Railway's "Bug Bounty Program" (aka, the "Program")

We recognize the important role that security researchers and our user community play in helping to keep Railway, Inc. ("Railway") and our users secure. If you have discovered a site or product vulnerability, you may be eligible, subject to Railway's sole discretion and your agreement to the terms below, to a monetary award in accordance with the terms and conditions set forth below (the "Program Terms")

If an issue is it is not explicitly "Out of Scope" and there is a security impact, we want to know about it. Issues without security impact that are submitted to our program will be closed. Please review the program's "Out of Scope" section and all other policies before submitting a report.

Your participation in the Program is voluntary. Before finding and reporting any vulnerabilities or other suggestion or feedback (a "Submission") to Railway you acknowledge that you have read and agree to the Program Terms. In these terms, references to "you" or "researcher" refer to a researcher that submits a high quality report in accordance with the Program Terms and "we" or "us" refers to Railway.

These Program Terms supplement the Railway Terms of Service and Privacy Policy available at https://railway.app/, and any other agreement in which you have entered with Railway (collectively "Railway Agreements"). The terms of those Railway Agreements will apply to your use of, and participation in, the Bug Bounty Program as if fully set forth herein. If any inconsistency exists between the terms of the Railway Agreements and these Program Terms, these Program Terms will control, but only with regard to the Bug Bounty Program. We may revise and update these Program Terms from time to time in our sole discretion. All changes are effective immediately when we post them to this website. You are expected to check this page from time to time so you are aware of any changes.

Table of Contents

I. Program Terms

1. Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted in compliance of this policy, we will make it known that your actions were conducted in compliance with this policy. Railway reserves all legal rights in the event of noncompliance with this policy.

2. Program Eligibility

To be eligible to participate in the Program, you must:

- Be at least 16 years of age. If you are at least 16 years old, but are considered a minor in your place of residence, you must get your parent's or legal guardian's permission prior to participating in the program.
- Not be employed by Railway or any of its affiliates or an immediate family member of a person employed by Railway or any of its affiliates.
- Not be a resident of, or make Submissions from, a country against which the United States has issued export sanctions or other trade restrictions and not otherwise be an embargoed or restricted person.

- Not be in violation of any national, state, or local law or regulation with respect to any activities directly or indirectly related to the Program.

If (i) you do not meet the eligibility requirements above; (ii) you breach any of these Program Terms or any other agreements you have with Railway or its affiliates; or (iii) we determine that your participation in the Program could adversely impact us, our affiliates or any of our users, employees or agents, we, in our sole discretion, may remove you from the Program and disqualify you from receiving any benefit of the Program.

3. Program Rules

Do:

- Do abide by these Program Terms.
- Do respect privacy & make a good faith effort not to access, process or destroy personal data.
- Do be patient & make a good faith effort to provide clarifications to any questions we may have about your report.
- Do be respectful when interacting with our team, and our team will do the same.
- Do perform testing only using accounts that are your own personal/test accounts.
- Do exercise caution when testing to avoid negative impact to customers and the services they depend on.
- Do stop whenever unsure. If you think you may cause, or have caused, damage with testing a vulnerability, report your initial finding(s) and request authorization to continue testing.

Do NOT:

- Do not leave any system in a more vulnerable state than you found it.
- Do not brute force credentials or guess credentials to gain access to systems.
- Do not participate in denial of service attacks.
- Do not upload shells or create a backdoor of any kind.
- Do not publicly disclose a vulnerability without our explicit review and consent.
- Do not engage in any form of social engineering of Railway employees, customers, affiliates or partners.
- Do not engage or target any Railway employee, customer, or partner during your testing.
- Do not attempt to extract, download, or otherwise exfiltrate data that may have Personal Identifiable Information or other sensitive data other than your own.
- Do not change passwords of any account that is not yours or that you do not have explicit permission to change. If ever prompted to change a password of an account you did not register yourself or an account that was not provided to you, stop and report the finding immediately.
- Do not do anything that would be considered a privacy violation, cause destruction of data, or interrupt or degrade our service.
- Do not interact with accounts you do not own.

4. Disclosure Policy and Confidentiality

Any data you receive, obtain access to or collect about Railway, Railway affiliates or any Railway users, customers, employees or agents (or any of their businesses, products, systems, strategies or technologies) in connection with the Program (including, without limitation, your

submissions and the vulnerabilities they report) is considered Railway's confidential information ("Confidential Information"). Confidential Information must be kept confidential and only used: (i) to make the disclosure to Railway under the Program; or (ii) to provide any additional information that may be required by Railway in relation to the submitted report. No further use or exploitation or disclosure of Confidential Information is allowed. Upon Railway's request, you will permanently erase all Confidential Information for any systems and devices. You may not use, disclose or distribute any such Confidential Information in any way, including without limitation any information regarding your submitted report, without our explicit prior written consent. To request such consent, you must submit a disclosure request to our Program. Please note, not all requests for public disclosure will be approved. Any unauthorized public disclosure will result in immediate disqualification from the Program and ineligibility for receiving Bounty Payments, in addition to all other remedies we may have.

5. Legal

Railway reserves the right to modify the terms and conditions of this program, and your participation in the Program constitutes acceptance of all terms. By making a Submission, you represent and warrant that the Submission is original to you and you have the right to submit the Submission. By making a Submission, you give us the right to use, distribute and take any other action with respect to your Submission for any purpose. Please check this site regularly as we routinely update our program terms and eligibility, which are effective upon posting. You can subscribe to receive email notifications when this policy is updated.

II. Submitting Reports

1. Report Quality

High quality submissions allow our team to understand the issue better and engage the appropriate teams to fix them. The best reports provide enough actionable information to verify and validate the issue without requiring any follow up questions for more information or clarification. We recommend you provide enough information to (i) outline the bug; (ii) reproduce the bug; (iii) assess the coverage the bug applies to; and (iv) provide additional related logs or information. Valid and accepted vulnerabilities would be the type of report that identifies a unique security impact on the Program's specific scope. Not all high quality reports look the same, but many share these common features:

- Detailed descriptions of your discovery with clear, concise, reproducible steps or a working proof-of-concept (POC). If you do not explain the vulnerability in detail, there may be significant delays in the process, which is undesirable for everyone.
- Screenshots and/or videos can sometimes assist security teams in reproducing your issue. Most teams prefer written reproduction steps, but screenshots and videos can be used to augment your report and make it easier for security teams to quickly understand the issue you're reporting.
- The impact of the vulnerability; if this bug were exploited, what could happen? Security teams need to file bugs internally and get resources to fix these issues. Describing why the issue is important can assist in quickly understanding the impact of the issue and help prioritize response and remediation.
- Check the scope page before you begin writing your report to ensure the issue you are reporting is in scope for the program.

- Think through the attack scenario and exploitability of the vulnerability and provide as many clear details as possible for our team to reproduce the issue (include screenshots if possible).
- Please include your understanding of the security impact of the issue. Our bounty payouts are directly tied to security impact, so the more detail you can provide, the better. We cannot payout after the fact if we don't have evidence and a mutual understanding of security impact.
- In some cases, it may not be possible to have all of the context on the impact of a bug. If you're unsure of the direct impact, but feel you may have found something interesting, feel free to submit a detailed report and ask.
- Video only proof-of-concepts (PoCs) will not be considered.
- A vulnerability must be verifiable and reproducible for us to be considered in-scope.
- All reports must demonstrate security impact to be considered for bounty reward.
- Submissions must be made via email and sent to bugbounty@railway.app

2. Out-of-Scope

If you have found a vulnerability on the Railway website that is not identified as Out of Scope in the list below, please submit a report for triage and review.

- Physical or social engineering attempts (this includes phishing attacks against Railway employees)
- Ability to send push notifications/SMS messages/emails without the ability to change content
- Ability to take over social media pages (Twitter, Facebook, LinkedIn, etc)
- Negligible security impact
- Unchained open redirects
- Reports that state that software is out of date/vulnerable without a proof-of-concept
- Highly speculative reports about theoretical damage
- Vulnerabilities as reported by automated tools without additional analysis as to how they're an issue
- Reports from automated web vulnerability scanners (Acunetix, Vega, etc.) that have not been validated
- SSL/TLS scan reports (this means output from sites such as SSL Labs)
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- CSV injection
- Best practices concerns
- Protocol mismatch
- Rate limiting
- Dangling IPs
- Vulnerabilities that cannot be used to exploit other users or Railway -- e.g. self-xss or having a user paste JavaScript into the browser console
- Missing cookie flags on non-authentication cookies
- Reports that affect only outdated user agents or - we only consider exploits in the latest browser versions for Safari, FireFox, Chrome, Edge, IE
- Issues that require physical access to a victim's computer/device
- Path disclosure
- Banner grabbing issues (figuring out what web server we use, etc.)

- If a site is abiding by the privacy policy, there is no vulnerability.
- Enumeration/account oracles
- Account oracles -- the ability to submit a phone number, email, UUID and receive back a message indicating a Railway account exists
- Distributed denial of service attacks (DDOS)

III. Bounty Awards

1. Pay At Triage

We strive to reward valid reports within 30 days of acceptance, often sooner. Bounty rewards will be calculated according to CVSS 3.1 as applicable. The official CVSS 3.1 reference used by our program is: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. At our discretion as Program owners, some report types will not receive rewards based on CVSS 3.1 score. These reports will receive either a fixed amount reward or the reward will be determined on a case-by-case basis. See Section 2 below.

2. CVSS Scoring Exceptions

The report types listed below will receive rewards without calculating a CVSS 3.1 score (Railway may add to the list below at any time in its discretion, including after you make your submission):

Type	Reward
Subdomain Takeover	$500
3rd Party Info Disclosures (Prezi, Trello, Google Doc, etc)	Case by case

3. Additional Reward Policies

You may be eligible to receive a monetary reward ("Bounty Payment") if and only if: (i) you are the first person to submit a site or product vulnerability and your submission is of high quality; (ii) that vulnerability is determined to be a valid security issue by Railway; and (iii) you have complied with all Program Terms. All Bounty Payments shall be considered gratuitous. All Bounty Payments will be made in United States dollars (USD). You will be responsible for any tax implications related to Bounty Payments you receive, as determined by the laws of your jurisdiction of residence or citizenship; if Railway becomes aware any tax reporting or withholding requirements related to your Bounty Payment or believes that any such requirements may apply, Railway is entitled file such reports and withhold any applicable amounts from your Bounty Payments and to defer payment to you until you have provided any information necessary to allow Railway to comply with such requirements. Railway will determine all Bounty Payments in consideration of the risk and impact of the vulnerability. Railway retains the right to determine if the bug submitted to the Bug Bounty Program is eligible. All determinations as to the amount of a bounty made by Railway are final. Bounty Payment ranges are based on the classification and sensitivity of the data impacted, ease of exploit and overall risk to Railway and its customers. Previous bounty amounts are not considered a precedent for future bounty amounts. Bounty awards are not additive and are subject to change as our internal environment evolves. We determine the upper bound for security impact and award based on that impact. When determining bounty amounts, we consider the security impact of any given issue --

things that influence security impact are the scale of exposure and the various mitigating and multiplying factors. Bounty payouts and amounts, if any, will be determined by us in our sole discretion. In no event are we obligated to provide a payout for any Submission. The format and timing of all bounty payouts shall be determined by us in our sole discretion. If we receive several reports for the same issue, only the earliest valid report that meets requirements and provides enough actionable information to identify the issue may be considered for a bounty.

Date: August ___, 2022.
View Changes: