CIS484 Lab3 Checklist

1. Use of parameterized queries wherever input comes from a TextBox to prevent SQL Injection attacks (#6 below is the one exception to this). HALF DONE Jay will work on this Friday 2/26

2. Use of the PBKDF2 Encryption technique and files to securely store any Passwords.

3. New Customers can create an account with the site using a “Customer Portal”. This will be a customer “facing” part of your application, whereas the rest is on the “employee” side.They can choose a username, password, and enter their Name, Email (this will be their username), Address, and Phone Number. Once they have a login, they will be able to send a Service Request with the following information: Type of Service; Date; Description of Needs. Once they “send” this, the system will place it within a notification list/area that Employees can see when they first log in. A Workflow / Service Ticket can be kicked of by accessing each of these “internal contacts” which bring along all the customer’s information for the Initial Contact Form in Lab #2.

~~4. Store user account information and passwords in a separate database called “AUTH.” I will already have this DB on my machine but it will be empty. You will also provide the SQL statements that will create the tables for this second database.~~

~~5. Web.config file contains connection strings for all databases.~~

6. Use at least one Stored Procedure that is passed parameters from your application to process login attempts. Include this stored procedure in a separate text file (your application will not automatically create the stored procedure). The name of the stored procedure AND the name of the file you list it in will be “JeremyEzellLab3”. Make sure you use this name in your application code when calling it.

~~7. Use proper encoding to prevent Cross-Site Scripting for TextBoxes~~

8. Configure your application and DB so that Auctions are unique events. When the workflow/service ticket for a customer reaches the employee that coordinates auctions, they can assign the customer’s inventory to be sold under a specific auction event.

9. Employees who are logged in can search for a specific customer (by first or last name) and click on that customer’s details to see all activities with that customer (all past service tickets, both open and closed). Details for tickets can then be drilled down into.

The following requirement if not met will result in an automatic 0 for the Lab:

• ~~No ID or primary keys will be displayed, used, or requested anywhere in the UI for your application. All listings, selections, and searches will be made using text descriptions/names of entities/records.~~

All submissions will include a test login with a username of “admin” and password of “password”. You will need to create this in its encrypted form and include this with your test INSERT statements.

~~• All SQL must be error free and written by you (no tool generated scripts).~~

• Include no DROP statements with your test SQL. (We will implement this before turning in)

• Include a separate TEXT file with your submission that details the full names of you and your partner(s), if any.