Link to the presentation: https://youtu.be/JG1paP2FQ88

Seungwon Burm, Yuchan Kim, Cristobal Newman, JeongYong Yang

CAS CS 357

Professor Goldberg

October 16th, 2022

Second-Deliverable Report

United Airlines keeps numerous cookies on its website. Prior to the login process, two cookies were set under united-app.quantummetric.com, named S and U, and numerous cookies were set under United.com. All of the cookies include names, values, domains, paths, expiration dates, sizes, whether they are HttpOnly, secure, same-site, or same-party cookies, and the priorities. Quantum Metric Cookies are cookies that allow the website to understand and improve the usage of the site. The numerous cookies set under United.com serve multiple purposes that either help the website to gather information regarding users and the user in terms of security issues or convenience. For example, the _gat_tealium_0 cookie is used to "ensure website functionality" and learn the preferences of the visitor to provide them with relevant advertising while the _abck cookie is used to "store and read data from the computer by using a cookie, pixel, API, cookieless tracking, or other resources." The session cookie allows the website to remember the user so that users do not need to log in again every time they navigate the website, such as "My travels" or "Checking in" pages.

After users log into United Airlines, three additional cookies are created. The cookies that get added after logging into the website are AuthCookie, SID, and User cookies, cookies that contain the most important information and therefore, must be secure and not shared with others. Therefore, United Airlines sets the AuthCookie and SID cookies as session cookies, cookies that expire after a certain period of time even if the user forgets to log out from the website directly. In addition, United Airlines forces the User cookie to expire after a month

from the login time. However, United Airlines fails to set the three cookies as HttpOnly cookies or same-site cookies, which provides opportunities for adversaries to attack the user by sending them an URL that includes Javascript to access the cookies using the code document.cookie, prior to their expiration.

Numerous URLs are fetched when United Airlines URL is loaded, to collect data regarding users for advertising and third-party analytics, as stated in United's Privacy Policy. Some of the URLs fetched (E-10398.adzerk.net, Lpcdn.lpsnmedia.net, Lptag.liveperson.net, etc.) are not HTTPS protected, allowing "man in the middle" attacks.

According to Chrome Developer Tools, HSTS is preloaded. The strict-transport-security, under Headers under Network in the Chrome Developer Tools, includes values max-age = 31,536,000 includesSubDomains, and preload. With the usage of HSTS, users attempting to connect to the URLs of United Airlines over HTTP will automatically be redirected to the HTTPS URL of United Airlines, bolstering the security of the website by preventing possible man-in-the-middle attacks. In addition, United Airlines does not include mixed HTTP/HTTPS content within the website by having all "src" tags of the images to begin with HTTPS. According to https://hstspreload.org/, the max-age value must be at least 31,536,000 seconds, which is 1 year converted into seconds and therefore, the max-age value of the URLs within United Airlines meets the requirement of HSTS-preload.

United Airlines defends possible CSRF in a few ways. Once a user logs into United Airlines, the cookies that contain the identification of the user are set as session cookies, which forces the user to log out of the website after a few minutes of inactivity. Therefore, if users become vulnerable by accessing malicious Javascript that tries to steal information regarding the user within United Airlines, the forcing of logout prevents the stealth of cookies since the cookies disappear after a certain period of time. In addition, cookies that contain important information regarding the user are set as same-site cookies, preventing browsers

from sending them along with cross-site requests. Hubspotutk and _fbp cookies are cookies that help save and keep track of the identity of users. By setting these cookies as same-site cookies, United Airlines prevents the stealing of cookies by adversaries.

United Airlines uses Javascript libraries within its URLs. However, a few of the libraries that are included within its URLs are outdated. According to Retire.js Chrome Extension, United.com contains Maxymiser Service, which “translates users' browsing sessions into information that helps website designers make websites easier to use and simpler to navigate.” Retire.js Extension informs that Maxymiser is not using the latest version of jQuery, but is currently using version 1.11.2, which can lead to security vulnerabilities, including but not limited to “3rd party CORS request executing CVE-2014-9251”, “jQuery, prior to the 3.4.0 version, mishandling jQuery.extend(true, {}, …) due to Object.prototype pollution”, and “regex in ints jQuery.htmlPrefilter introducing XSS.”

The privacy policies of United Airlines mention that “United and third-party service providers may use clear Gifs (also known as pixel tags), in connection with our sites and service to track the activities of visitors, help us manage content and compile statistics about usage.” United Airlines include tracking pixels within the headers of HTML and advertisements on the website to collect data from the users. Tracking pixels leave potential risks to users. They not only send information regarding users to other websites without the consent of users but are also created in small sizes (1 x 1), making it difficult for users to recognize their existence.

United Airlines displays a few ads within its URLs, such as theexplorercard.com (Chase Credit Cards), cruises.united.com (United Cruises), and ihg.com (IHG Hotels). The ads that United Airlines displays are from companies that formed a partnership with United Airlines. Advertisers collect information regarding the user, including the contact information of the user, the MileagePlus Number, payment information, etc, once the user clicks on the

advertisements. Even though the natural sending of information regarding the user can lead to possible attacks, due to the sending of information to only trustable companies that formed partnerships with United Airlines, advertisements within the URLs of United Airlines are assumed to be safe. However, the sharing of information implies that once the websites of the partners, which are not controlled by United Airlines, become vulnerable, attackers would have an opportunity to steal information from the users of United Airlines as well.

During the sign-up process, United Airlines requires users to choose five questions to answer in a way that United Airlines provides a few predetermined options (about ten to fifteen) per question to gain more information regarding users. Such methods of choosing options protect the website from possible SQL injection attacks. After the signup process, when a user attempts to log in with his/her MileagePlus Number, a unique set of characters and numbers provided by United Airlines, and a password, chosen by the user during the signup process, United Airlines detects whether the user is logging in with a new device. United Airlines keeps track of the browser and the device that each user used to log in. If a user tries to log in from a different device that is not remembered by United Airlines, United Airlines asks two of the five pre-answered questions, randomly, that the user has chosen during the signup process. If the answers to at least one of the questions are incorrect, the account gets locked automatically, forcing the user to check his/her email to unlock the account. If the user forgets his/her MileagePlus Number, he/she needs to fill out a form that includes the name, email address, and birthdate of the user. After the user completes the form, United Airlines emails the MileagePlus Number to the user. If the user forgets his/her password, he/she has to type his/her name and the MileagePlus Number in the box that United Airlines provides and answer two of the five pre-answered questions, once again, chosen randomly. Failure to answer the question correctly will result in the lock of the account, which can only be unlocked by contacting United Airlines directly through a phone

call, which attackers cannot do. If the user answers the question correctly, the user can recreate the password within the URL that United Airlines provides through email. The only possible concern for the user is when the attacker guesses the answer to the questions correctly. Since there are about ten to fifteen possible options per question, the attacker has about 6.66% to 10% to guess a question correctly. Answering two of the questions correctly is a percentage ranging from 0.44% to 1%, which is a very low percentage.

During the signup process, United Airlines collects the following information from all users: name, date of birth, gender, email address, and personal address. Once users log in to United Airlines, they can include additional information, such as payment information, passport information, government ID, etc. According to United Airlines, the information collected from users is used within United Airlines directly or sent to third parties: Network Advertising Initiative, About ds-Digital Advertising Alliance, DoubleClick, and Google Analytics. However, United Airlines does not provide an option to protect its information from being sent to third parties due to the partnership between these companies. In addition, the website fails to explain the method used to share the information of users. Therefore, users, by creating an account and filling in the information, naturally agree to send their information to third parties.

United Airlines does not officially have a GDPR notice on its URLs. However, the website mentions implicating tracking methods for cookies and pixel tags in its Privacy Policy. According to its privacy policy, “cookies help establish a user session and allow our server to provide site users with the appropriate information, advertisements and services.” United Airlines gives an option for users to opt out of their usage of cookies by continuing their actions within its website as a guest. The privacy policy of United Airlines mentions that pixel tags are used to save information regarding the preferences and transactions of

users and “facilitate effective website administration.” Pixel tags are used by United Airlines and its third-party providers both on their websites and emails.

Overall, United Airlines protects the information of users effectively. It sets important cookies as either session cookies or same-site cookies to defend against possible CSRF attacks, preloads HSTS to force the website to be loaded only via HTTPS, and includes sophisticated login and signup process. However, it can enhance its website by including only the URLs with HTTPS, including GDPR notice within its URLs, updating Javascript libraries to the current version, and allowing the option to protect its information from third parties.

Sources Used:

1. https://www.carsvansandbikes.com/about/cookies
2. https://tealium.com/cookie-policy/
3. https://cookiedatabase.org/cookie/tiktok/_abck/
4. https://stackoverflow.com/questions/39205434/sid-and-hsid-cookies-what-are-they-uses
5. https://www.united.com/ual/en/us/fly/privacy.html#use_of_cookies
6. https://www.cookiepro.com/knowledge/tracking-pixel/
7. https://en.ryte.com/wiki/Tracking_Pixel
8. https://www.radissonhotelsamericas.com/en-us/rewards/offers/united-airlines-50?cid=a:rf+b:uni+i:Home+e:rhg
9. https://villas.mileageplus.com/?utm_source=united.com&utm_medium=tile&utm_campaign=q4_2022&utm_content=1015_300x300
10. https://shopping.mileageplus.com/signin/?source=cl_UA_ALL_cl__link__HomePg300_ACQBns_20221001&utm_source=cl&utm_medium=link&utm_campaign=HomePg300&utm_content=ACQBns&chan=cl&seg=&med=link&strm=&cam=HomePg300&cont=ACQBns&end=1
11. https://cruises.united.com/promotion/sweepstakes.do?utm_medium=banner&utm_source=ual-partner_site&utm_campaign=20221001&utm_content=ual_hp_728x90_sweeps
12. https://www.theexplorercard.com/rewards-cards/explorer-card?CELL=DS5&int_source=loyalty&mode=d&int_medium=dotcom&int_campaign=0480_60k3kafw_list&alm=1380&int_content=60kbm&partner_category=cc&partner_name=chase_acq&asset_type=homepage&asset_position=hplowrt&promo_code=cell_ds5&targeting=cell_explorer60k&launch_date=2022-08-11&rpc=0480&campaign_type=cce&offer_trackingid=null&source_code=null&MPNumber=a8cf5a0d5503604da76a20e488236ec6ed9b163b363a53f5b450ad7e54ffea0904b45d70add2f8be3777a4a923f8aa58
13. https://web.dev/what-is-mixed-content/
14. https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content
15. https://hstspreload.org/
16. https://www.chromium.org/updates/same-site/faq/
17. https://support.outgrow.co/docs/using-hubspotutk-cookie-in-your-outgrow-content
18. https://cookiedatabase.org/cookie/facebook/_fbp/
19. https://chrome.google.com/webstore/detail/retirejs/moibopkbhjceeedibkbkbchbjnkadmom?hl=en
20. https://service.maxymiser.net/cdn/lufthansa/cookie_optout_en.htm?redirect=1&optout=1
21. https://www.united.com/ual/en/us/fly/privacy.html#targeted_advertising
22. https://www.united.com/ual/en/us/fly/privacy.html#use_of_cookies