Executive Summary

Ryan Boyce

November 29, 2016

Philadelphia Truck Lines Packet Analysis with Burp Suite

**INTRODUCTION**:

This report summarizes the packet analysis conducted against Philadelphia Truck Lines on November 28, 2016. The reconnaissance performed against the company earlier in the semester aloud for a better understanding of the company as well as the shipping industry as a whole. The information contained within packets obtained using Burp Suite were more readily interpreted.

Philadelphia Truck Lines’ home website is phltrucklines.com. There is a link presented to the user who is an employee of the company to login to “input or update a new shipment”, <http://www.phltrucklines.com/login_new.asp>. Upon following this link and reviewing the packet structure in Burp Suite, it was found that the Username and Password fields are easily identifiable and highly vulnerable as SSL certifications are not used. Upon further investigation, it was that the user does not, in fact, have to be logged in to perform any inputs or updates shipment information. Following the link, <http://www.phltrucklines.com/airupdatesearch_new.asp>, a list of shipments with unique IDs is presented. Using Burp Suite, it was possible to edit the ID of a shipment, send the request to the site, and receive data back including Date of Arrival, Broker, Weight, Date Picked Up, and specific Comments.

**OBJECTIVE**:

The Objective of this analysis was to identify where, if any, flaws existed in the ways in which Philadelphia Truck Lines presented data from its site to users using Burp Suite as a proxy server.

**CONCLUSION**:

It has been determined that the Philadelphia Truck Lines website is critical flaws that present detailed shipping information to potentially unwanted individuals. It is recommended that the company place shipping information “behind” a log-in screen and use SSL certificates to encrypt data in transit.