Geo bug bounty program rules and guidelines

As a cloud based SaaS platform, we are proud to be a part of the ITSec and research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a bug bounty program for Geo-owned web properties.

Services in scope

In principle, any Geo-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:

- *.geoworkforcesolutions.com
- *.geoop.com
- *.geoworkforce.io

Bugs in Geo platform and Geo-developed apps (published in Google Play store and in the Apple App Store) will also qualify.

On the flip side, the program has some important exclusions to keep in mind:

- **Third-party websites/services/apps.** Unfortunately, Geo cannot provide reward for any systems not directly owned by us. Should you find vulnerabilities in any of our partners systems, we ask that you contact their security team and seek reward from their bug bounty programs directly.
- **Workable insights.** In order for us to release a bounty, our team must determine the vulnerability is of a legitimate concern. If our team finds the disclosed vulnerability to be inconsequential or otherwise irrelevant, it may not be eligible for a bounty reward. Our team may also request any reasonable assistance on your part in resolving the vulnerabilities in question before processing the bounty.

Qualifying vulnerabilities

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,
- Cross-site request forgery,
- Mixed-content scripts,
- Authentication or authorization flaws,
- Server-side code execution bugs.
- Man-in-the-middle/packet injection attacks

Note that the scope of the program is limited to technical vulnerabilities in Geo-owned mobile apps and web applications; please do not try to sneak into Geo offices, attempt phishing attacks against our employees, and so on.

Out of concern for the availability of our services to all users, please do not attempt to carry out DoS attacks, leverage black hat SEO techniques, spam people, or do other similarly questionable things.

We also discourage the use of any vulnerability testing tools that automatically generate very significant volumes of traffic.

Non-qualifying vulnerabilities

Depending on their impact, some of the reported issues may not qualify. Although we review them on a case-by-case basis, here are some of the common low-risk issues that typically do not earn a monetary reward:

- **Bugs that require exceedingly unlikely user interaction.** For example, a cross-site scripting flaw that requires the victim to manually type in an XSS payload into Geo website and then double-click an error message may realistically not meet the bar.
- **Logout cross-site request forgery.** For better or worse, the design of HTTP cookies means that no single website can prevent its users from being logged out; consequently, application-specific ways of achieving this goal will likely not qualify.
- **Flaws affecting the users of out-of-date browsers and plugins.** The security model of the web is being constantly fine-tuned. We will typically not reward any problems that affect only the users of outdated or unpatched browsers. In particular, we exclude Internet Explorer prior to version 9.
- **Presence of banner or version information.** Version information does not, by itself, expose the service to attacks - so we do not consider this to be a bug. That said, if you find outdated software and have good reasons to suspect that it poses a well-defined security risk, please let us know.

Monetary rewards aside, vulnerability reporters who work with us to resolve security bugs in our products are a valuable part of the internet's ecosystem and we acknowledge and thank you for your contribution.

Reward amounts for security vulnerabilities

As a small startup, our bug bounty program can't match the likes of Google or Facebook, but we also believe it is important to reward those individuals who do the right thing and try to make the world a better place. As such, rewards for qualifying bugs range from Geo branded Swag, to up to $100. The following table outlines the usual rewards chosen for the most common classes of bugs, though each submission is qualified on a case by case basis. Please also note, as we are a New Zealand based company, all amounts are in New Zealand Dollars (NZD). The bounties listed below are awarded per report, rather than individual exploit.

Category	Examples	Geo Web Platform (console)	Geo Mobile Apps	Geo Backend/ Database	Other
Vulnerabilities giving direct access to Geo servers					

Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$100	$100	$100	Up to $100
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$50	$50	$100	Up to $100
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$50	$50	$50	Up to $100
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile / Hardware: *Code execution*	$50	$50	$50	Up to $100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile / Hardware: *Information leak, privilege escalation*	$25	$25	$25	Swag

Investigating and reporting bugs

When investigating a vulnerability, please, only ever target your own accounts. Never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to your fellow users or to Geo.

Visit Google's Bug Hunter University articles to learn more about sending good vulnerability reports.

If you have found a vulnerability, please contact us at support@geoop.com.

Note that we are only able to answer to technical vulnerability reports. Non-security bugs and queries about problems with your account should be instead directed to the live chat built into your Geo accounts help section.

Frequently asked questions

Q: What if I found a vulnerability, but I don't know how to exploit it?

A: We expect that vulnerability reports sent to us have a valid attack scenario to qualify for a reward, and we consider it as a critical step when doing vulnerability research. Reward amounts are decided based on the maximum impact of the vulnerability, and Geo is willing to reconsider a reward amount, based on new information (such as a chain of bugs, or a revised attack scenario).

Q: How do I demonstrate the severity of the bug if I'm not supposed to snoop around?

A: Please submit your report as soon as you have discovered a potential security issue. Geo will consider the maximum impact and will choose the reward accordingly. We routinely pay rewards for otherwise well-written and useful submissions where the reporter didn't notice or couldn't fully analyze the impact of a particular flaw.

Q: I found an outdated software (e.g. Apache or Wordpress). Does this qualify for a reward?

A: Please perform due diligence: confirm that the discovered software had any noteworthy vulnerabilities, and explain why you suspect that these features may be exposed and may pose a risk in our specific use. Reports that do not include this information will typically not qualify.

Q: Who determines whether my report is eligible for a reward?

A: The reward panel consists of various members of the Geo Team.

Q: What happens if I disclose the bug publicly before you had a chance to fix it?

A: In essence, our pledge to you is to respond promptly and fix bugs in a sensible timeframe - and in exchange, we ask for a reasonable advance notice. Reports that go against this principle will usually not qualify, but we will evaluate them on a case-by-case basis.

Q: My report has not been resolved within the first week of submission. Why hasn't it been resolved yet?

A: Reports that deal with potential abuse-related vulnerabilities may take longer to assess, because reviewing our current defense mechanisms requires investigating how a real life attack would take place and reviewing the impact and likelihood requires studying the type of motivations and incentives of abusers of the submitted attack scenario against one of our products.

Q: I wish to report an issue through a vulnerability broker. Will my report still qualify for a reward?

A: We believe that it is against the spirit of the program to privately disclose the flaw to third parties for purposes other than actually fixing the bug. Consequently, such reports will typically not qualify.

Q: What if somebody else also found the same bug?

A: First in, best dressed. You will qualify for a reward only if you were the first person to alert us to a previously unknown flaw.

Q: My employer / neighbour / dog frowns upon my security research. Can I report a problem privately?

A: Of course. If you are selected as a recipient of a reward though, and if you accept, we will need your contact details to process the payment.

Q: My account was disabled after doing some tests. How can I get my account restored?

A: We recommend that you create an account dedicated only to testing before beginning any tests on our products, since we cannot guarantee that you will get access back to your account if it is disabled due to your testing activities. If you accidentally used a non-test account or you suspect your personal account was disabled due to your testing, you can request to have your account restored by contacting our Support team.

Legal points

We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Cuba, Iran, North Korea, Sudan and Syria) on sanctions lists. You are responsible for any tax implications depending on your country of residency and citizenship. There may be additional restrictions on your ability to enter depending upon your local law.

This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time and the decision as to whether or not to pay a reward has to be entirely at our discretion.

Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own.