**Incident Report:** CL-15052-Intro-Burp-Suite

**Date:** 10-18-2022

**Executive Summary:**

As a means of an introduction to the Live Project, the goal of this reserve story was to become familiar with Burp Suite, one of the most popular pen-testing and vulnerability finder tools that will be used in the majority of the offensive Live Project tasks.

**Methodology:**

To complete this task successfully, I took the following actions, in order:

1. Watched the initial linked YouTube tutorial - Port Swigger’s “How to intercept HTTP requests and responses using Burp Suite”
2. Watched additional Burp Suite essential videos, including:
   1. “How to scan a website for vulnerabilities using Burp Scanner”
   2. “How to resend individual requests using Burp Repeater”
   3. “How to use Burp Proxy interception rules”
   4. “A guide to Burp Suite user interface”
3. Downloaded and installed Burp Suite on my device

**Findings/Solutions:**

From these tutorial videos, I learned about the basic features of Burp Suite, a proxy-based tool used to evaluate the security of a web application that acts as a “man in the middle” between a user’s browser and the website being accessed. The tasks one can complete using the various Burp Suite features serve as the foundation of a security testing workflow, starting with intercepting and analyzing traffic, including encrypted connections on TLS/SSL connections. Some of the features that I learned about through these tutorial videos includes:

* Launching the Burp embedded browser and viewing request and response information
* Personalizing interception items by adding and creating rules within the settings tab
* Scanning sites for vulnerabilities using Burp Scanner
  + End-to-end scanning - crawling and auditing
  + Selecting individual items to audit
* Identifying various scan details to learn more about detected vulnerabilities
  + Issue Activity Log
  + Target tab details
  + Identifying specific file paths with vulnerabilities
* Reporting scans in order to have a log of the identified issues within a web application
* Using the Burp Repeater to edit or modify requests and view response information
  + Automating redirects using the Repeater

**Conclusions:**

Burp Suite is a collection of offensive tools that can be used to test the risks associated with a given web application. By using its built-in features and functionalities, this resource can be used by cyber security professionals to identify specific vulnerabilities and risks within an application and can help analysts audit web traffic in order to ensure an application is safe for both a user and site server.