SDEV 300 6381 Building Secure Web Applications (2178)

JOHN DELANEY

FALL 2017

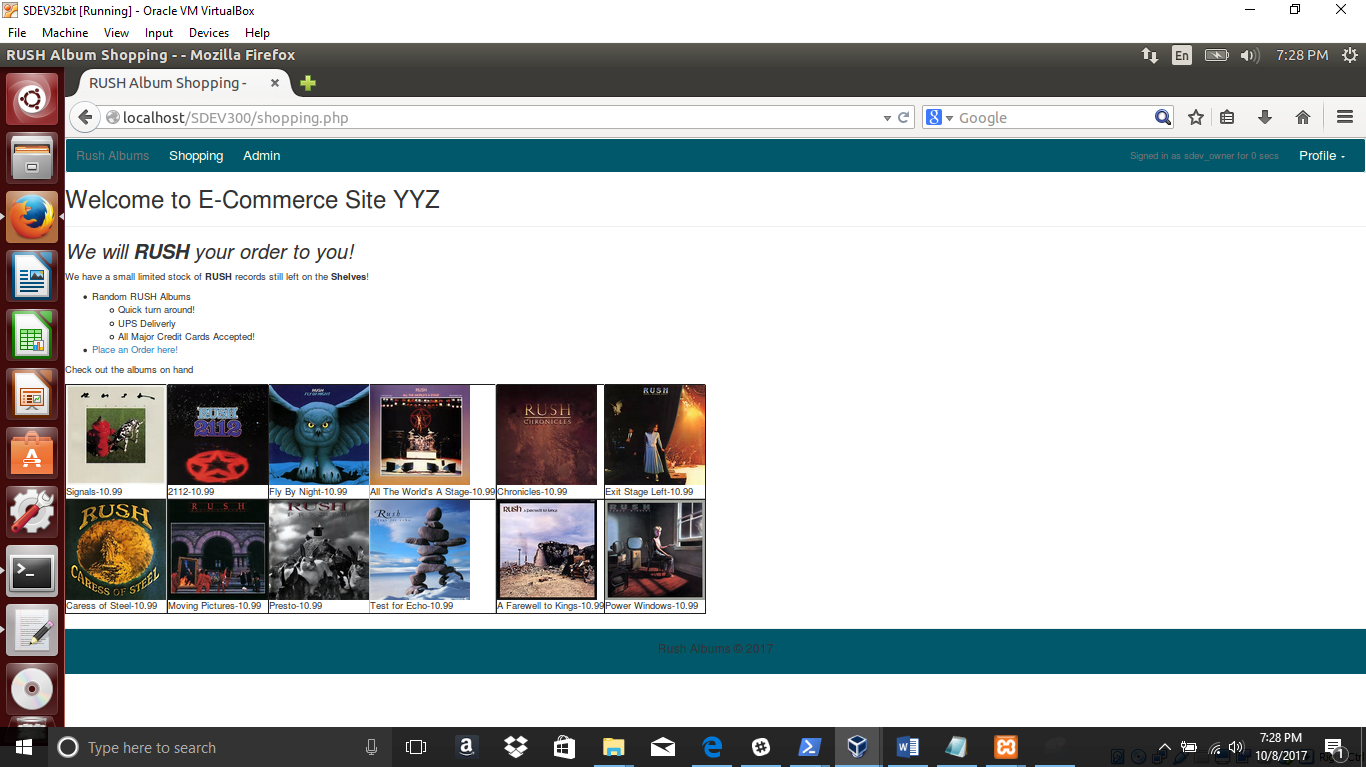
10/08/2017

**Description**

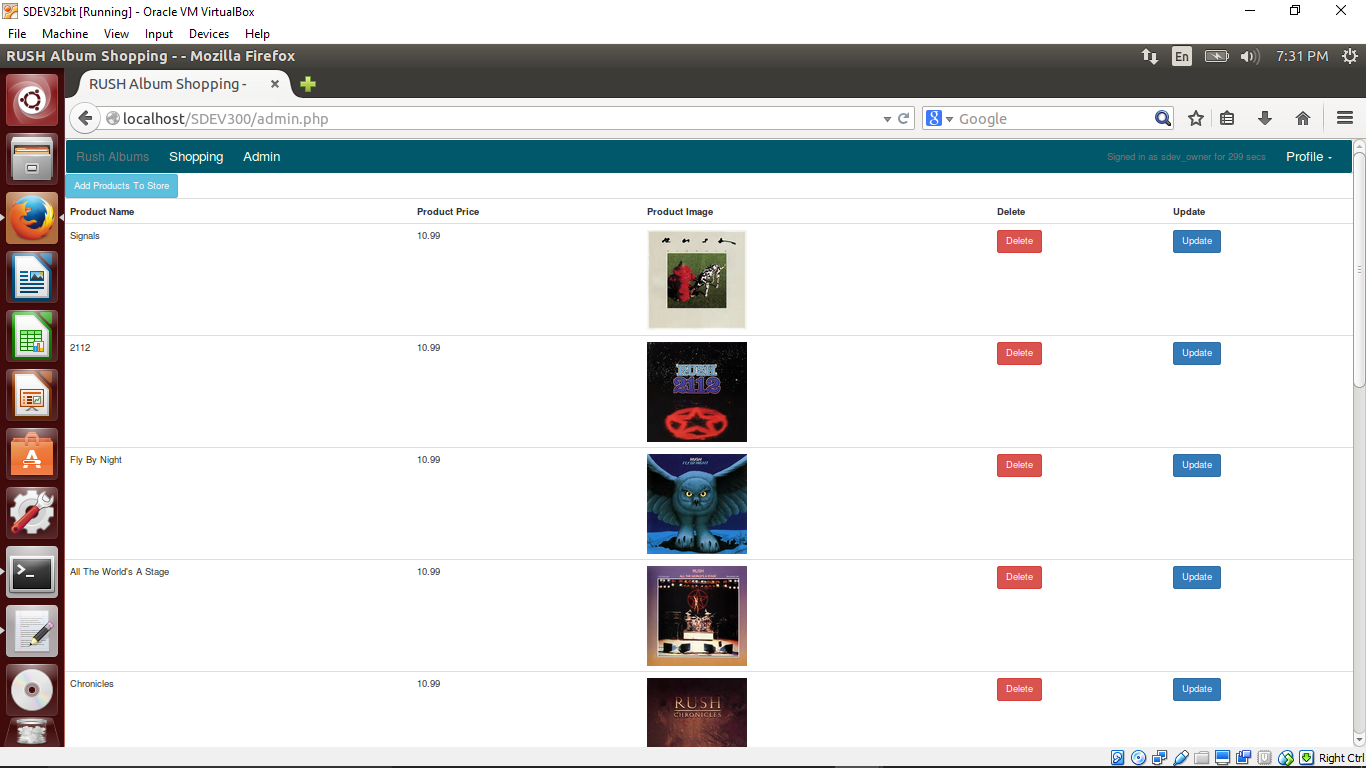
The follow lab was to build an e-Commerce site and have the ability to add, update, delete and view the items in the store as an owner. Additionally, the site had to store user data as the purchases were made. There is no real password for this application since I wanted there to be ease of use during the grading. The username is important to get the two experiences for the lab. The username: sdev\_owner is the admin for the site and can perform the adding, deleting and updating for the store. Any other username can be used to purchase from the store. I built the database to store additional information than required and used for the lab for future uses and design. The lab extends the lab for making an e-Commerce site and will build on that foundation.

**Screenshots:**

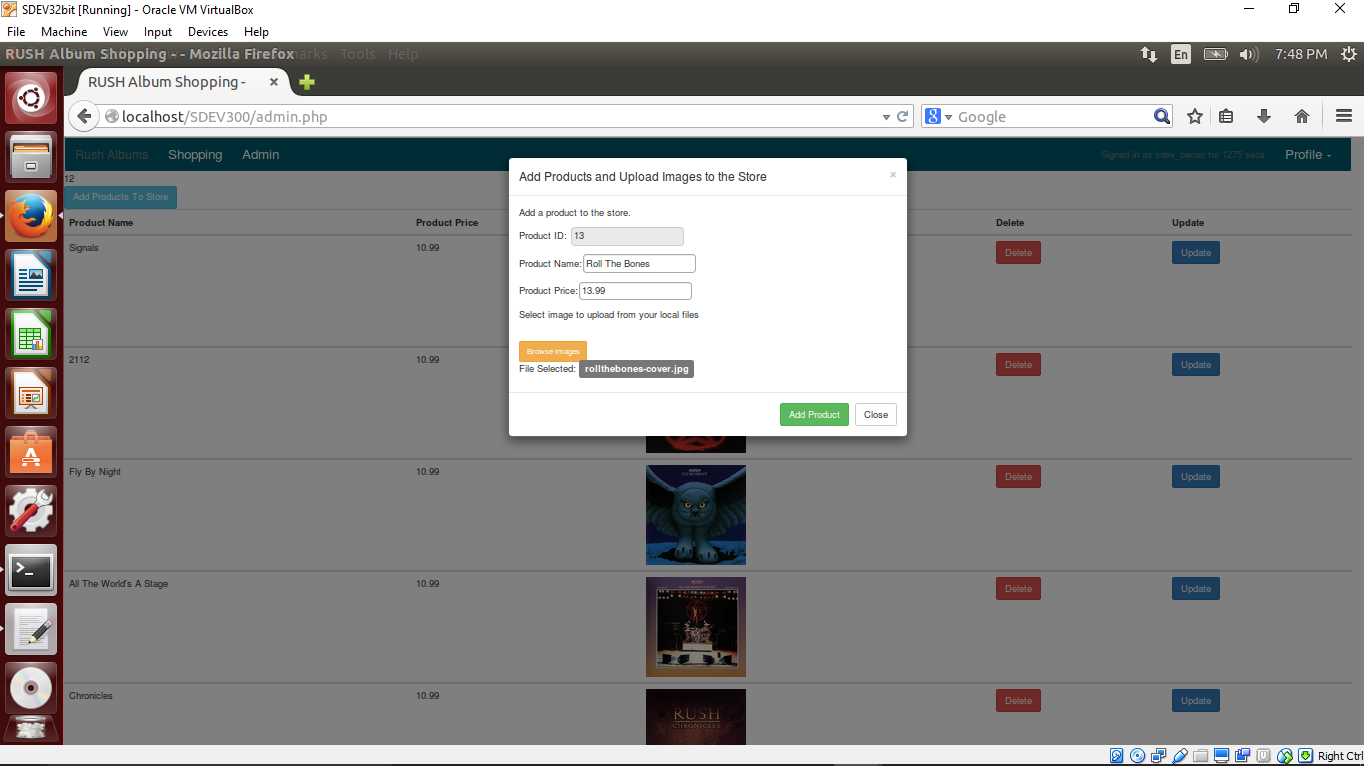
1. The first screenshot is when sdev\_owner logs into the site and the admin option on the toolbar is available. This is the normal shopping site that a user can see but also to check if your added your product correctly.



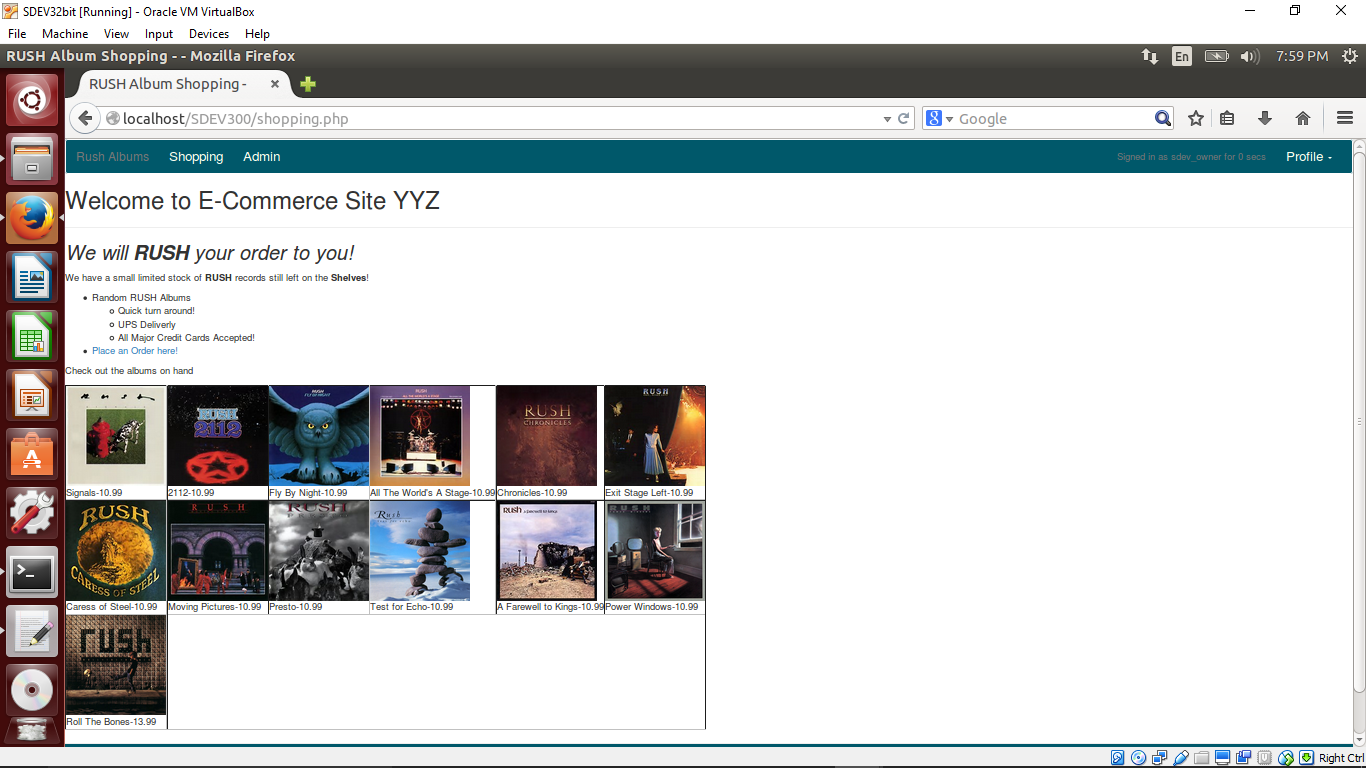
2. This screenshot shows the admin.php site that allows the admin to add, update, or delete the products in the store.



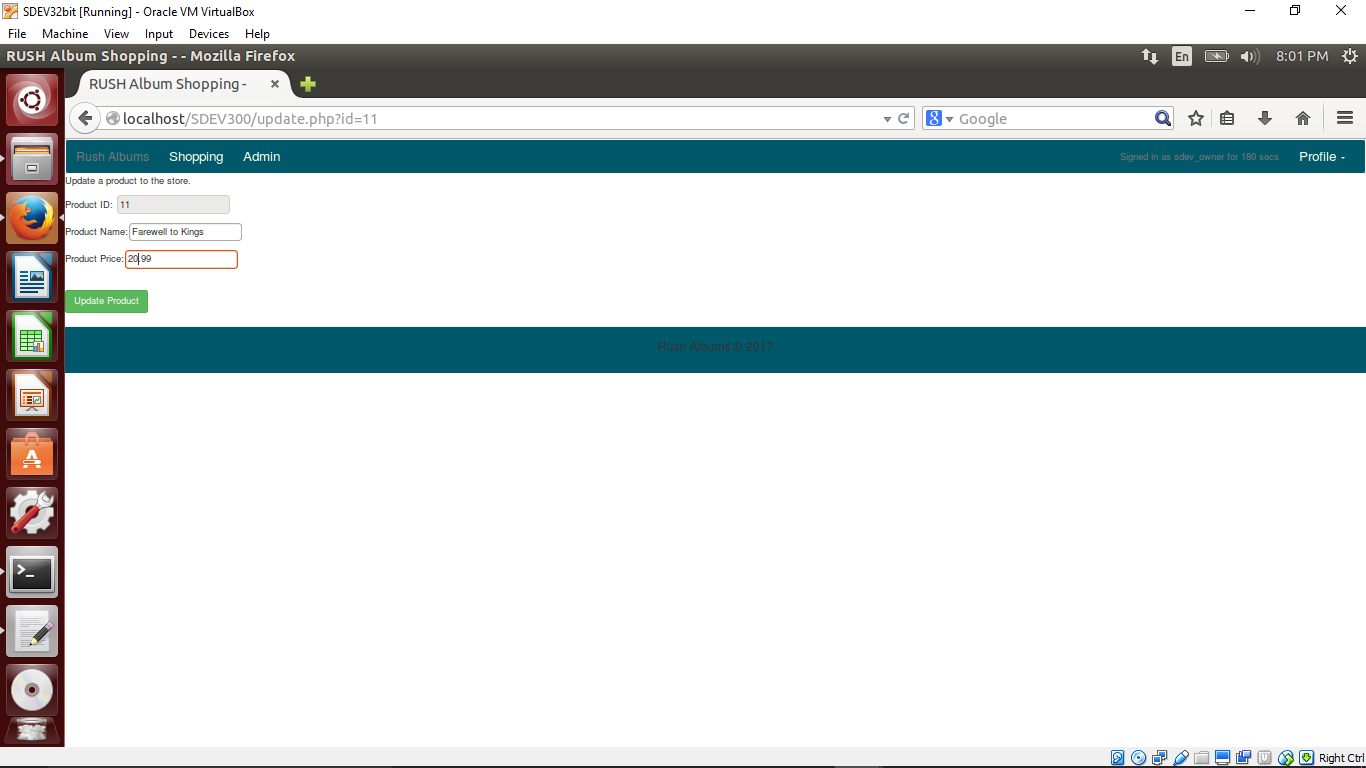
3. To add a product click on the “Add Products to Store” Button and a modal will appear. Simply add all the information including the path to your product picture and it will upload into the directory. The database only housing the link to the image.



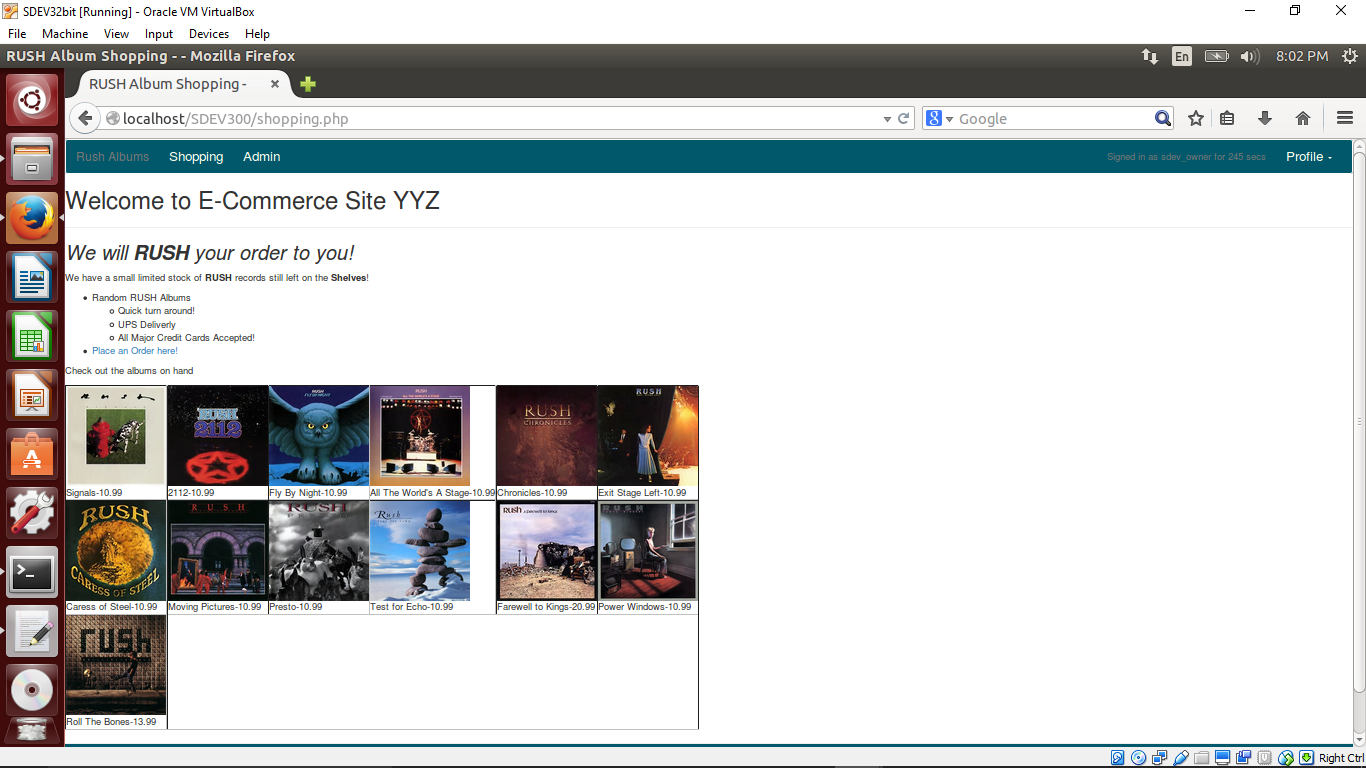
The result of adding the new album to the store. Roll the Bones was added and the price is 13.99.

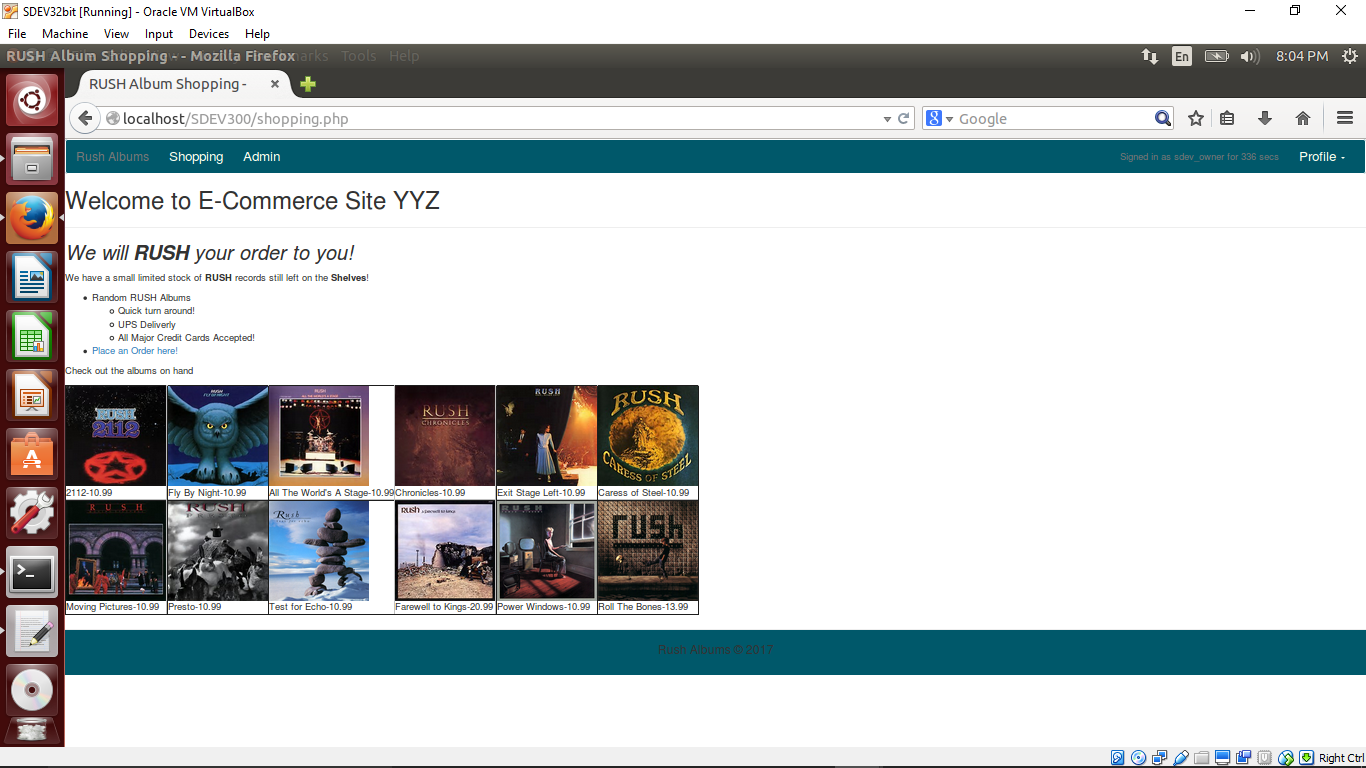


4. Screenshot of changing the price and name of “A Farewell to Kings” to “Farewell to Kings” and updating the price to show 20.99.

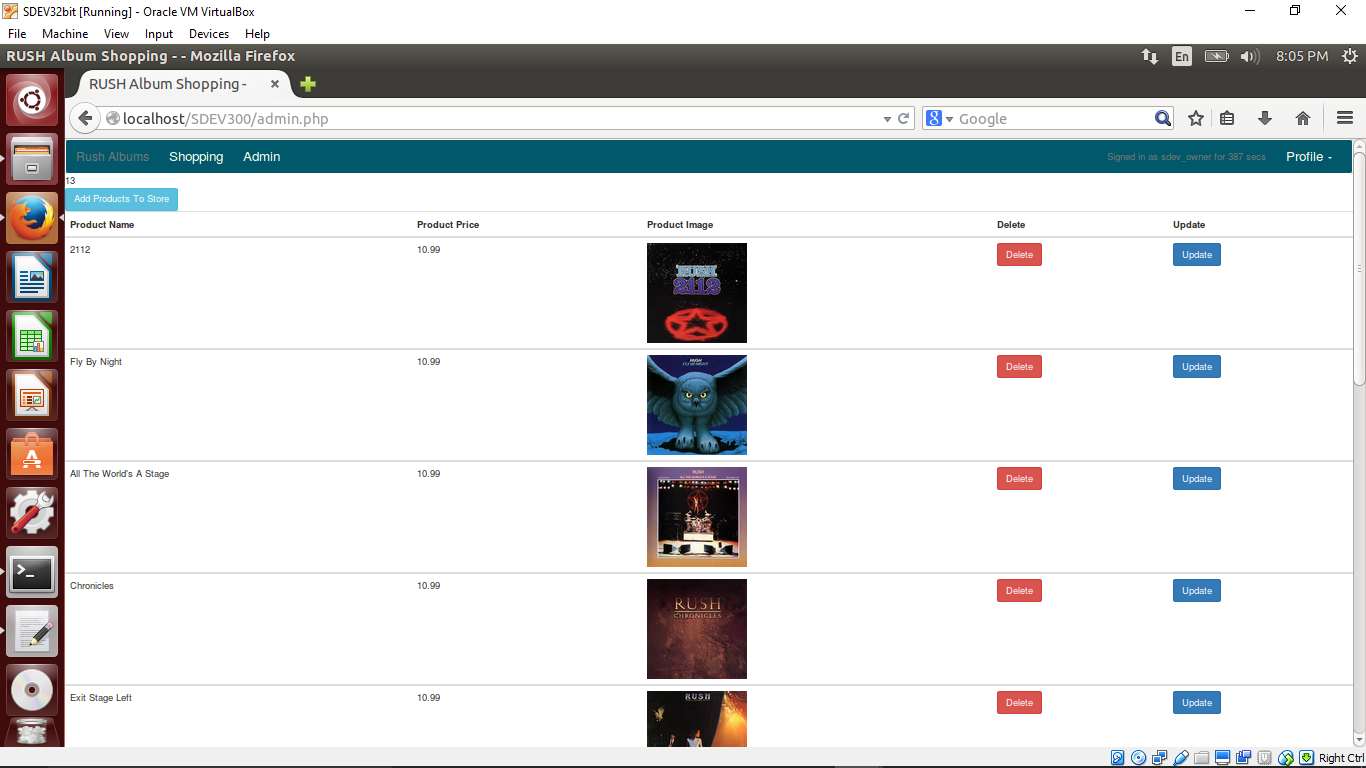


The result shown on the shopping page.

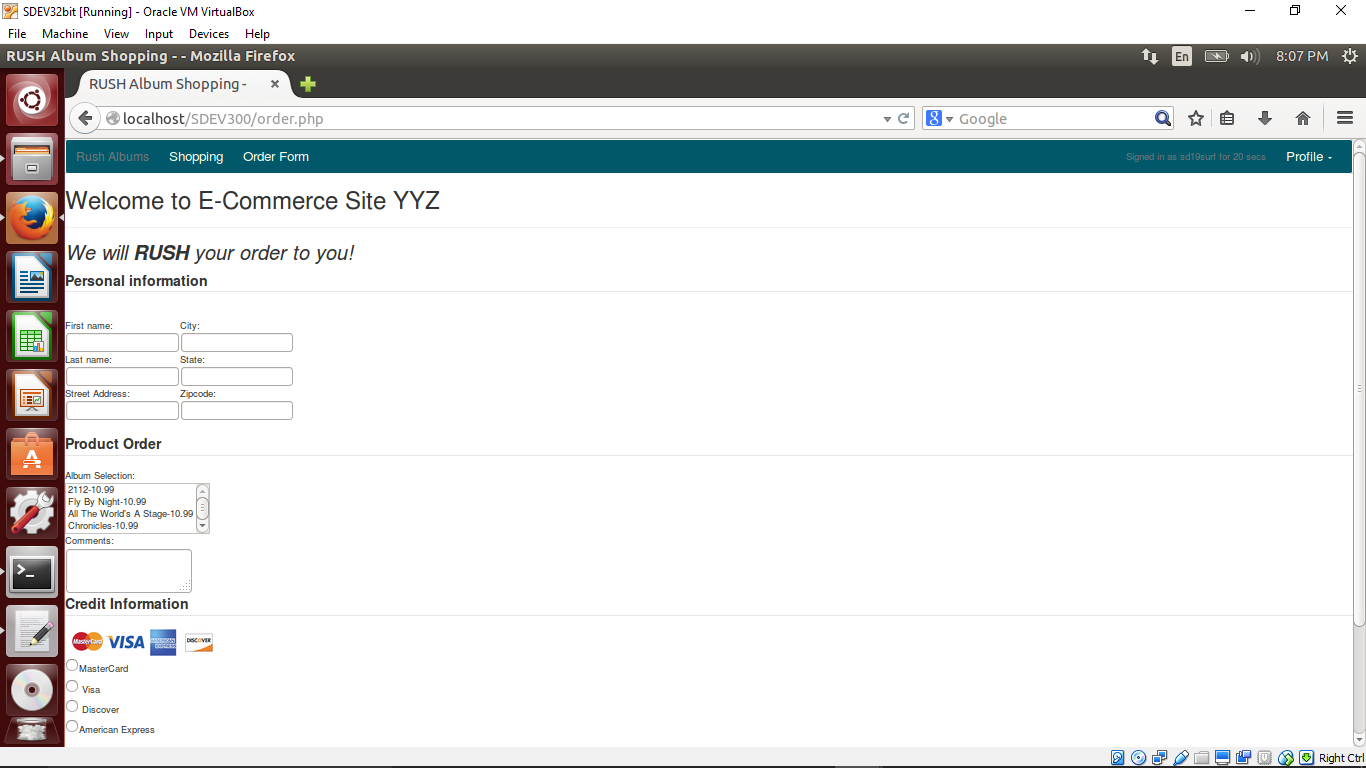


5. Deleting one Album we are now out of stock on. Removing “Signals” from the shopping page.

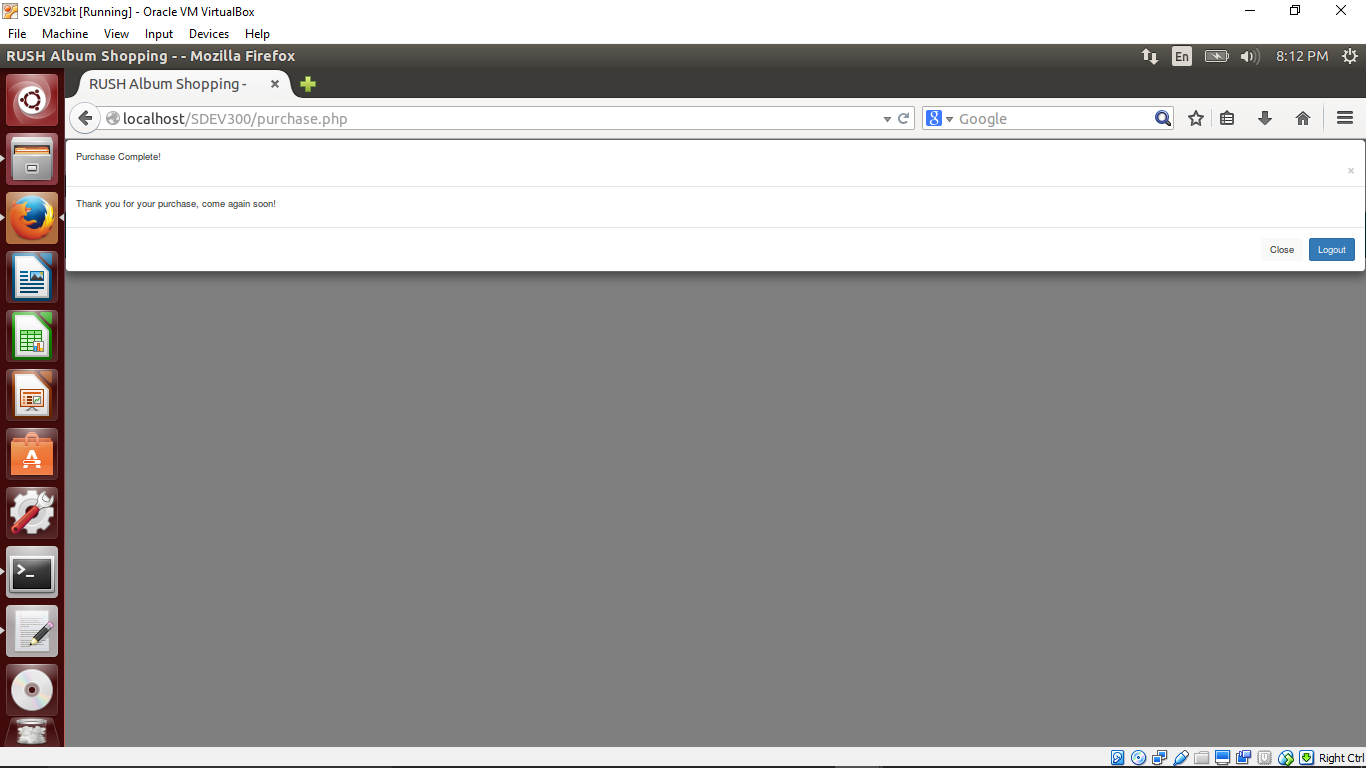
6. The admin page will list the products by product id in ascending order to search for them easier.



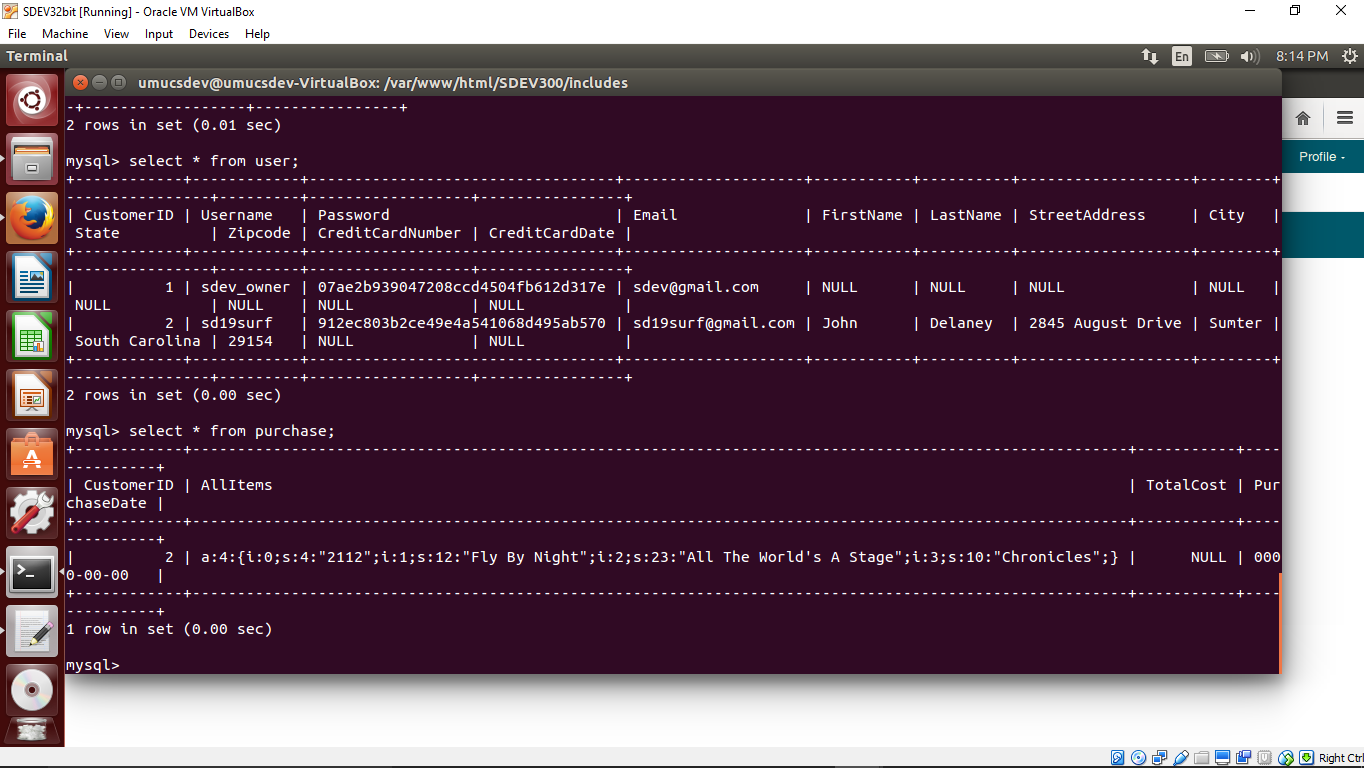
7. Once logged in with a different account other than sdev\_owner the Order Form link on the toolbar will appear. The dropdown for the available products reflects what is currently in the store.



8. Once the selection on the Order form page is submitted the data is collected in the database and the user is allowed to return to shopping or select the modal to logout of the site.



In the Database you can see the captured user data and the purchase data.



**Lessons Learned**

Oh, the lessons on this project. The easy one first was case sensitivity matters in Linux for the SQL and for the php. The interesting lesson was the array into the mySQL database. Some sources were suggesting to serialize the array into a string…that was all well and good but the insert query would still not accept the data. It wasn’t until I escaped all the characters in the serialized array that it was able to be inserted. I thought this was pretty interesting. There were a few things I purposely left off since it did not meet the requirements on the rubric. I would have continued to create a login and password function, a register function and a function to update user information. The capturing of CreditCard information was purposely left off. Another issue was permissions to the img/ directory which houses the pictures that are uploaded. Linux was being secure here by blocking create and delete but for this lab I had to change the permissions to keep the lab inside a nice folder. The correct way would be to upload into a sandboxed folder and run a virus scan before allowing the web server to use the files.