Shain Amzovski

MIS 5211 .001

Burp Suite Analysis

**Victory Brewing Company**

The company I decided to analyze using the Burp Suite proxy intercept is Victory Brewing Company. Victory Brewing Company is a brewery, with its headquarters located in Downingtown, Pennsylvania. Victory specializes in craft beers, which are specialty beers and higher quality than your average Miller, or Budweiser. The company was founded by two life-long friends named Bill Covaleski and Ron Barchet. Victory Brewing company first opened its doors on its Downingtown location on February 15, 1996. The location was previously a Pepperidge Farm factory and has been repurposed as a restaurant and brewery. The initial restaurant had 144-seats and a 70-foot-long bar. In its first year, Victory brewed 1,725 barrels of beer, and this number has since risen to 125,713 in 2014. Victory currently has three breweries, including their original location in Downingtown, PA. Each brewery also serves as a restaurant location, similar to the initial set-up from 1996.

For the Burp Suite Analysis on Victory Brewing Company, I used a personal desktop running Windows 8.1, and Google Chrome Web Browser Version 54.0.2840.99 m (64-bit). Burp Suite Free-Edition Version 1.7.10 was used to act as an intercepting proxy to capture packets from Victory Brewing Company’s website. While running Burp Suite proxy on Victory’s website, I noticed in the “Target” tab, all of the other websites that were interacting with https://victorybeer.com/. One discovery I noticed was what YouTube channel Victory’s site was publishing to. I was able to drop-down the tree with http://youtube.com/ and see the Raw PHP code that used the “GET” function, and showed the name of the YouTube account. A second important discovery was that when I ran the “Spider” feature on on Victory’s Website, a form popped up. This form was for the WordPress Admin Site Login page. No where on Victory’s public page was there a login button, so it was safe to assume the page was hidden. The spider feature was able to discover the Login Page for the WordPress site. Target also indicated that this site was built on a WordPress platform because it revealed some wp-content folders. A security flaw with Victory was that they used the common WordPress Admin Login page, /wp-admin. This is dangerous if someone has an employees’ computer proxied and is listening for packets because they may be able to capture a username and password in plaintext. I had the Intercept feature turned on, and attempted a fake username and password, which came back to me in plain text. After doing some research, I found that when you connect a proxy to the localhost, via port 8080, none of the data is encrypted until it goes out to the server.

In conclusion, it was determined that Victory Brewing Company, a smaller brewery company, has its website on a WordPress platform being hosted by register.com. Since the site does not contain any customer information, sales information, employee logins, or other critical confidential information, a WordPress site is sufficient. Victory has added security on their site with valid SSL certificates and https. For employee confidential information, a link re-directs users to ADP. In the employment opportunities section, employees have to look for open positions on ADP’s website and apply only in that location. Any other third-party applications would not be considered. The biggest security threat Victory could face is if the WordPress admin credentials are stolen, false links can be planted throughout the site to mislead customers to potentially malicious sites, download links, etc. Hackers could also plant false news stories about the company that could potentially harm their reputation etc. Overall, the website is secure and serves the necessary purpose as needed by Victory Brewing Company.