

Team: Heriberto Varela, Rongda Kang, Kevin Guo, Minglan Zheng

Robinhood is an investing and trading application. In this report, we will be auditing their main website and other relevant domains looking for vulnerabilities. At first glance, Robinhood utilizes good web security practices: it sends all connections over HTTPS and has a DigiCert SHA2 certification. Our analysis includes various interesting findings and some security concerns. We will be exploring these aspects in sections for clarity.

1. Cookies

We have two points to share about Robinhood and its cookies. First, Robinhood uses cookies without HttpOnly flag or secure flag or both to store sensitive information. In particular, the `log_in` cookie, which stores a boolean value indicating the user's login state, has a two year lifetime and is not set secure nor HTTP-only.

Secondly, we find cookies provided by Facebook, Twitter, Snapchat, Google that analyze user interaction with the Robinhood site and gain insights for advertising. Cookies from these four companies are across the Robinhood site, on pages including transfer and banking. Robinhood uses first-party cookies to bypass a user's privacy preferences. To count a few pieces of evidence of first-party cookie syncing [1]:

(1) `_fbp` is a Facebook first-party cookie for targeting and advertising [16].

(2) `_sctr` is used by Snapchat to determine whether a third-party tag will be called in Snap Ads Pixel [2].

Furthermore, some Robinhood subdomains employ third-party cookies that are relative to its featured content. For example, LinkedIn drops third-party cookies such as `UserMatchHistory`, `lang`, `li_sugar`, `personalized_id` on the Robinhood career subdomain. These LinkedIn cookies store user's information and have a life of 1-3 months [2]. Please see the **Appendix I** for a partial list of cookies.

2. Ads & HTTPS

Robinhood shows no sponsored ads, rather, it features articles that can be categorized into two types: external sites, and articles hosted in a Robinhood-related domain.

Articles that redirect to external connections are done so via HTTPS and its hyperlink contains a 'noopener' tag. These tags prevent the new page from being able to access the `window.opener` property, i.e. it prevents malicious javascript that wants access to the site that opened it. [3] Robinhood improves its security by properly setting HTTP headers. HSTS is set to redirect any HTTP request to HTTPS for the target domain, X-Frame-Options is set to protect against clickjacking attacks. [10] See Appendix II for Robinhood's practice over HTTP secure headers.

For articles that are hosted on the Robinhood subdomains [11], only a few contain sponsored content. For instance, “Get 2 months of a WSJ subscription for \$1” link, redirects the user to a third party-domain (store.wsj.com) via HTTPS. We noticed that these redirecting URLs use trackingCode and cid as parameters. These parameters are used to monitor a deployed marketing campaign, which in this case is monitored via Adobe Analytics [5].

3. Tracking Pixels

We also want to address that there is the possibility of advertisers obtaining user information via Google Analytics. Tracking pixels provided by Google Analytics are requested by a form on several important pages [6]. Reference [7] is an example of this 1x1 pixel. These tracking pixels can share user info such as the OS used, the type of website and client visited, the time the page was loaded, and different activities on the website done by the user [8]. As per Robinhood's privacy policy, all of this information can be shared, in addition to the user common identifier that allows for cross-device recognition by other services mentioned before.

4. Log in

When a user logs in, Robinhood uses the OAuth2 ROP flow to carry out a Password grant. The client (Robinhood) needs to collect the user's credentials (i.e. password, client_id, device_token) and send it to the authentication server in exchange for an access token. Although Robinhood's server sends this request over HTTPS, and no third-party is involved, this process is not safe and disallowed by the latest OAuth 2.0.[9] The reason originates from the fact that user credentials have been exposed to the client application, see **Appendix V**. This implies that if the client application is compromised, the attacker can manipulate the user's entire account.

5. User Input

Robinhood has some flaws in validating user input values into its forms. For instance, **Appendix III** shows a newsletter registration form and its HTML code. In this form, the input needs to end with an email extension. However, the system does not validate it through 2-step authentication, which implies that an attacker can exploit the form by entering someone else's email address.

6. Sub Sources/Off Site URL/Loaded Plugins

Robinhood loads more than 20 third-party sub sources across its different sites. A partial list of these image, style sheets, JavaScript, web fonts, and video source file are explained in **Appendix IV**.

We observed that Robinhood is inconsistent with employing subresource integrity. In image 1 of Appendix IV, the ‘integrity’ attribute is set with a

base64-encoded sha384 string. In contrast, the <script> element in image 2 does not tell the browser to first verify with an expected hash before loading the script. Based on our analysis, Robinhood potentially made this decision because script integrity is not compatible with browsers such as Internet Explorer and Safari on iOS.

There is a facebook plugin loaded in on Robinhood.com that is for redirecting users to the Robinhood facebook profile.

7.Privacy Policy & Violation

According to the Privacy policy [12], they collect location data; usage and device data; third-party data including account linking, third-party services, and publicly available data. As Robinhood states in disclosures of personal information, “We do not sell or rent your personal information to third parties, aside from substantial corporate transactions”. The second half of this statement leaves the doors for selling order data of high-frequency traders to other financial firms, as reported in many sources in 2019 [13]. Nevertheless, the policy addresses that all the transactions between data should be consent by the user and it includes a Customer agreement [14].

Also stated in the policy, Robinhood utilizes Google Analytics to track user interaction with the site. This tracking can include a common account identifier and hashed user data for cross-device identification. Combining this statement with the evidence of cookies and plugins, we suspect that Robinhood also has similar contracts with other parties, such as Facebook, Twitter, and LinkedIn. In the aspect of Privacy Policy, the ISA has two possible ways if they eavesdrop or buy data from Robinhood, if ISA is able to find target information for Robinhood, Robinhood could share user data if they make a contract. Secondly, Robinhood's substantial third party has a contractual relationship with ISA.

8.GDPR Compliance

Robinhood's GDPR compliance status is unknown. However, according to the GDPR tracker, Robinhood fulfills some of the GDPR principles. [15] **General Data Protection Regulation (GDPR)** is a regulation on data protection and privacy. We think Robinhood partly complies with GDPR mainly because it provides a customer agreement. This agreement is well-formatted and contractual on the data subject, especially when the subject is underage. However, Robinhood does not regulate the practice of authorized third parties on its user. These implications could be the reason behind why Robinhood is not legitimately certified for GDPR.

Appendix I. Cookie Chart

Yellow - on blog.robinhood.com, **Green** - on career.robinhood.com

Domain	Name	HTTP-only	Secure	Long life (yr)
sc-static.net	X-AB		x	
snapchat.com	sc_at		x	1
facebook.com	dpr, datr, sb, fr, wd	sb, fr, datr	x	max 2
youtube.com	LOGIN_INFO	x	x	2
	YSC	x	x	Session
	VISITOR_INFO1_LIVE	x	x	2
doubleclick.net	IDE (Google)	x	x	2
twitter.com	twitter_sess	x	x	Session
	personalization_id		x	
ads.linkedin.com	lang		x	Session
robinhood.com	logged_in			
	device_id		x	10
	is_in_beta			
	_fbp (facebook)			1
	_sctr, _scid (snapchat)			
	_ga_au (Google analytics)			
blog.robinhood.com	_sctr (snapchat)			
	crumb			Session

linkedin.com	li_sugr, lang, UserMatchHistory		x	30-90 days
--------------	---------------------------------	--	---	------------

Appendix II. HTTP secure headers

Name	Value	Purpose
X-XSS-Protection	1; mode=block	Controls Cross-Site Scripting (XSS) filters built into the majority of web browsers.
X-Frame-Options	deny	Robinhood.com can't be embedded in an iframe by another website.
Referrer-Policy	strict-origin-when-cross-origin	Only reveal complete referrer information (including the URL) for same-origin requests
Strict-Transport-Security	max-age=31536000	Enforces HTTPS connection

Appendix III. User Input Validation

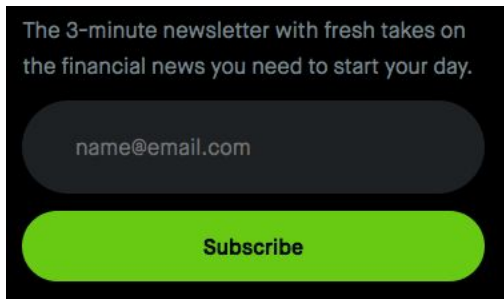
A dark-themed newsletter sign-up form. At the top, it says "The 3-minute newsletter with fresh takes on the financial news you need to start your day." Below this is a dark rounded rectangular input field containing the placeholder text "name@email.com". Underneath the input field is a bright green rounded rectangular button with the word "Subscribe" in white text.

Image 1. Newsletter RSVP form on Robinhood.com

```
<form class="css-1emd6gn-EntryForm">
  <div class="css-45u70t-EntryForm">
    <input type="email" placeholder="name@email.com" required value class="css-12uwfyf-EntryForm">
  </div>
  <div class="css-18cy2vl-EntryForm">
    <button type="submit" class="css-fkqzh0-UnstyledButton">...</button>
  </div>
</form>
```

Image 2. HTML code for Image 1

Appendix IV.

Purpose	
tracking	tr.snapchat.com, tr.facebook.com, fbevents.js
	https://sc-static.net/js-sha256-v1.min.js https://sc-static.net/scevent.min.js
	https://connect.facebook.net/signals/config/1887010164928006?v=2.9.27&r=stable
Google analytics is a website analytics service that tracks and reports website traffic, which can be useful in measuring the popularity of Robinhood and how effective it is at marketing its product around social media and the web.	https://www.google-analytics.com/analytics.js
Google tag manager helps smooth out the process of running google analytics.	https://www.googletagmanager.com/gtm.js?id=GTM-5Q7W7D3

This twitter url is for an iframe that allows twitter to appear as a cohesive webpage to Robinhood.	https://platform.twitter.com/widgets.js
	https://itstillworks.com/embed-twitter-iframe-32896.html

```
<script async src="https://sc-static.net/js-sha256-v1.min.js" integrity="sha384-W4RqaNUbvBdTRc41QQAWDcd2aX9wGruak2WnLXwyjVAlhi56zatCk4e/RSqrAg6" crossorigin="anonymous"></script>
```

Image 1. <script> element with integrity attribute

```
<script type="text/javascript" async src="https://sc-static.net/scevent.min.js"></script>
<script src="https://connect.facebook.net/signals/config/1887010164928006?v=2.9.27&r=stable" async></script>
<script src="https://connect.facebook.net/signals/plugins/identity.js?v=2.9.27" async></script>
<script type="text/javascript" async src="https://connect.facebook.net/en_US/fbevents.js"></script>
<script async src="https://www.google-analytics.com/analytics.js"></script>
<script async src="https://www.googletagmanager.com/gtm.js?id=GTM-5Q7W7D3"></script>
```

Image 2. <script> element without integrity attribute

Appendix V. Password Grant

Verification Code 🔒

To continue, please enter the verification code we sent to your email address.

[Text me instead](#)

[Resend Code](#)

The screenshot shows a web browser interface on the left and a network inspector on the right. The browser displays a 'Verification Code' screen with a text input field containing '000000' and buttons for 'Back', 'Confirm', and 'Resend Code'. The network inspector shows a POST request to the path '/oauth2/token/' with the following headers: 'accept: */*', 'accept-encoding: gzip, deflate, br', 'accept-language: en-US,en;q=0.9', 'content-length: 232', 'content-type: application/json', 'origin: https://robinhood.com', 'referrer: https://robinhood.com/', 'sec-fetch-dest: empty', 'sec-fetch-mode: cors', 'sec-fetch-site: same-site', 'user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36', and 'x-robinhood-api-version: 1.411.9'. The request payload is a JSON object: {'grant_type': 'password', 'scope': 'internal', 'client_id': '...', 'device_token': '...', 'expires_in': 86400, 'password': '...', 'scope': 'internal', 'username': '...'}. The password field is redacted with a black box.

References

- [1]<https://freedom-to-tinker.com/2014/08/07/the-hidden-perils-of-cookie-syncing/>
- [2]<https://www.linkedin.com/legal/cookie-table>
- [3] https://developer.mozilla.org/en-US/docs/Web/HTML/Link_types
- [4]<https://cdn.robinhood.com/assets/robinhood/legal/RHFPrivacy.pdf#page=6&zoom=100,72,826>
- [5]
<https://docs.adobe.com/content/help/en/analytics/components/dimensions/tracking-code.html>
- [6] <https://www.google-analytics.com/collect>
- [7]<https://www.google.com/ads/ga-audiences?t=sr&aip=1&r=4&slfrd=1&v=1&v=j86&tid=UA-46330882-9&cid=019845cd-2ffa-4a91-b9fd-75f7b3704d00&jid=154513365&u=SKCAgAABAAAAAE~&z=519858882>
- [8] https://en.ryte.com/wiki/Tracking_Pixel#How_does_a_tracking_pixel_work
- [9] <https://oauth.net/2/grant-types/password/#:~:text=The,>
<https://tools.ietf.org/html/draft-ietf-oauth-security-topics-13#section-3.4,>
<https://auth0.com/docs/flows/call-your-api-using-resource-owner-password-flow>
- [10] <https://www.netsparker.com/blog/web-security/http-security-headers/>
- [11] [newsfeed-images.robinhood](#) and robinhood.com/news
- [12]<https://cdn.robinhood.com/assets/robinhood/legal/RHF%20Privacy.pdf>
- [13]<https://www.cnn.com/2019/04/18/a-controversial-part-of-robinhoods-business-tripled-in-sales-thanks-to-high-frequency-trading-firms.html>
- [14][https://cdn.robinhood.com/assets/robinhood/legal/Robinhood%20Customer%20Agreement%20\(June%2022\)%20\(1\).pdf](https://cdn.robinhood.com/assets/robinhood/legal/Robinhood%20Customer%20Agreement%20(June%2022)%20(1).pdf)
- [15]<https://gdprtracker.io/compliance/robinhood/>
- [16]<https://cookiedatabase.org/cookie/facebook/fbp/>

People discussed the project with (outside group): Professor Sharon Goldberg, Yuval Marcus

Video:

<https://drive.google.com/file/d/1Vp4dLQWk2gDRlr5lJjLMi7Rjc6z8uxUA/view?usp=sharing>