Introduction

Security is core to our values, and we value the input of external security researchers acting in good faith to help us maintain a high standard for the security privacy of our users and systems. This policy sets out our definition of good faith in the context of finding and reporting security vulnerabilities, as well as what you can expect from us in return for your effort, skill, and dedication.

Guidelines

We require that all security researchers to:

- Act in good faith to avoid privacy violations, degradation of our services, disruption to production systems, and destruction of data during security testing (including denial of service);
- Perform research only within the scope set out below;
- Be clear and succinct, a short proof-of-concept link is invaluable;
- Only interact with your own accounts or test accounts for security research purposes. Do not access or modify our data or our users' data, without the explicit permission of the owner; and
- Keep information about any vulnerabilities you've discovered confidential between us until we've had 90 days to resolve the issue.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);
- Recognize your contribution on our Leaderboard, if you are the first to report the issue and we make a code or configuration change based on the issue.

Expectations

When working with us according to this policy, you can expect us to:

- Work with you to understand and validate your report, including a timely initial response to the submission;
- Work to remediate discovered vulnerabilities in a timely manner; and
- Recognize your contribution to improving our security if you are the first to report a unique vulnerability, and your report triggers a code or configuration change.

In-Scope Vulnerabilities

The vulnerabilities listed here are explicitly eligible for our security program. Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include:

- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Authentication or Authorization Flaws
- Server-Side Request Forgery (SSRF)
- Server-Side Template Injection (SSTI)
- XML External Entity (XXE)
- Remote Code Execution (RCE)

While this list represents our primary focus for security research, we are interested in reports for all of our software and dependencies especially if it impacts reasonably sensitive user data.

This can include any open source libraries, software, or third-party components. At our discretion, we will issue rewards for reports not included in the In-Scope Vulnerabilities list.

Out-of-Scope Vulnerabilities

The following are considered out of scope for our security program and will not be rewarded:

- Policies on presence/absence of SPF/DMARC records.
- Password, email and account policies, such as email id verification, reset link expiration, and password complexity.
- Logout Cross-Site Request Forgery.
- Attacks requiring physical access to a user's device.
- Vulnerabilities that require a potential victim to install non-standard software or otherwise take active steps to make themselves be susceptible.
- Social engineering of our employees or clients.
- Any physical attempts against our property or data centers.
- Presence of autocomplete attribute on web forms.
- Missing cookie flags on non-sensitive cookies.
- Any access to data where the targeted user needs to be operating a rooted mobile device.
- Missing security headers which do not lead directly to a vulnerability.
- Host header Injection
- Reports from automated tools or scans that haven't been manually validated.
- Presence of banner or version information unless correlated with a vulnerable version.
- UI and UX bugs and spelling mistakes

Ground Rules

To encourage vulnerability research and to avoid any confusion between legitimate research and malicious attack, we ask that you attempt, in good faith, to:

- Play by the rules. This includes following this policy any other relevant agreements;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;
- Handle the confidentiality of details of any discovered vulnerabilities according to our Disclosure Policy;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research conducted under this policy to be:

- Authorized in view of any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Authorized in view of relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Acceptable Usage Policy that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Fine Print

This is not a competition, but rather an experimental and discretionary rewards program. We may modify the terms of this program, terminate this program at any time, or not pay a reward entirely at our discretion.

We won't apply any changes we make to these program terms retroactively. Reports from individuals who we are prohibited by law from paying are ineligible for bug bounties. You are responsible for paying any taxes associated with bug bounties. Any bug bounties that are unclaimed after 12 months will be donated to a charity of our choosing.

Last update: January 1, 2021