Mengqi He
MIS 5211: Introduction to Ethical Hacking
Analysis Report 3: Burp Proxy Analysis
Date: 12/01/2016

Burp Proxy Analysis for Barnes & Noble

For this assignment, we are going to use Burp Proxy to have an intercepting proxy analysis for security testing of Barnes & Noble, the largest retail bookseller in the United States. Burp Proxy is an intercepting proxy server for security testing of web applications. It operates as a man-in-the-middle between user's browser and the target application, allowing users to intercept and modify all HTTP/S traffic passing in both directions. The target website for this analysis this time is www.barnesandnoble.com . Barnes & Noble sells books, eBooks, magazines, toys & games, music, DVD and Blu-ray, and related products and services both online and in its 640 retail stores over the US. B&N started selling books online since the late 1980s. In 2012 October, B&N was reported to suffer a credit card data breach that credit card information for customers who shopped in August and September at 63 Barnes & Noble stores across the country. Hackers broke into the keypads in front of registers where customers swipe their credit cards and enter their PINs.

In this analysis, I tested the security of B&N's website to see the safety and security of its online store. I conducted this test using Firefox Browser on a Windows 10 virtual machine. Leaving the intercept on, I firstly accessed its homepage. The intercepting report showed that I accessed the homepage through search.yahoo.com and I found all important information is encrypted. Another thing I found was that Burp also reported an another host which is assets.adobedtm.com. Adobe Dynamic Tag Management is a tag manger enabling company to easily manage their analytics, media, and other tags, and oversee the tracking rule sets across all of the sites. Secondly, I tried to access the sign-in page, and there seemed to be no great flaw. The log-in page was hosted by a subdomain of barnesandnoble.needle.com. Need.com is an ecommerce sales chat platform to improve online customer experience. Burp also reported several advertising hosts including id.adnxs.com, ads.yahoo.com, pixel.rubiconproject.com, and static.criteo.net. Thirdly, I clicked on the "create an account" link to register as a customer and I logged into my test account. Burp reported these two register and account pages and I found no flaw and everything seemed secure. Fourthly, I clicked on the "membership" link and then "join today" link. I was directed to the shopping cart page with a membership card added to may cart. During these two steps, I did not find anything suspicious in the intercepting reports. In addition, Burp also reported host gecounters.us1.gigya.com. After research, I found that gigya.com is a customer identity management platform that helps companies build trusted digital relationships with consumers. It's great to see that B&N use a trustworthy third-party platform to manage their customer identities. Fifthly, I randomly opened a harry potter events page and then clicked on a promotion ad of "Fantastic Beasts and Where to Find Them". Since these two pages did not involve customer information, I did find anything unsecure. Burp also reported several other hosts. One type of websites were media sites bat.bing.com, msn.com and twitter.com. The

second one type were advertising analysis websites. One was siteintercept.qualtics.com, an online marketing and research tool used to dynamically interact with targeted website visitors for surveys, polls, ads, promotions, and more. The last one was log.dmtry.com owned by Adometry Inc. that provided marketing analytics and intelligence services, including tracking of users to link buying behavior with particular marketing channels. It was acquired by Google and now is called Google Attribution 360.

Through the proxy analysis, I found that B&N basically did a good job on protecting customer information. However, it creates too much cookie for advertising and tracking customer behavior. I think this would be a potential threat to customer information.