Web Audit: Penn-Testing

Wagwalking uses many different cookies for monitoring its users. Some of these cookies are from ad services, and they track the user's movement throughout the website. Others are there for pulling and posting different kinds of data, such as images. [10][11]These cookies come from greater APIs, such as Google Analytics API, Branch API, and Relic Spa API. [12][14][15] Cookies from WagWalking's own OPS API, the new Relic API, and the Mixpanel API are set to expire in 2-3 days. The expiration times for the advertising cookies from Facebook, Google and the other big name companies range from a few days to a whole year, with JS.stripe cookies set to expire all the way in 2022. Most of the cookies identified are persistent cookies that eventually expire. The only session cookies found were from Mixpanel. When signing up, something that caught our attention was the Prod API cookie, which sent WagWalking data about the user's dogs and personal information. It has a three-day lifespan, but underneath a label named "access-control-allow-header," there was an allowed label of CSRF-Token, so theoretically it could be possible to use this [19] OPS API cookie to gain access to their cloudflare server, which stores all the site's images and account information, within a certain amount of time.

Ads are additionally shown to the user with cookies. There were ads found from Google, Pinterest, Bing and Facebook. Each company had its ow
n server for their cookies. Google's server was named "café," and Amazon's server to receive data was simply named "server". [17][18] Wagwalking has incorporated sql zeotap API and samplicio API to send data to amazon servers, which sorts data with demographics. While looking into wagwalking's google ads, we also found an API called fountain API which is associated with cloudflare and stores users' information when they sign up to become a dog walker. Moreover, adding on to our findings, google ads had a request URL in javascript that pulled requests from inside google chrome's extension page, chrome://extensions. These advertisements can learn anything from the information you put into the forms in WagWalking's site. All of the website's Urls are protected with HTTPS, these Request URLs are mainly used for the associated API application.

There weren’t many signs of mixed HTTP/HTTPS content in WagWalking’s website. However, in their signup page (https://app.wagwalking.com/signup/welcome), we found that there is a svg element (a tag in html) with an attribute “xmlns” that refers to http://www.w3.org/2000/svg. If this creates a HTTP request, the information security of WagWalking would be undermined. A man in the middle attacker could easily read or even rewrite the response to insert malicious Javascript code. This could result in sensitive user information being read or altered.[1] To find out if WagWalking was actually making HTTP requests via their svg tag, we inspected the network requests made by wagwalking using Chrome debugger while refreshing the page. It turns out that there was no HTTP request emitted by WagWalking. Additionally, the URL in xmlns attribute is referring to the XML namespace which is a trusted site.[2][3] Therefore, WagWalking is safe from mixed HTTP/HTTPS security issues.

There are many tracking pixels on WagWalking’s website. The most identifiable tracking pixels were Facebook’s and Microsoft’s tracking pixel (bat.bing.com). Having a tracking pixel can jeopardize user’s information security by gathering and analyzing the following sensitive data: (1) operating system used; (2) type of website or email used; (3) type of client used; (4) client’s screen resolution; (5) time and email was read or website was visited; (6) activities on the website during a session; (7) IP address.[4] Although WagWalking explained in their Private Policy possible actions users could take regarding the gathering of their data, an option to refuse being tracked via these tracking pixels didn’t seem to be one of them.[5] Facebook’s tracking pixel uses Facebook cookies to map WagWalking users with their Facebook account in order to track advertising-related actions of users.[6] Microsoft’s online conversions tracking is similar. It registers users’ destination URL, duration, pages viewed per visit and custom events, and analyzes those data to help develop a personalized advertising campaign.[7] WagWalking can use this information to improve their advertising strategy.

According to their private policy, WagWalking collects the user's info if they do any of the following actions: register for an account, request service from a Pet Care Provider, contact a Pet Owner looking for a Pet Care Provider, fill out forms, sign up for promotions, request help from customer service, or communicate with WagWalking or other users with WagWalking services. The info that WagWalking collects involves the user’s name, email address, phone number, and address. The user may also grant WagWalking permission to access the user’s address book on their phone. If such permission is granted, WagWalking would store on their servers all of the user’s contacts and their associated phone numbers. WagWalking also collects financial information such as credit card numbers and location information when the user uses their services. If the user sends text messages to a Pet Care Provider using their number available via the services, WagWalking tracks those messages. It collects and stores the date/time of the message, the user’s phone number, and the content of the text message.

If the user accesses the services of WagWalking through a social media account, WagWalking gains access to information stored in that account, including the user’s name, profile picture, gender, networks, user IDs, list of friends, location, date of birth, email address, photos, videos, people they follow and/or who follow them, and/or their posts or "likes."

WagWalking may share its users’ information with business partners or affiliates, i.e. other businesses that integrate WagWalking’s services in their own product. WagWalking assumes no control over third party services’ policies in regards to information collection and storage, so if the affiliate service has a lax privacy policy or weak security, users’ data could be stolen or bought from said affiliate by the ISA. WagWalking complies with the GDPR by outlining in their Private Policy certain rights users have. These rights include the right to edit and/or delete user information once provided to them, the ability to unsubscribe from their mailing list, the right to opt out of cookie and analytics processing, and some other rights granted to Nevada or California residents. WagWalking points out that some requests to this end may be rejected because the information in question may be needed for their “legitimate interests” or for a legal obligation.

Wagwalking uses js.stripe API for online payment. They would use the js.stripe API to tokenize the customer payment information[13]. They also use Node.js to monitor their site and to confirm customer payments/transactions[16]. The form that allows a user to input information about their dog comes with a CSRF Token. This is found in the response header for said form.

Wagwalking's login and password flow applies some attack-proof strategy. When signing up for this website, the system rejects any common password or passwords can be easily decrypted. The process of logging in to WagWalking is discrete, that is to say, the website makes their user submit login information on separate pages instead of all at once—the user inputs their email address and has to hit submit before they can input their password. After the user submits their email and password for login, WagWalking calls on cloudflare and sends a session cookie to cloudflare's server which contains a one-way hashed IP address of the user. According to cloudflare, this information is for detecting malicious visitors of the website. This communication is performed through HTTPS requests. However, the cookie value containing users' IP address is stored in cloudflare's server for up to 7 days.[8] This can be a possible security or privacy issue. It is reasonable for WagWalking to use cloudflare's service to prevent attackers from attacking their servers, but if cloudflare is only checking for whether the user is malicious, they shouldn't need to store the user's IP address, at least not for seven days. Thus, it is possible that this action is a violation of user privacy.

Citations:

[1] - https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content
[2] - https://www.w3.org/2007/xmlsec/ws/papers/09-lockhart-bea/
[3] - https://stackoverflow.com/questions/25450600/what-does-the-svg-xmlns-attribute-do
[4] - https://en.ryte.com/wiki/Tracking_Pixel
[5] - https://safety.wagwalking.com/privacy

[6] - https://developers.facebook.com/docs/facebook-pixel/implementation/
[7] - https://about.ads.microsoft.com/en-us/solutions/ad-products/conversion-tracking
[8] - https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies
[9] - https://theconversation.com/what-does-gdpr-mean-for-me-an-explainer-96630
[10] - https://www.facebook.com/business/help/742478679120153#:~:text=The%20Facebook%20pixel%20is%20an,shown%20to%20the%20right%20people.
[11] - https://support.google.com/google-ads/answer/6331314?hl=en
[12] - https://developer.mixpanel.com/docs/javascript-full-api-reference
[13] - https://stripe.com/docs/js
[14] - https://discuss.newrelic.com/t/relic-solution-what-is-bam-nr-data-net-new-relic-browser-monitoring/42055
[15] - https://docs.newrelic.com/docs/browser/browser-monitoring/browser-agent-spa-api
[16] - https://docs.newrelic.com/docs/apm/transactions/transaction-traces/introduction-transaction-traces
[17] - https://medium.com/@zeotapstories/growing-a-data-billionaire-aws-redshift-dca4ba38a280
[18] - https://developer.lucidhq.com/#introduction
[19] - https://prod-ops-api.wagwalking.com/api/v5/owner/signup/services
[20] - https://s.pinimg.com/ct/lib/main.2424edb5.js
[21] - https://branch.io/glossary/api/
[22] - https://recruitis.io/#uvod
[23] - https://stackoverflow.com/questions/41729774/what-are-consequences-of-mixpanel-token-being-exposed
[24] - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy