Marcus Wilson

MIS5211.001

Burp Analysis

**GEICO Burp Analysis Executive Summary**

The Burp Suite is a platform that consists of several tools used to perform security testing on web applications. I completed my Burp testing using a Kali Linux VM. I used the Burp Proxy tool to setup a proxy server to intercept all web traffic coming from my Firefox web browser. I chose GEICO.com as my target to investigate what traffic was being exchanged. GEICO is an insurance company that is based in Chevy Chase, MD and manages over 14 million policies ranging from auto to home insurance. The GEICO website presents current and potential customers with the opportunity to browse policy offerings and receive insurance quotes. There is a secure part of the website that allows policy holders to manage their existing policies.

Once I connected to the GEICO homepage I had several requests to forward to the browser in the intercept tab of Burp. I was initially denied by the browser as I had to setup a security exception to validate the certificate that Burp was providing. Once I granted the security exception, the first requests consisted of images, fonts, homepage layout variables, and general tracking cookies. The Site Map tab showed a large volume of third-party sites that GEICO was also requesting information from. These sites included internal company sub-domains such as boats, claims, home owners, etc. The additional sites also included social media, ad companies, and customer experience management firms.

The second part of my analysis I attempted to login to a policy account using a test username and password. The site first created a unique session ID and gave me a randomly generated token. Once I submitted the form I could see the username and password being passed back to the website in plain text. This was very concerning because if someone was being malicious and setting up a man-in-the-middle attack they could easily grab a user’s login and password.

Following my analysis, I tested a few additional sites such as Amazon, Gmail, and MLB.com. I noticed that compared to these additional sites, GEICO has very little request activity. Amazon and MLB were full of ad activity and creating cookies to track user activity.