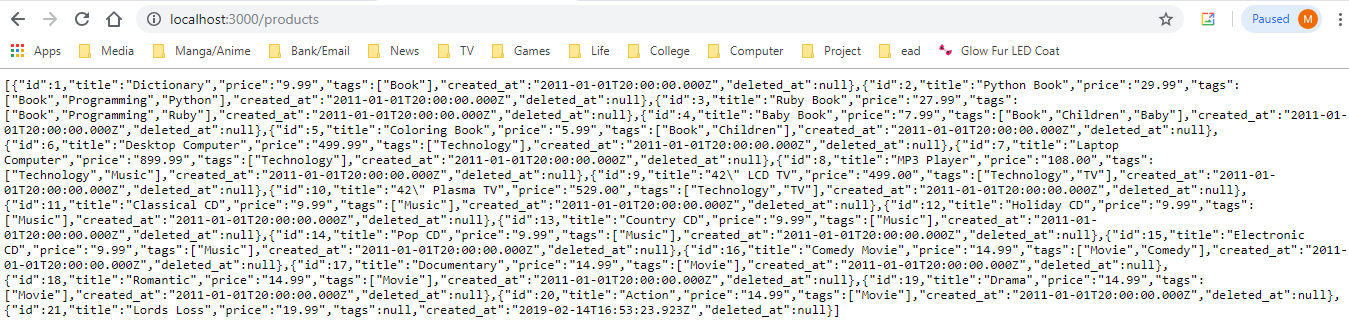
Console output:

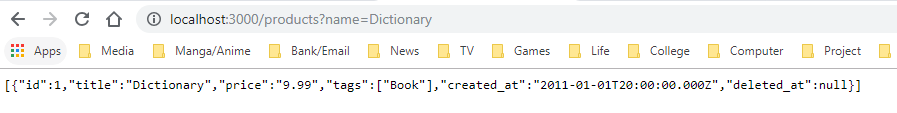


6)

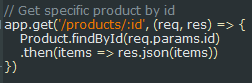
GET /products[?name=string]

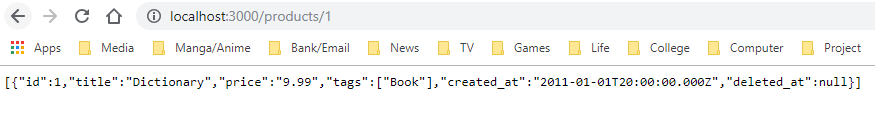




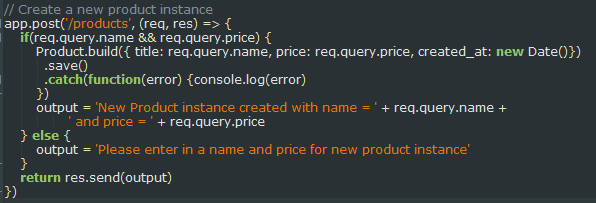


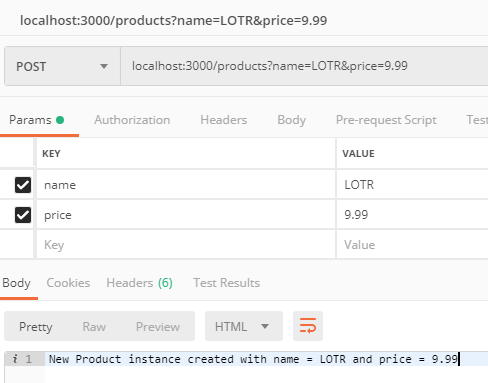
GET /products/:id



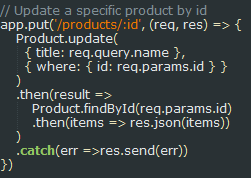


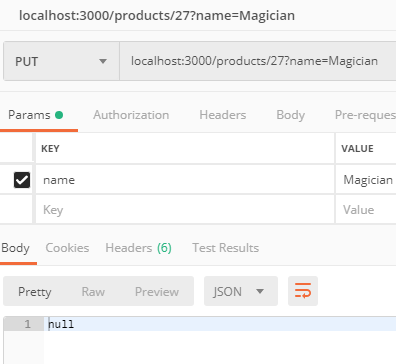
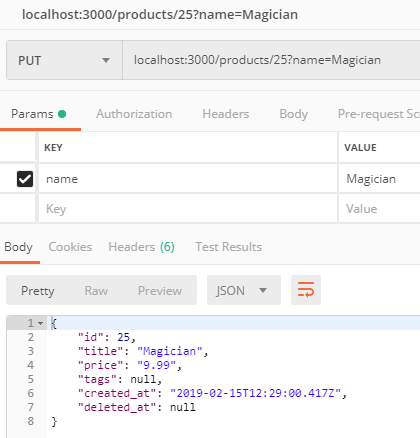
POST /products





PUT /products/:id





DELETE /products/:id

