Phala Network Responsible Disclosure

At Phala Network, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our community and our systems.

We offer bug bounties for the accepted vulnerability reports. Please don't submit non-security bugs or feature requests as vulnerability reports. Instead, you can check out Code Bounty Program.

This Responsible Disclosure program, Bug Bounty program, and any listed rewards are subject to change at any time.

Please:

- Make sure that your findings are actually a security vulnerability and within our infrastructure and/or code repositories. Missing or misconfigured SPF, DKIM, DANE, Headers, open directories, external code, etc. do NOT qualify in 99% of cases and will be denied. Vulnerabilities where you can access servers, execute code, etc. do qualify for report submission.
- E-mail your findings to cert@phala.network.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people’s data,
- Do not reveal the problem to others until it has been resolved,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
- Consider if the found issue poses an actual security risk, and do not assume so because your scanner told you so.

What we promise

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,

- We will inform you if we accepted your report as a found security issue or that we deny the report as the reported issue and/or Proof-of-Concept does not work.
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The type and/or amount of the reward will be determined based on the severity of the bug and the quality of the report.

Severity:	Critical	High	Medium	Low
Up to:	$15,000	$4,500	$1,500	$1 - $300

Reward amounts will be determined only at the end of remediation of the disclosed issue. Actual reward amounts may exceed $15,000 or be as low as $1. The SYSOPS / CERT Team will provide their assessment and recommendation regarding severity or regarding reward amount but the final decision is solely at the discretion of the Phala Team.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication of the problem after it is resolved.

Scoping

- Core blockchain runtime & client
- Websites: homepage, forum, Phala web apps, wiki, etc
- Mining subsystem: pherry, runtime-bridge, helper scripts