Executive Summary #3 Analysis
Mengxue Ni
MIS 5211 Intro to the Ethical Hacking
December 1, 2016

Burp Suite Analysis—Groupon

Introduction

Burp Suite is an integrated platform for performing security testing of web application. It is a great and versatile tool that help beginners to start with security of web-based applications. Today, by downloading the free version in Kali Linux, I was able to perform a test on groupon.com.

Here is a short introduction of Groupon, Groupon is a deal-of-the-day recommendation service for consumers. Every 24 hours, Groupon broadcasts an electronic coupon for a restaurant or store in your city, (in my case, Philadelphia) recommending that local service while also offering you a 40% to 60% discount if you purchase that service. I used to like to use Groupon, but recently I found it was insecure and didn't get rid of past-date discounts on time.

Findings

First, I went to the homepage of Groupon, then I signed up with a test user. Finally, I logged in with the test account. With the proxy function on Burp Suite, on the homepage (www.groupon.com), I was able to see the division is Philadelphia. Although I can tell other data is encrypted. I observed that there is a host called https://stags.bluekai.com showed up in the HTTP history. I searched the Bluekai, BlueKai is the industry's leading cloud-based big data platform that enables companies to personalize online, offline and mobile marketing campaigns with richer and more actionable information about targeted audiences. Then I researched the relationship between BlueKai and Groupon. It turns out last year, Groupon found their manual approach to scheduling ads in daily deal emails to consumers had become slow and cumbersome. They turned to OpenX, allowing the company to schedule ad deliveries overnight. BlueKai and OpenX are competitors. This new was published on February 9th, 2011. Therefore, I didn't find other recent news, I should expect to see OpenX instead of BlueKai on Groupon website. This could be a risk for Groupon since they don't work with BlueKai anymore, but they are still on the host of Groupon.

Besides this problem, there are a lot of cookies, most of them are session cookies. Cookies should be created when I use the browser to visit a website that uses cookies to keep track of my movements within the site, help me resume where I left off, remember your registered login, theme selection, preferences, and other customization functions.

Through this exercise, I was able to understand Burp proxy function. Burp Proxy is an intercepting proxy server for security testing of web applications, it operates as a man-in-the-middle between the browser and the target application, which allows me to intercept and modify all HTTP/S traffic passing in both directions, view all traffic in the detailed Proxy history, work with custom SSL certificates and non-proxy-aware clients.

Resources:
http://www.mediapost.com/publications/article/144503/groupon-moves-to-new-openx-global-publisher-platfo.html
http://www.oracle.com/us/corporate/acquisitions/bluekai/index.html
https://portswigger.net/burp/proxy.html