Jeongyong Yang

CAS CS 357

Professor Goldberg

October 22nd, 2022

Capstone Report

I watched the videos that explained the privacy policy and security of the following websites: Canva, Indeed, Lululemon, and Tesla. Even though these websites all provide sufficient security protection against possible threats, their privacy policy fails to protect personal information regarding users by sharing them with third parties.

Lululemon, Tesla, Canva, and Indeed successfully protect the information of users from adversaries. Most of the cookies from these websites are not set as same-site, HTTPonly, or session cookies, raising the potential risk of cookie theft. However, these websites protect the cookies of users by including CSRF defense within their website: Canva, Indeed, and Tesla include CSRF validation tokens, and Lululemon and Tesla use referer validation. In addition, all of the websites have HSTS preloaded, preventing connection to their URLs with HTTP and therefore preventing man-in-the-middle attacks. Finally, they all include the most updated Javascript libraries and have the majority of the URLs that are fetched with the website set as HTTPS.

Despite the fact that the four websites protect the information of users, they share some of the information of the users with third parties listed in their privacy policies. All of the websites include tracking pixels, which allow advertising websites to naturally collect information about the users, within their URLs. For example, Canva includes tracking pixels from Reddit and Lululemon has tracking pixels from Snapchat. According to the privacy policies of these websites, the websites collect information regarding personal information from users, including name, address, payment information, etc. Some of the information

collected is naturally shared with the third parties of each website, which surprised me because the sharing of information implies the possibility of stealth of users' information if one of the third parties of the website becomes vulnerable to security risks.

Another surprising factor was the absence of multi-factor authentication, except with Tesla. I believe that two-factor authentication is important, especially nowadays, because if passwords get hacked (or even guessed), the adversary still requires an additional step to log in as a victim, which makes the password alone useless, and therefore bolsters the security of websites. However, according to the video reports of these websites, Lululemon, Indeed, and Canva did not authorize users again after the user logs in with their login credentials.