CIS 655 Assignment 6
Database Stored Procedures, Security and Encryption

Instructions:

1. Modify table definitions and stored procedures to "appropriately" restrict or check the data to increase database integrity and keep the data clean. Implement the "CRUD" stored procedures to manage/encrypt/decrypt credit card data – you have already implemented the "Retrieve" stored procedure. These stored procedures must do input validation, protect from injection (so as to disallow cross-site scripting) and raise errors back to the web server.

   When you believe you are ready, remove the "cleartext" (PlainText) credit card column. Make sure that stored procedures still work, i.e., the data format displayed on your web page matches the data displayed from my server (10.6.55.20). Submit all stored procedure code to Canvas.

   Finally, configure the "stephen" account so it can no longer access the DB, except through the stored procedures.

   Grading Rubric (60 points): We will attempt to insert and retrieve data through the "http://10.6.55.20/new/InsertCC_Form.asp" (sp_insertCC), "http://10.6.55.20/new/UpdateCC_Form.asp" (sp_updateCC), "http://10.6.55.20/new/RetrieveCC_Form.asp" (sp_retrieveCC), "http://10.6.55.20/new/DeleteCC_Form.asp" (sp_deleteCC) pages. And, we will check that the "stephen" account can no longer run string based queries. We will evaluate the level of validation sophistication (whitelisting) in each stored procedure.

2. Configure your server to restrict direct connections ONLY from the 10.6.55.20 web server – thus the "stephen" account can only authenticate from the web server.

   Grading Rubric (10 points): We will attempt to direct connect the "stephen" account from another server IP.