Onramp Defect Disclosure Program

Onramp Invest looks forward to working with the security community to identify security vulnerabilities in order to keep our businesses and customers safe. At Onramp Invest, we welcome contributions from security researchers to help us build and secure our products. If you have discovered a vulnerability, please submit a report directly to Onramp Invest (defectdisclosure@onrampinvest.com). Onramp Invest will investigate all valid reports and get back to you in a timely manner. Please read this policy prior to filing a report to Onramp Invest. By making a submission or otherwise participating in this program, you acknowledge your agreement to the terms of this policy.

Response Targets

Onramp Invest will make a best effort to meet the following response targets for researchers participating in our program:

- Time to first response (from report submit) - 5 business days
- Time to triage (from report submit) - 10 business days
- Time to mitigation – dependent on severity

Scope

In scope projects:

- advisor.onrampinvest.com

Disclosure Policy & Disclosure Requirements

As this is a private program, please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from Onramp Invest.

Complying with our safe harbor policy requires researchers to adhere to our Disclosure policies and processes. Disclosure requires that researchers abide by the following requirements:

- Share a detailed report that includes all information as it relates to the vulnerability. That report should be sent to defectdisclosure@onrampinvest.com
- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact
- Social engineering (e.g. phishing, vishing, smishing) is prohibited
- Do not access or modify our data or our users' data without explicit permission. Only interact with your own accounts or test accounts for security research purposes
- Do not profit from or allow another party to profit from a vulnerability
- Do not defraud Onramp Invest or its customers in the process of participating in our program

- Act in good faith to avoid privacy violations, destruction of data, and interruption or degradation of our services (including denial of service)
- If you inadvertently caused a privacy violation, or accessed, modified or destroyed any user data, you must disclose this in your report
- Otherwise comply with all applicable laws

Out of scope vulnerabilities

When reporting vulnerabilities, please consider the attack scenario/exploitability and the security impact of the defect. The following issues are considered out of scope for rewards:

- Reports relating to clickjacking on pages with no sensitive actions
- Reports relating to unauthenticated/logout/login CSRF
- Reports relating to attacks requiring MITM or physical access to a user's device
- Reports relating to previously known vulnerable libraries without a working Proof of Concept
- Reports relating to Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Reports relating to missing best practices in SSL/TLS configuration
- Reports relating to any activity that could lead to the disruption of our service (DoS)
- Reports relating to content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Reports relating to email enumeration
- Reports relating to password strength or complexity
- Reports relating to missing security hardening headers
- Reports relating to rate limiting issues
- Reports that target vulnerabilities on outdated or deprecated browsers, open-source libraries, or infrastructure
- Reports from automated tools or scans
- Vulnerabilities that involve physical access to a device
- Vulnerabilities or weaknesses in third party applications that integrate with Onramp Invest
- Social engineering of Onramp Invest employees, contractors, or customers
- Presence/absence of SPF/DMARC/DKIM/CAA records
- Ability to abuse existing banking functionality such as ACH or credit card chargebacks
- Any access to data where the targeted user needs to be operating a rooted or jailbroken mobile device
- Vulnerabilities that have already been reported and/or documented are not eligible for reward

Reward Program

Our current reward program has a minimum of $50 USD and a maximum of $350 USD for agreed upon vulnerabilities that meet the above criteria.

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and legal action will not be initiated against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy. We consider security research and vulnerability disclosure activities conducted in accordance with this policy and the guidelines described to be authorized conduct under the Computer Fraud and Abuse Act and applicable anti-hacking laws.

Thank you for helping keep Onramp Invest and our users safe!