

Securing Access Guide

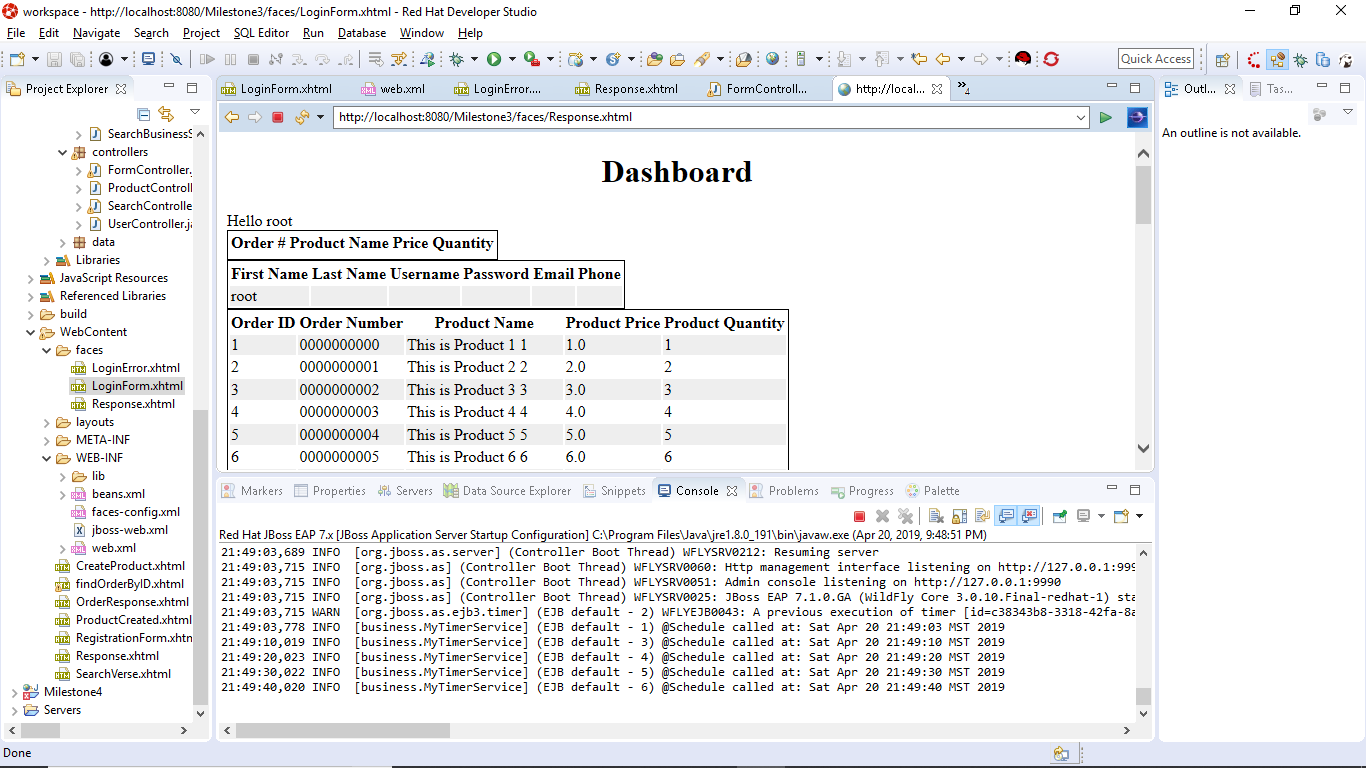
Charles Henderson

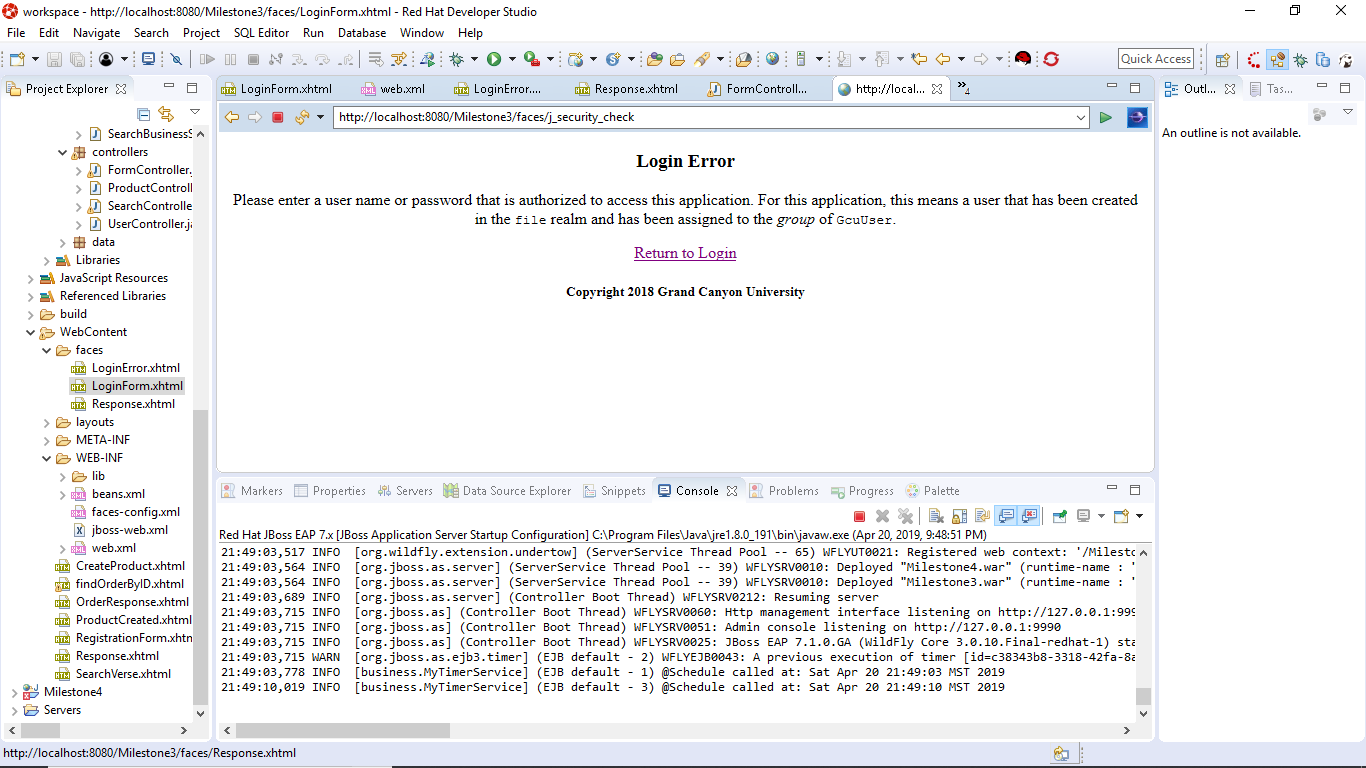


April 20, 2019

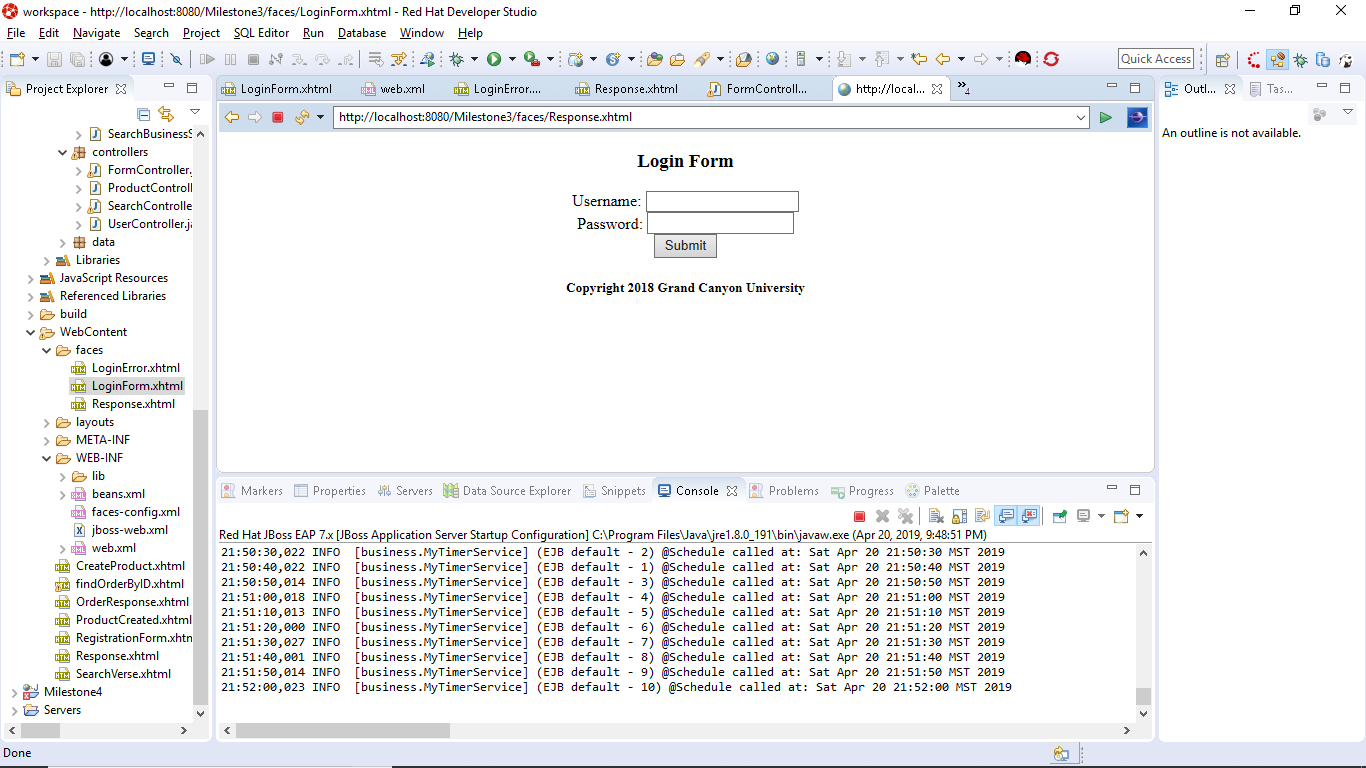
CST-235

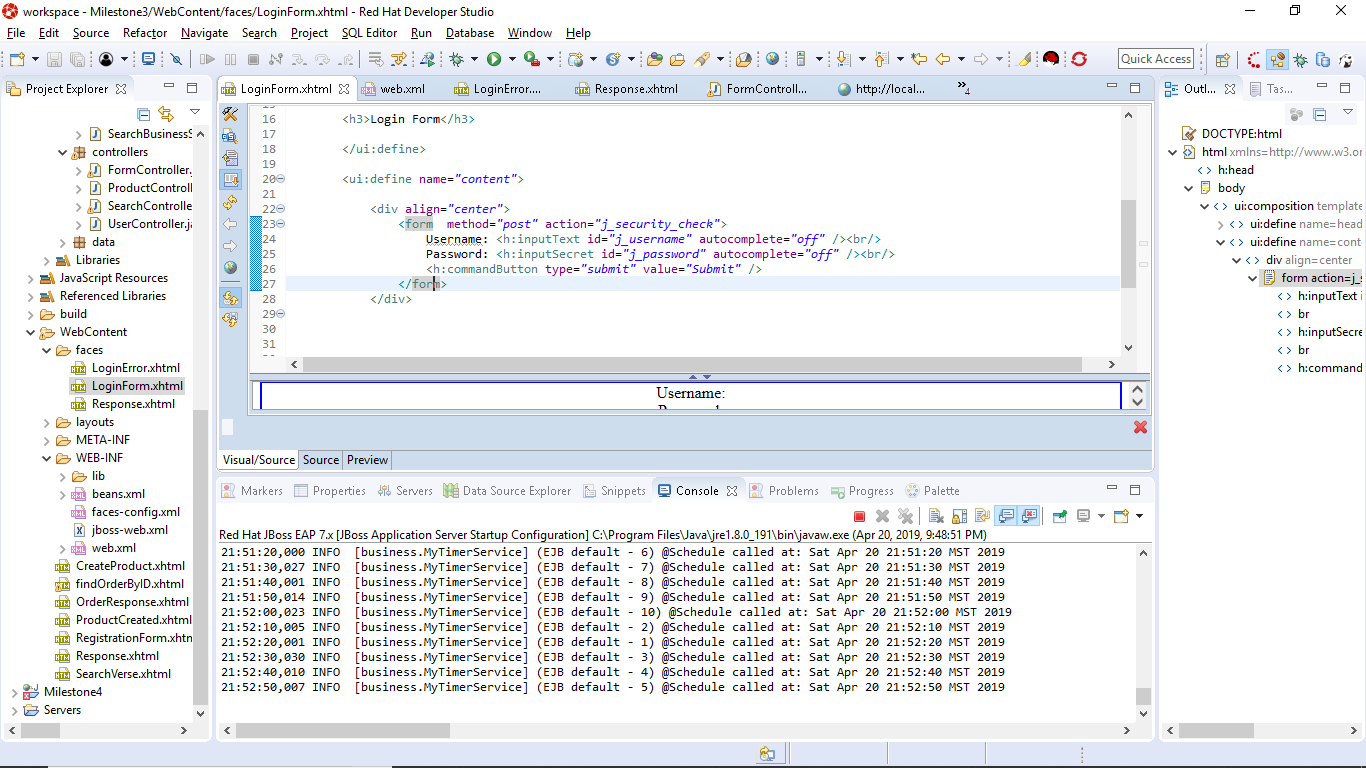
Jackson

Connected with proper login credentials: 

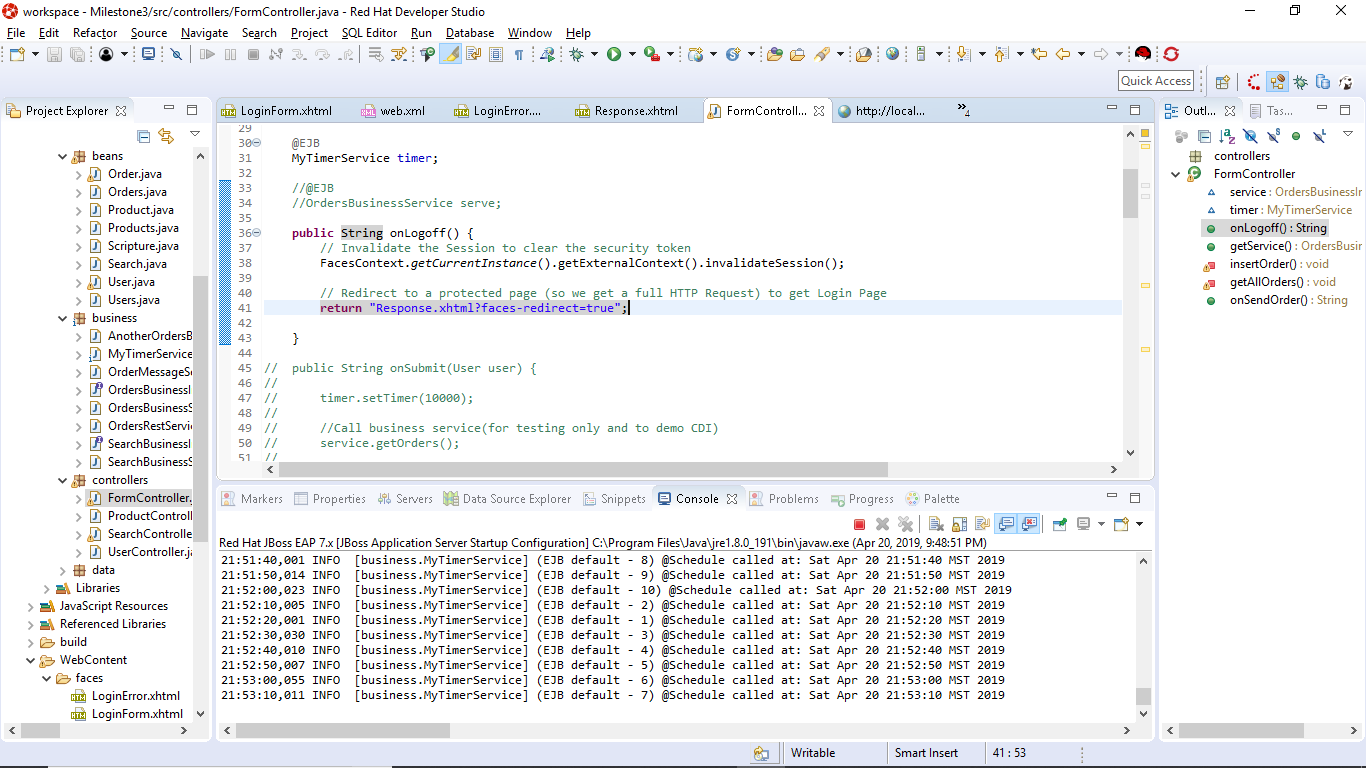
Unauthorized Access: 

Logout page displayed after hitting the Log Out button:



Implemented Code: 

New modified form controller:



Theory of Operation:

The security of our program has since used DB verification and a hiding of SQL queries. Not only this, but it has also included form validation and proper N-layer code implementation. This new type of security is covering the bases of URI manipulation. In an application that doesn’t have this type of proper security in it’s design, a potential hacker could come and go to pages directly and bypass some of the other security without going through the proper authorization. Here, we configure security directly into JAX-WS security realm. This prevents the URI’s from being projected and reroutes someone if they attempt to move to a page. Not only this, when a user logs out it will clear the current faces context and the current session beans to prevent this information from being extracted as well. Overall this has been highly interesting to me because this connected the world of session variables in php to session beans in java.