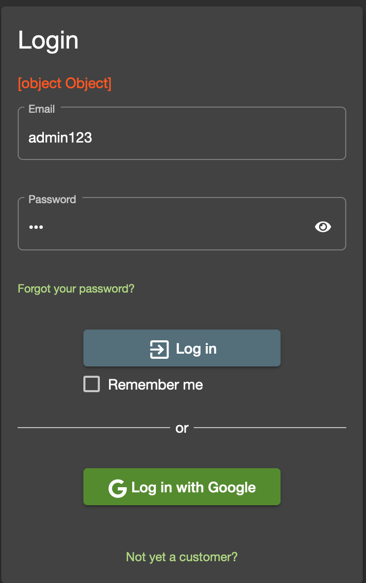
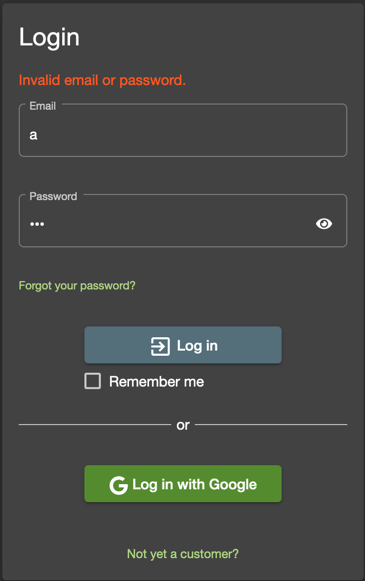
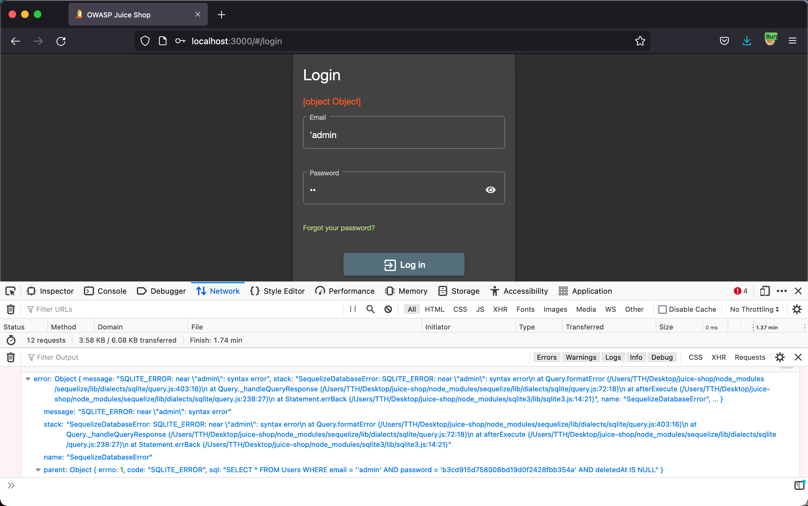
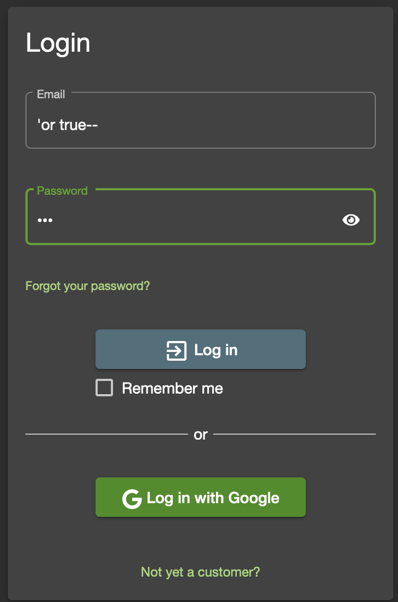
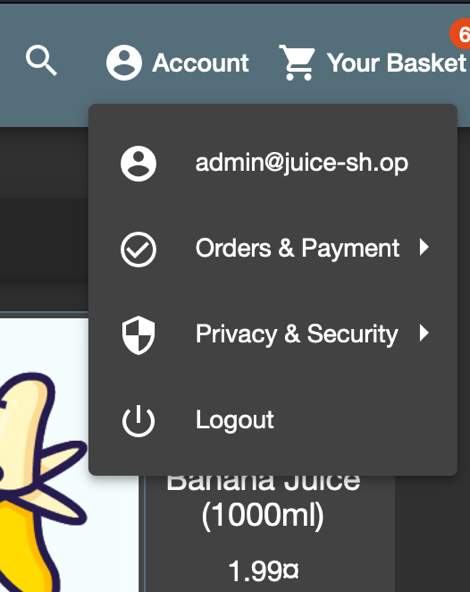
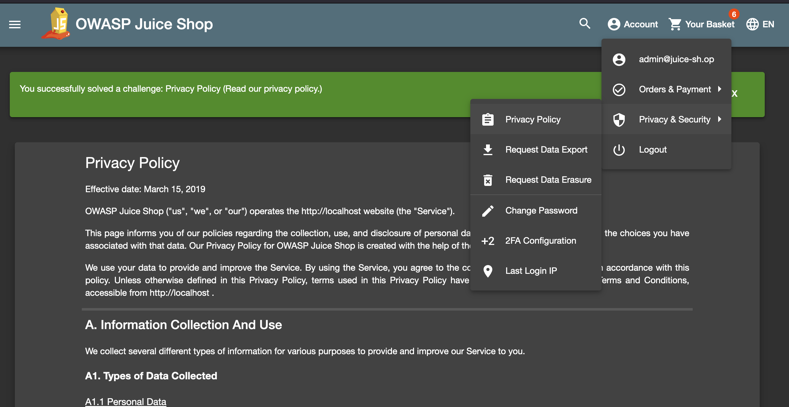
**Login Admin \*\***

Tested some random username and password trying to find out if it can be injected

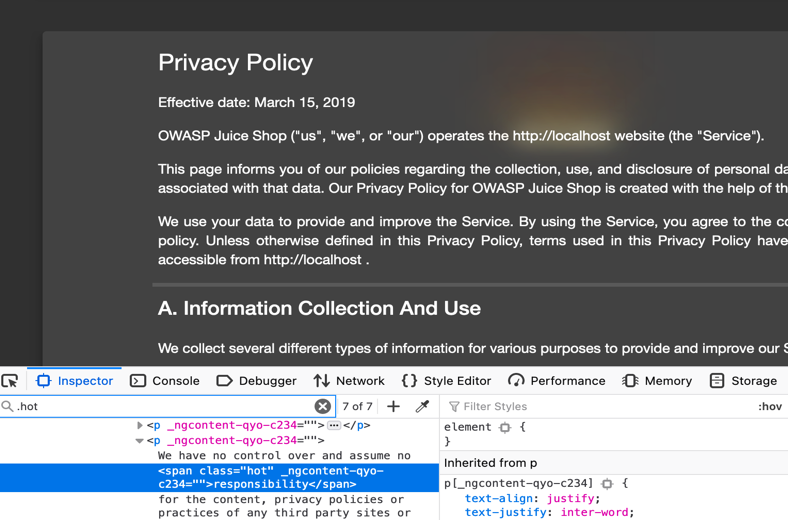
Attempted using the ‘ to close the email string, as shown there that the error prompted were in SQL format under the network tab in firefox.

Since we now know, we just inject Sql into the username and password by inserting ‘ to close the string and use SQL query “OR” to set the condition and returning the Boolean value TRUE. Lastly we can use – to omit the rest of the SQL query after setting it to TRUE.

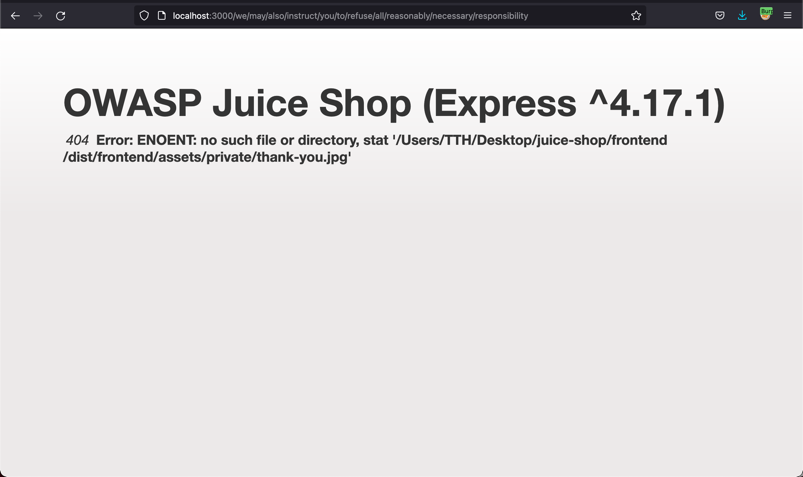
**Privacy Policy Inspection \*\*\***



Completing 1 \* Task: Privacy Policy.

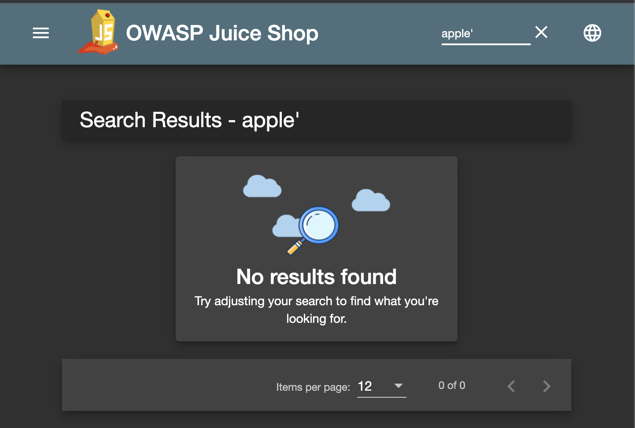


While reading the Privacy policy thinking to solve the 3 stars Privacy Policy Inspection, I came across the highlighted part where it shows http://localhost. Out of curiosity, I inspected the HTML and search for the “.hot tag and realising there are 7 keywords being highlighted.

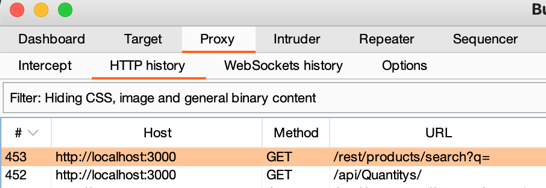
Then, proceeded to form a link using the keyword provided.

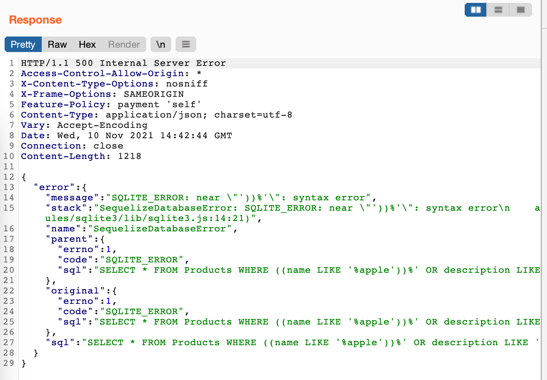
http://localhost:3000/we/may/also/ instruct /you/to/refuse/all/reasonably

/necessary/responsibility

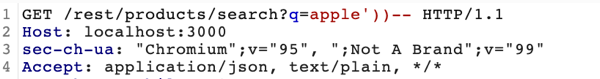
**Database Schema \*\*\* & Users credential \*\*\*\***

Firstly, head over to search bar in juice-shop and try searching for something. By using Burp Suit, under Proxy and HTTP history we can get the URL for the search query when adding a ‘ character.

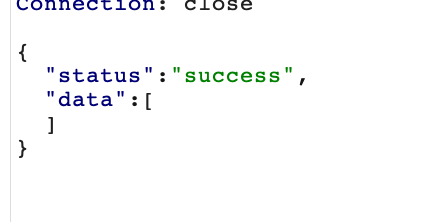
By clicking into the response tab in Burp suit, we can see that we are close to the schema.

With a little bit of Database knowledge, we can simply modify the search query using different character to achieved our desired outcome. Using the Repeater in Burp suit.  
  
By editing line 1: “/rest/products/search?q=apple’))--”

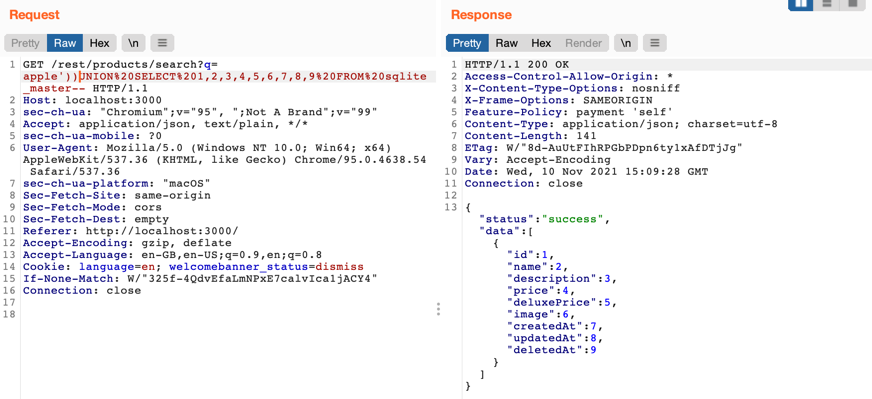
‘ testing query

)) trying to close the query

-- nullifying the rest of the of the information behind.

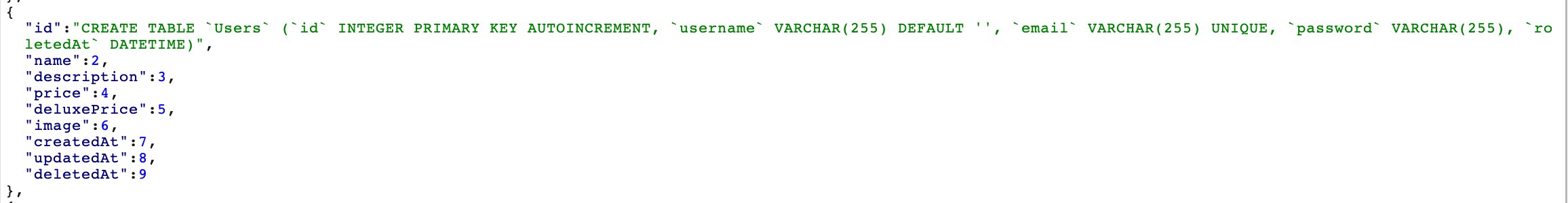


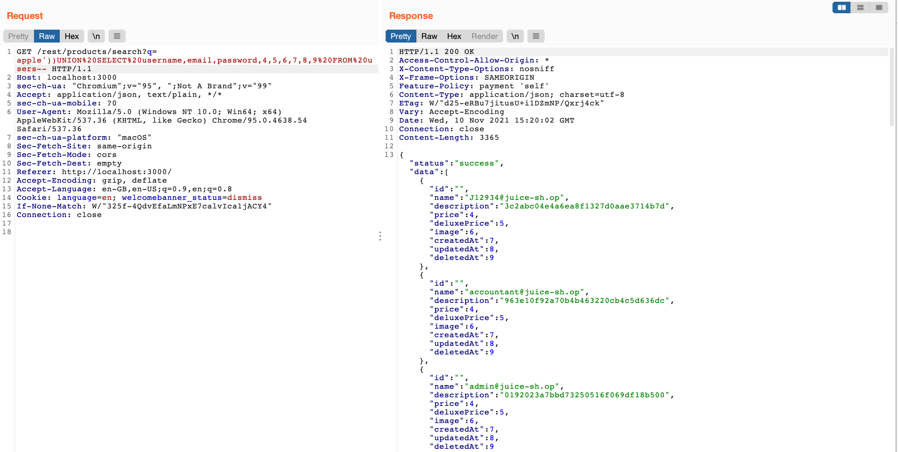
And it shows the correct status, this means that we are halfway correct.

Prior to SQL knowledge,   
UNION combines and each number representing each columns in a table.

Brute force through to figure out the number of columns.

Sqlite\_master a schema where it contains all the table in the Database schema

By changing column 1 to sql, we will be able to see the list of all the tables and access the user table, from there we can clearly spot the username, email and password..



With this we have successfully access the database and users credentials using the following query:

apple'))UNION%20SELECT%20  
username,

email,password,4,5,6,7,8,9%20  
FROM%20users--