**Vaibhav Shukla**

**MIS 5211**

**Introduction to Ethical Hacking Analysis Report 3 – Burpe Suite Analysis**

**Date-11/29/2016**

**Introduction**

The Burp Proxy tool gives direct view into how the target application works "under the hood". It operates as a web proxy server, and sits as a man-in-the-middle between the browser and destination web servers. This allows the interception, inspection and modification of the raw traffic passing in both directions.

**OBJECTIVE**:

The Objective of this analysis was to intercept and inspect the ways in which Test Panda presented data from its site to users using Burp Suite as a proxy server.

**Executive Summary**

There were serious flaws which came out using the analysis tool. The site is accessible from URL-www.testpanda.com.I started my analysis by registering to the site and then logging with the given credentials, the page had necessary security in place during new registration and logging. All the information intercepted as user input was sent to the server in an encrypted format.

I then proceeded to the edit profile page which has some flaws. All the section of edit profile when submitted were sending the input as it is without being encrypted.

Name, Address, Mobile-Number, User Name, Password, and Email Id were clearly visible.

I navigated to a few more pages and then came across the Add Cart section where I can add the test series I wanted to purchase. I selected a test series and clicked on the checkout option. It had the payment box being auto filled with the payment amount. The burpe suite could capture that amount and was clearly visible. Any man-in-middle can easily change this amount to his wish. The payment server will hit with that amount and the hacker can get any amount of money deducted from the customer account.

**Conclusion**

The Test Panda website contains some critical flaws and it should use an encrypted channel for sending the data like SSL.