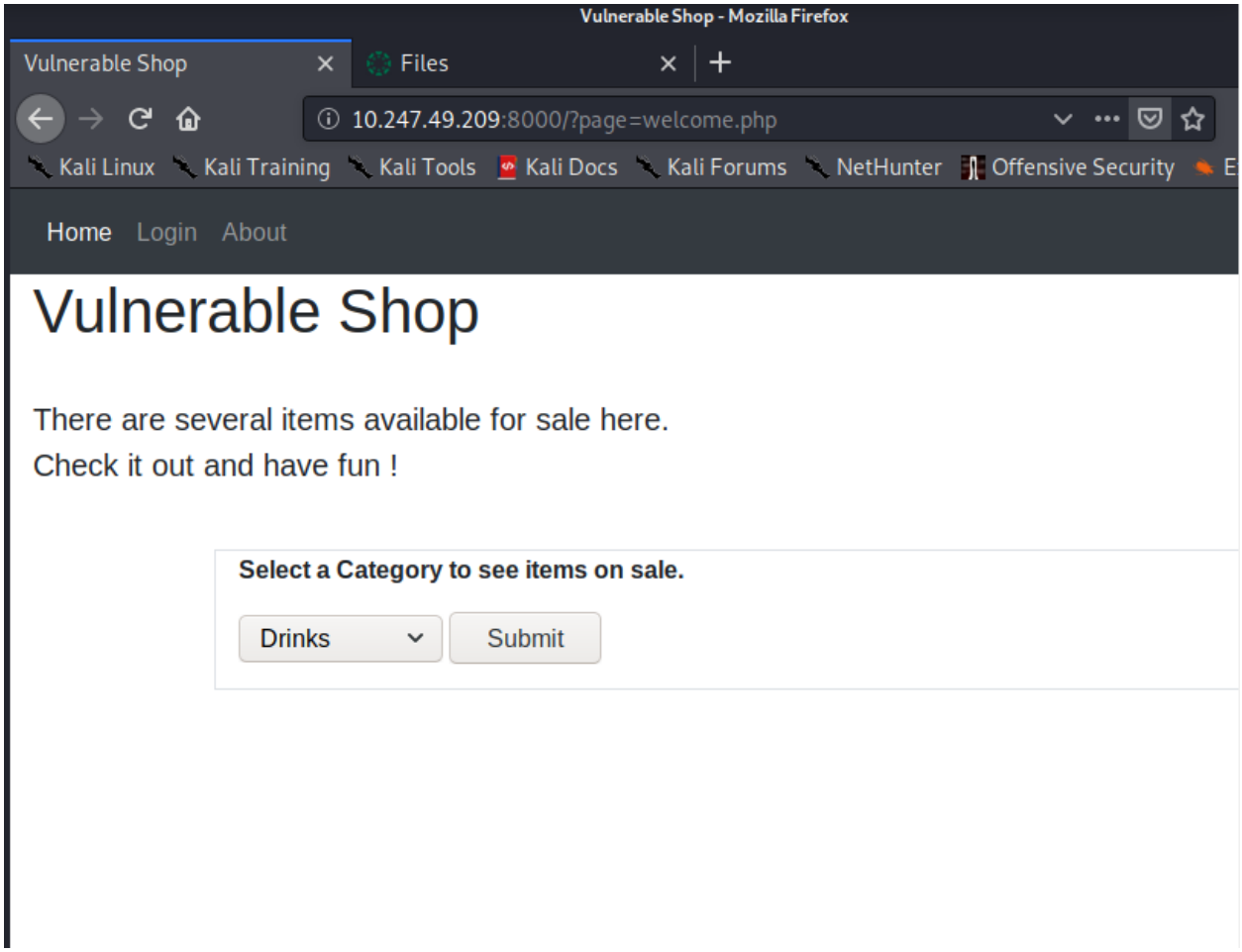
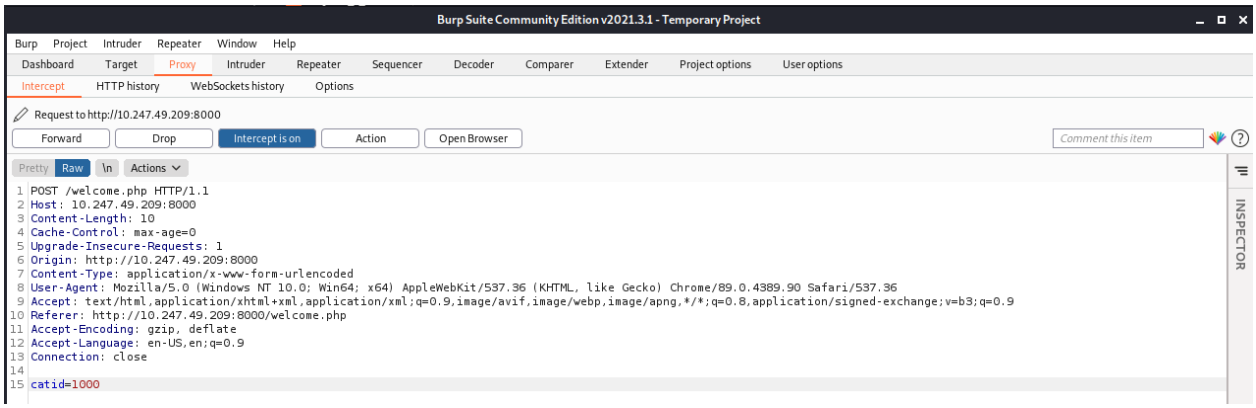
IP: 10.247.49.209:8000

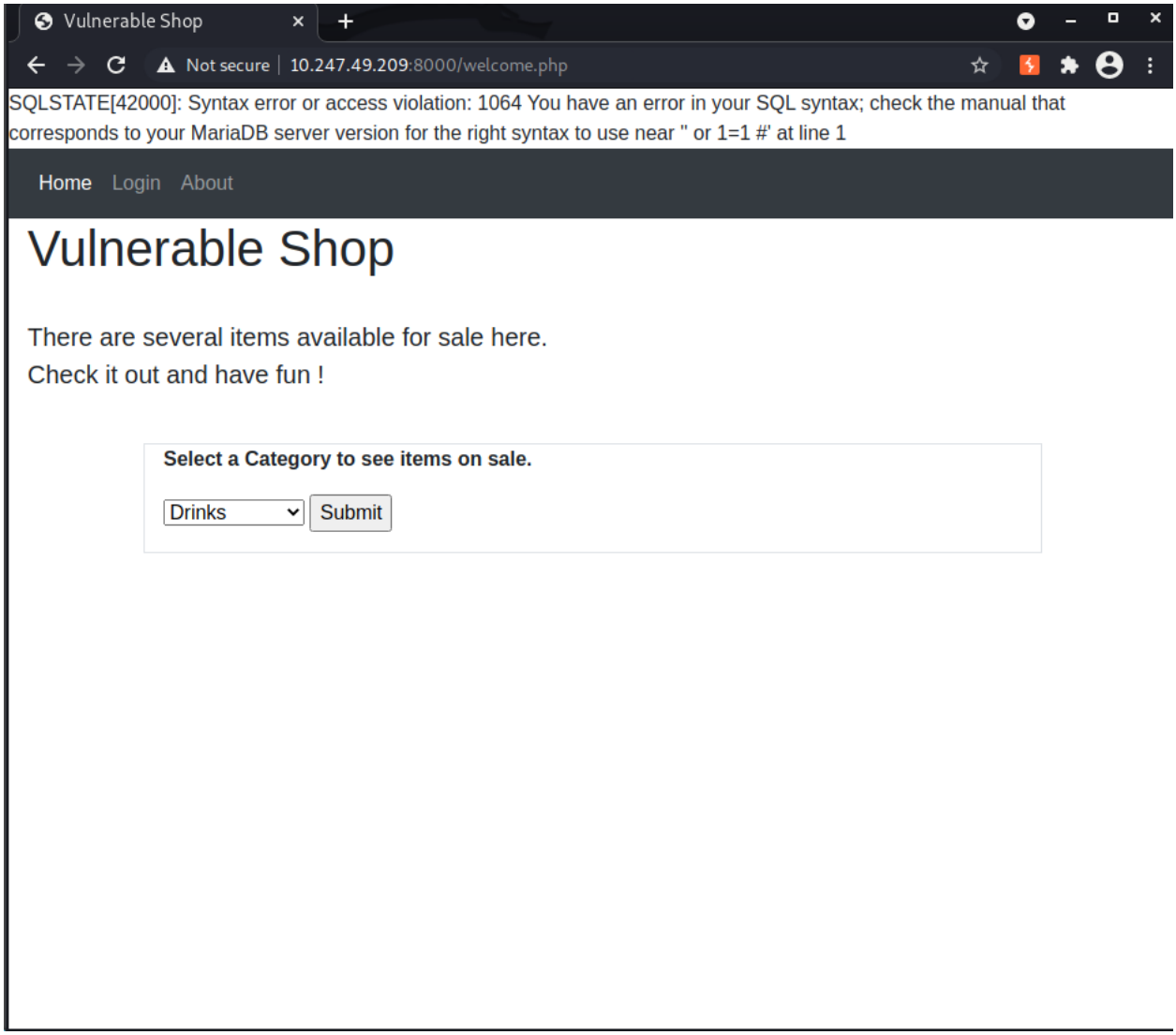
1. 

   a. After visiting the IP address given, the first thing I attempted was adding “**?page=”** to see what would happen and noticed that the webpage just went to the home page meaning it was ignoring anything I entered.

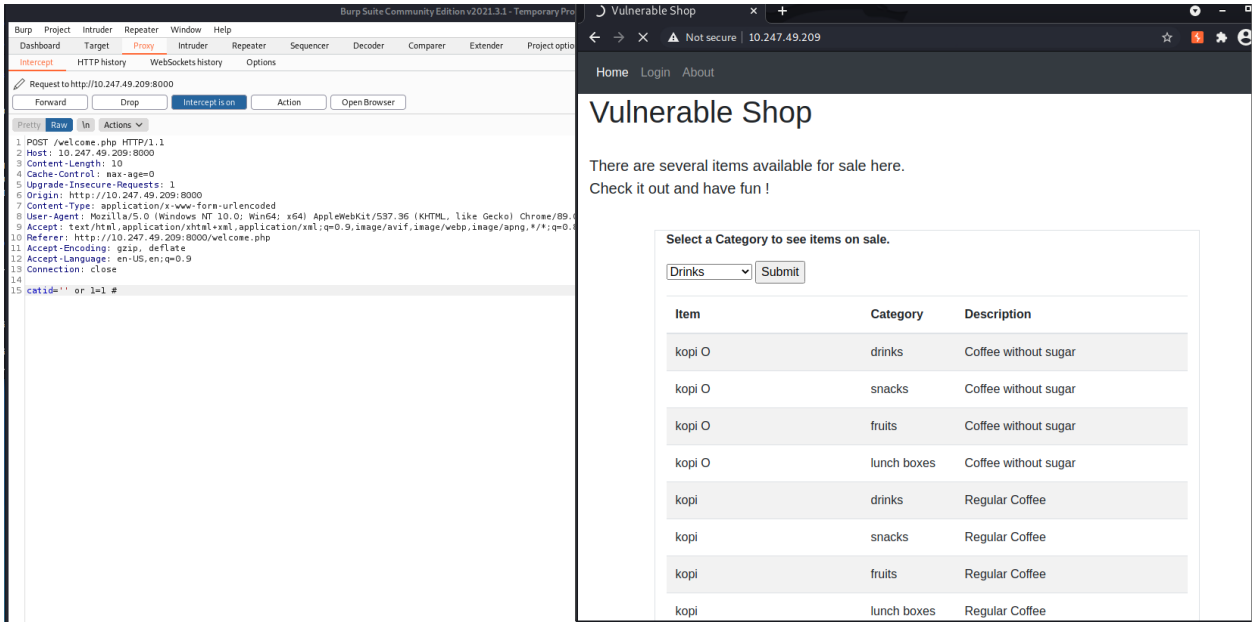
2. 

   a. After being unsuccessful with my first attempt, I then decided to run the IP given in burpsuite to get a better idea of what was happening when I hit “submit” on the welcome page. In doing so, I noticed there was a place to

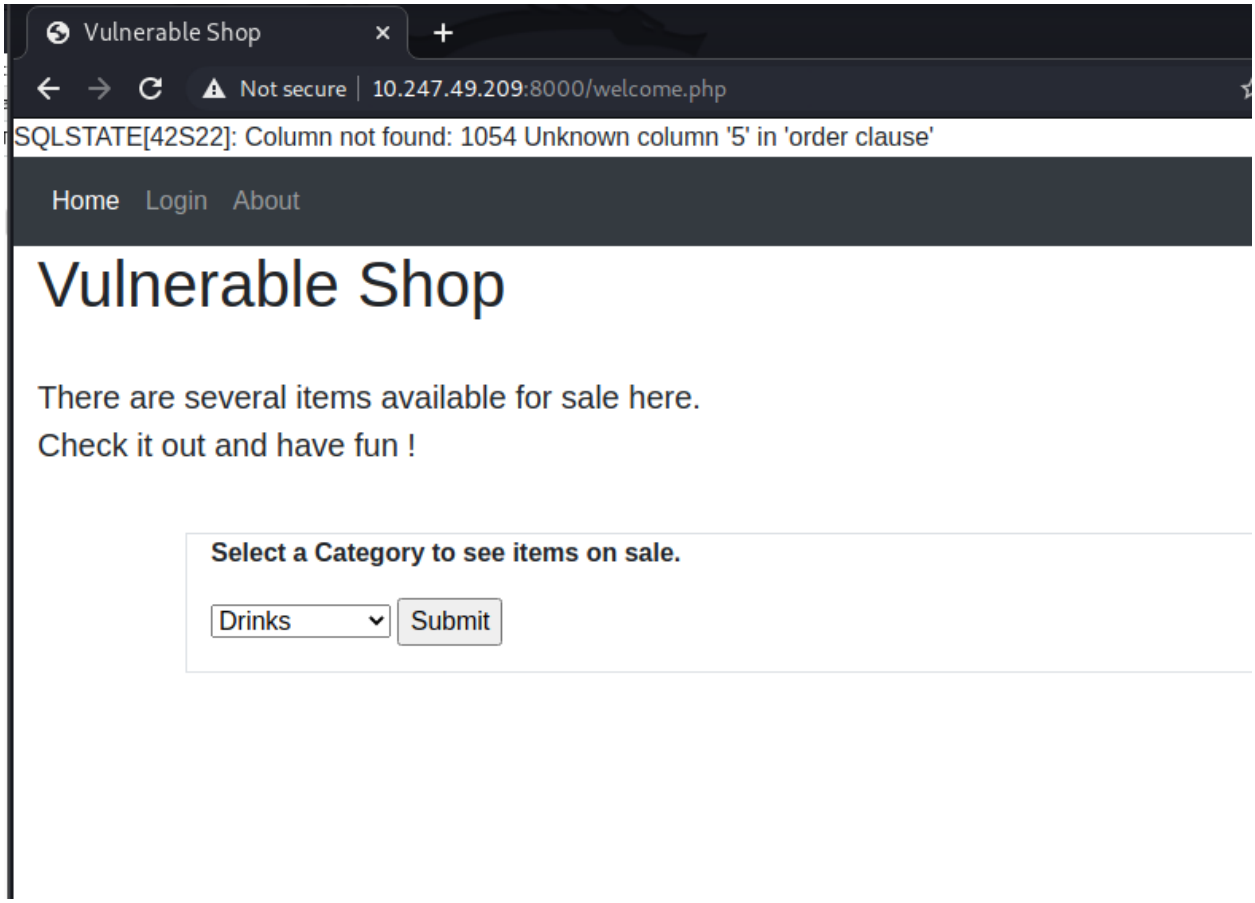
change the input based on the catid, which is originally at 1000. Originally I tried altering the input to: **‘ or 1=1#** and got the following

3. 

   a. This error message showed me that I was on the right path. I noticed that the ‘ was missing from the error message which made me think maybe it was being filtered out some way. On my next attempt I tried: **‘’ or 1=1#** received no error message and got the following screen

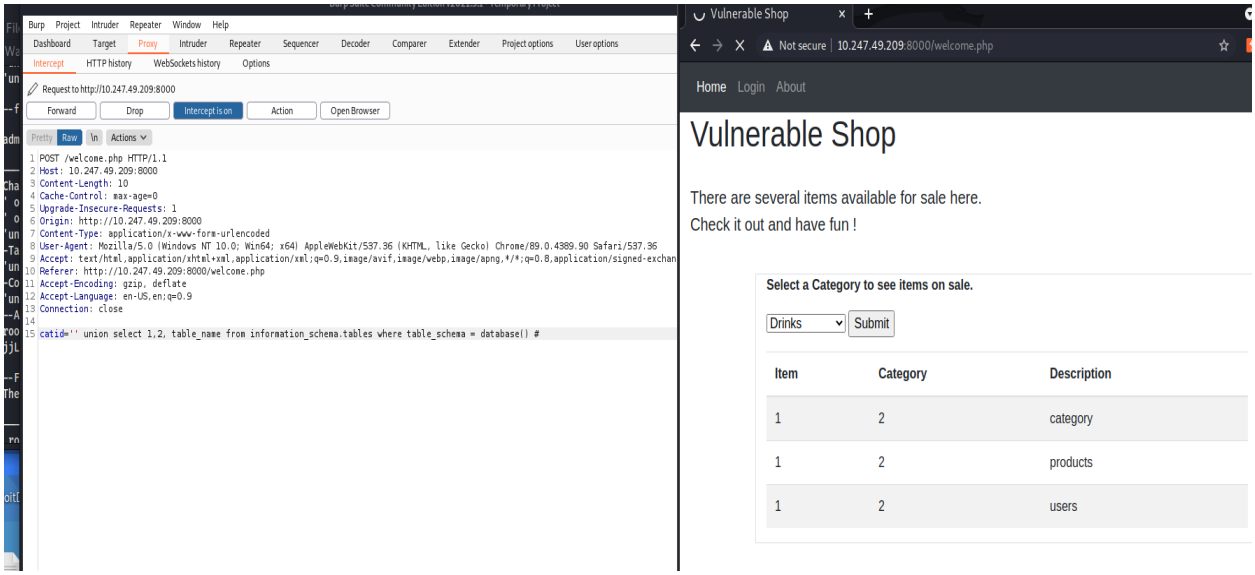
4. 

   a. Now I can begin to search the database for the flag. My next step was to find the number of columns by entering the following: **'' order by 1#**

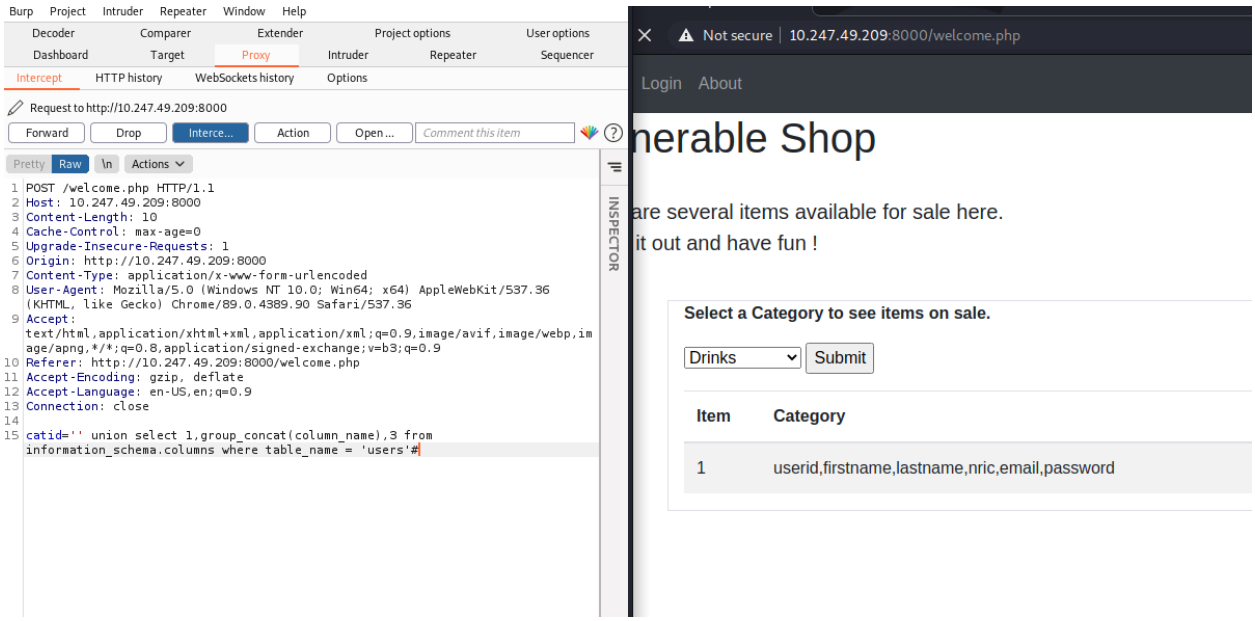
5. 

   a. Seeing that “Unknown column ‘5’ in ‘order clause’ error showed that I still had guessed too many columns. I was then able to determine that there

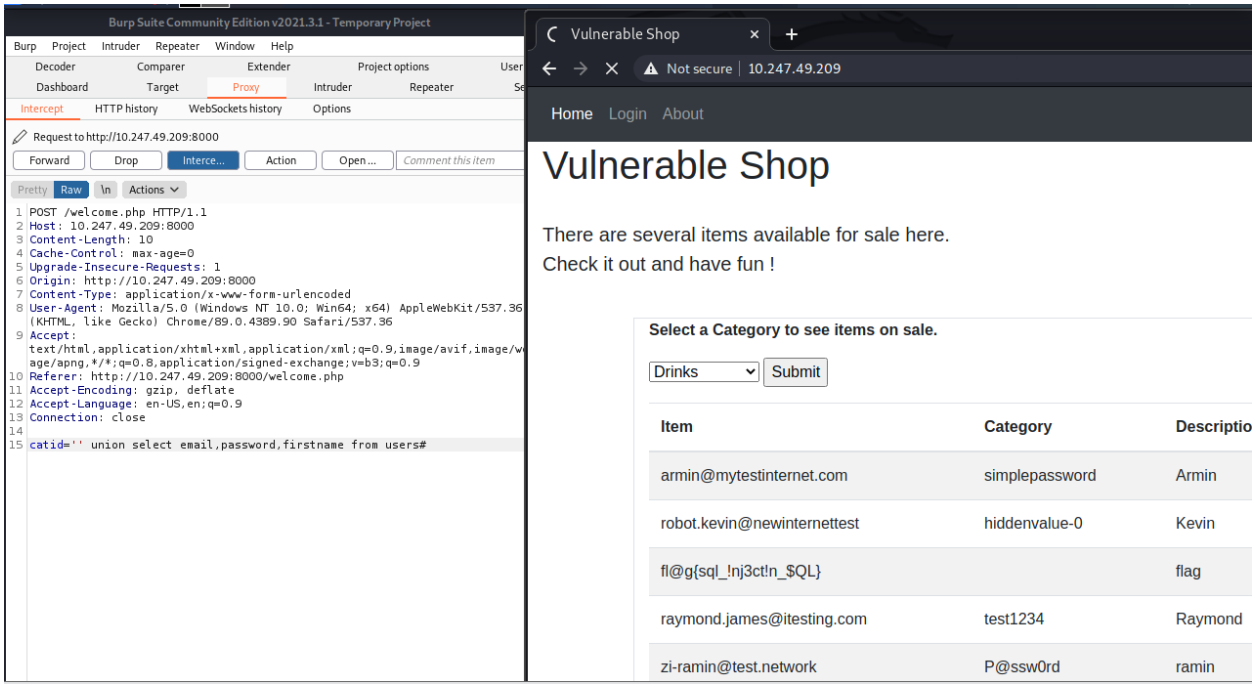
were 3 columns after more trial and error. The next step was to determine the names of tables.

6. 

   a. I then entered: **'' union select 1,2, table_name from information_schema.tables where table_schema = database() #** and was able to obtain the table names so that I can search them for more information.

7. 

   a. I then entered: **'' union select 1,group_concat(column_name),3 from information_schema.columns where table_name = 'users'#** because I wanted to search the table “users” and see what columns were in it. Upon doing so, I saw columns userid,firstname,lastname,nric,email,password and decided I would look into these first.

8. 

   a. Using the discovered names, I then made a SQL query to read the data: **'' union select email,password,firstname from users#** and from this I was able to determine the flag: fl@g{sql_!nj3ct!n_$QL}