Ahmed Alkaysi

11/27/16

Burp Suite Analysis QVC

For the Burp Suite assignment, I chose to do analysis on the company QVC. QVC, headquartered in West Chester PA, is a company that sells products primarily through the TV and internet. As part of the analysis, I navigated to [www.QVC.com](http://www.QVC.com) site and clicked on a few links. I also attempted to login using my email address without actually having an account, as well as start a live chat to see what kinds of packets were being sent back and forth. Through this experiment, I discovered a number of external sites that were communicating with QVC, and identified a few packets that had some pretty interesting data.

The first step during this experiment was just to go to QVC.com and click on a few links. Immediately, I noticed a number of external sites communicating with qvc.com including: monetate.net, tiqcdn.com, google, Bing, Facebook, and Pinterest. The Google and Bing sites were being used for ads. I wasn’t sure what monetate.net or tiqcdn.com were, so I looked them up. When I went to Monetate.net, a web page was not returned. Instead, googling referred me to Monetate.com, which was a company that provided products around customer intelligence. Tiqcdn.com was a domain owned by Tealium, which was used for on-line user tracking and tag management for web pages. Another site I found pretty interesting was skimresources.com, a domain owned by skimlinks.com. This was a company that provided affiliated marketing products centered around the type of content that was on a website. After looking at navigating through the site, I decided to get more active by going to the My Account page and trying to login.

To login, I went through My Account page. I saw a packet that was received that had multiple different parameters for the page. I especially was tempted to modify the ‘cart\_qty’ parameter from value of ‘0’ to something greater than ‘0’, and parameter ‘cmNPOType’ from value ‘NOTCHECKOUT’ to ‘CHEKCOUT’ just to see how the page would behave. Another interesting parameter was ‘curntChnl’. It had a value of ‘QVC’, which made me think that there were other ‘channels’ that products on QVC can be sold through. After entering my email address, I was navigated to the registration form, as the email account did not exist. One thing I noticed were the field names and their corresponding error messages in the POST packet, even though none of the error messages were shown on the actual page itself. After this, I wanted to see what kind of information was being exchanged within packets if I were to start a live chat.

For the live chat, I put a phony name and email address, briefly connected, then closed chat before the other party could type anything. In the POST packet, I saw my email address and name being used. I also saw multiple possible messages that could be prompted during a live chat session, including messages regarding the ‘agent’ starting a video chat or transferring a file. The domain that was being used for live chat was live.qvcchat.com. When I navigated to this site through the browser, there was a single page that had big letters ‘IIS7’ and the word ‘Welcome’ translated in multiple different languages. When I clicked on the letters, it took me to www.iis.net, which stood for Internet Information Services owned by Microsoft. I thought this was very interesting. Although I did not discover anything crazy through this experiment, I gained knowledge on the different parameters used during a packet, external sites being leveraged for QVC, and the service that is running the live chat function. I would consider this recon mission successful.