HYCON Bounty$_{\underline{code}}$ Program Handbook

Release 001C

Developer HYCON

Contents

1. Introduction 3
   1.1 Purpose 3
   1.2 Document Conventions 3
   1.3 Project References 4
2. Bounty Program Intro & Rules 5
   2.1 Introduction to the Bounty Program 5
   2.2 Rules 5
3. Ways to Contribute 7
   3.1 Scope 7
   3.2 Issues Report 7
   3.3 Pull Requests 7
   3.4 Custom Projects powered by HYCON 8
4. Security Bugs / Vulnerabilities 9
   4.1 Process 9
   4.2 Category 9
   4.3 Disclosure 9
   4.4 Public Recognition 10
5. Submission Process & Legal Information 11
   5.1 Submission Process 11
   5.2 Legal Information 11
6. Addendum 12
   6.1 Scope of Security Issues 12
7. Revision History 12
   Updated Content 12

1. Introduction

1.1 Purpose

This document provides guidelines and instructions for HYCON's bounty program. It's designed to help developers who wish to contribute towards the Hycon project. Individuals (referred hereinafter as "Contributors") can report a problem or make a proposal of improvement to earn HYC.

Note: This is a live document and may be edited and updated as time progresses.

1.2 Document Conventions

The use of the words Glosfer, Glosfer corp., Infinity Blockchain, Hycon, HYC, and the Glosfer corp. trademark all refer to the company named Glosfer corp. and/or the Hycon project. The above may be used interchangeably.

The use of the words Bounty program, Bounty, Coding Contribution program, and Coding Contribution all refer to the Bounty program within the Hycon project. The above may be used interchangeably.

The use of the words *must, must not, required, prohibited, shall, shall not, should, should not, recommended, not recommended, may, may not, optional, comprise* or *compose* in a statement have the following meanings:

- *must, required,* or *shall* means that the statement is absolute.
- *must not, prohibited,* or *shall* not means that the statement is an absolute prohibition.
- *should* or *recommended* means that prerequisites and implications must be understood before selecting the statement's course.
- *may* or *optional* means that the statement is completely optional and assumed.
- *usually* means that the statement's behavior is assumed and the assumed actions are likely to occur.
- *comprise* means that the statement encompasses all elements, but may also include additional, unnamed elements.
- *compose* means that the statement consists of all named elements, and no more.

1.3 Project References

GitHub Guides

GitHub Labels - HYCON core

OWASP risk rating model

CVE - Common Vulnerabilities & Exposures

2. Bounty Program Intro & Rules

2.1 Introduction to the Bounty Program

Team HYCON's bounty program spans end-to-end: from soundness and implementation compliance (such as the consensus model, p2p protocols, proof of work, etc.) to network security and consensus integrity. The program is an experimental and discretionary rewards program for the community to encourage and reward those who help improve the platform. Please submit all issues and code-submissions to Team Hycon's GitHub and/or security@glosfer.com.

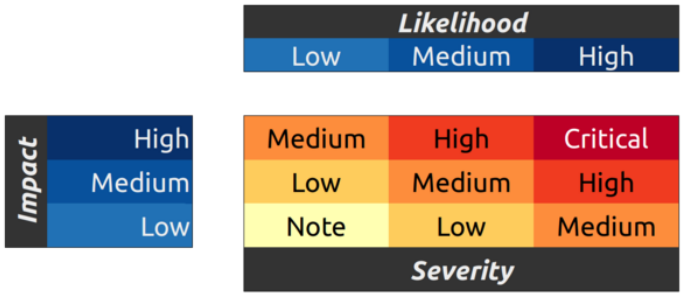
2.2 Rules

2.2.a General Rules

Please refer to the following list before you participate.

- Any submission that has already been submitted and are either in the claiming process or have completed it are not eligible for rewards.
- Issues and Pull Requests that are already known to the HYCON R&D team are not eligible for bounty reward.
- Pull requests for accepted *Note* reward-size (see 2.2.b Reward Sizes) are only accepted once per month, per user (see 3.3 Pull Requests).
- Public disclosure of a vulnerability makes it ineligible for a bounty (see 4 Security Bugs).
- Please start or fork a private chain for bug hunting. Please respect the main and test networks and refrain from attacking them.
- The R&D team, employees and all other people paid by Hycon or Glosfer corp., directly or indirectly, are not eligible for rewards.
- There are multiple variables in determining rewards. Determinations of eligibility, score, and all other terms related to bugs, vulnerabilities, and rewards are at the sole and final discretion of the Bounty Program team.

The value of rewards paid out for issues will vary on **Severity**. This is determined according to the OWASP risk rating model based on *Impact and Likelihood*.



In addition to **Severity**, other variables are also considered, such as the following:

- **Quality of Description.** Higher rewards for clear, well-written submissions.
- **Quality of Reproducibility.** Including test code, scripts, and/or detailed instructions will improve response time.
- **Quality of Fix, if applicable.** Higher rewards for solutions or description of how to fix the issue.

See 5.2 Legal Information for other issues that may affect bounty rewards.

2.2.b Reward Sizes

Reward sizes are *guided by* the rules below but are still subject to the determination and sole discretion of the Bounty Program team.

- **Critical:** Contact Us
- **High:** Up to $5,000
- **Medium:** Up to $1,000
- **Low:** Up to $500
- **Note:** Up to $100

Submissions that include fixes and patches are also eligible for an additional 100% of the initial reward size.

3. Ways to Contribute

3.1 Scope

This section provides guidelines, processes, and standardized information for Contributors. The Bug Hunting and Reporting activities will primarily be used on the GitHub repository for Hycon and the corresponding email: security@glosfer.com.

3.2 Issues Report

Note: For a detailed walkthrough about issues on GitHub, check out Mastering Issues!

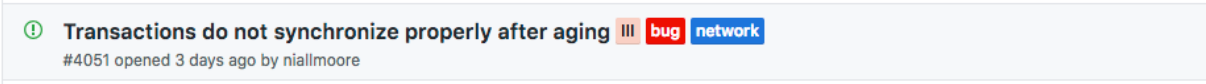


Figure 1 | An example of an issue

Contributors can add issues as a way of keeping track of tasks, enhancements, and bugs. These issues are shared and discussed publicly. **Vulnerabilities should never be disclosed here.**

The corresponding bounty must have an email submission format described below:

- ID#: ID number of the issue
- GitHub username
- Hycon wallet address
- Short summary or description of the issue.

3.3 Pull Requests

Note: For a detailed walkthrough about pull requests on GitHub, check out About pull requests.

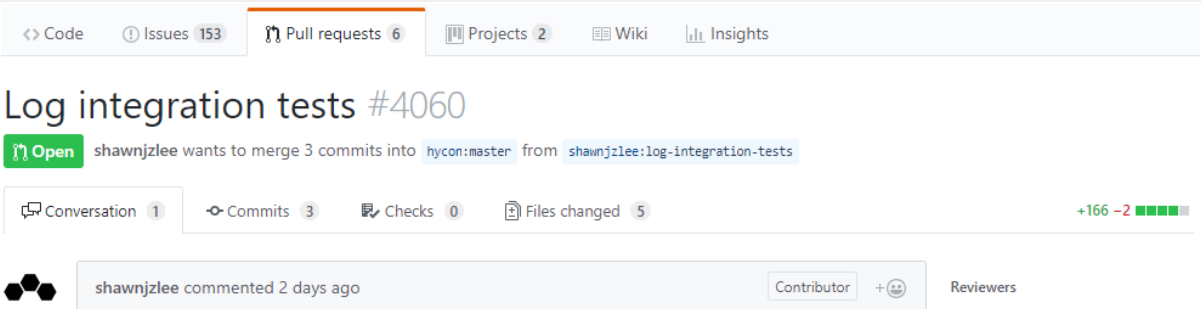


Figure 2 | An example of a pull request

Contributors can submit pull requests to improve the codebase for everyone for all users. Team HYCON appreciates any and all pull requests that provide a meaningful change to the codebase: from type corrections and translation help (generally “Note” reward size), to code compliance and integrity.

Pull requests may reference other users’ issue(s). The corresponding bounty must have a detailed email submission format described below:

- Personal Details
    - GitHub username
    - Hycon wallet address
- Pull Request Details
    - ID number of the pull request
    - ID number of the relevant issue (if applicable)
    - Summary of Implementation
    - Test Requirements and Test Cases (if applicable)

3.4 Custom Projects powered by HYCON

One of Team HYCON’s core philosophies is to make the HYCON ecosystem easy to use and easy to develop on. Contributors who have great ideas that which are not yet developed are welcome to speak have it planned and validated with the Team to make it happen. Projects may fall into, and are not limited to, any the following categories:

- API integration
- Commercial Plugin
- Games
- Hardware Integration
- HYCON related apps

Custom projects must follow the MIT License and must not overlap an existing bounty reward. Please get in touch with us at security@glosfer.com for more details.

The corresponding bounty must have a detailed email submission format described below:

- Personal or Team Details
    - Name, GitHub username, Country of Residence
    - Hycon wallet address
- Custom Project Details
    - Category of the project
    - Timeline / Time Required to Completion
    - Detailed summary of project or business plan (for larger projects)

4. Security Bugs / Vulnerabilities

4.1 Process

Security issues are similar to pull requests but need to be reported to security@glosfer.com **confidentially**. These are not shown to the public and will be tracked until completion via email.

Information may be shared with the Contributor's domain experts at the discretion of the bounty team providing that it is made clear that the information is not for public disclosure and that security@glosfer.com must be copied on any communication regarding the vulnerability.

Any findings of public disclosure will result in the blacklisting of the Contributor.

4.2 Category

As per the scope of the Bounty$_{code}$ Program, there are one or more categories in which security issues can fall under. If the security issue falls under a specific CVE, the Contributor should provide one or more CVE number relevant to the issue. Otherwise, see 6.1 Scope of Security Issues.

4.3 Disclosure

The contents of the vulnerability report will initially remain non-public to allow sufficient time to publish a remediation. The following is a set of options regarding the timeline of such disclosure:

- **Default:** If neither the Primary Contact nor the Contributor raise any objections, the contents of the report will be made public within 30 days.
- **Mutual Agreement:** A mutually agreed timeline can be made between the Primary Contact and Contributor given that an open communication regarding such timeline is made.
- **Extension:** Due to complexity and other factors revolving around the vulnerability, more time may be necessary to complete the remediation. As a result, a request by the Primary Contact should be made to extend any aforementioned disclosure timeline.

4.4 Public Recognition

The Contributor is allowed to receive public recognition given the following set of rules:

1. The Contributor is also the discoverer of the particular vulnerability.
2. The vulnerability is confirmed to be a valid security issue by the R&D team.
3. The Contributor accurately states their account and interaction in solving the vulnerability.
4. The Contributor has complied with all of the above guidelines (4.1, 4.2, 4.3).

Team HYCON encourages Contributor to share their findings, remediations, and experience through the medium of their choice given that they follow the above set of rules.

4.5 Guidelines

The corresponding bounty must have a detailed email submission format described below:

- Personal Details
    - Name(s) or Alias of Contributor
    - Country of Residence
    - Hycon wallet address
- Pull Request Details
    - CVE ID (if applicable)
    - Scope of Work (see 6.1 Scope of Security Issues, if applicable)
    - Latest Release Version affected
    - Detailed Summary of Implementation
    - Test Requirements and Test Cases

5. Submission Process & Legal Information

5.1 Submission Process

The Bounty Program Team may offer monetary rewards for issues, pull requests, custom projects, and vulnerabilities alike. However, not all of the above will result in a reward and is at the sole discretion of the team to grant a reward. Furthermore, the amount of each bounty payment will be determined by the team. Each reward is unique and is in no way correlated to any other reward. Appeals regarding reward conditions will never be accepted.

Note reward size submissions will only be counted once per month per GitHub user. Please try to consolidate these submissions together.

All rewards are paid on the first Tuesday at the beginning of every month for contributions accepted and merged during a previous month. A Bounty Program Team Member will contact the Contributor prior to payment. All responses regarding submissions will be processed within three (3) working days.

5.2 Legal Information

Rewards are subject to the following eligibility requirements:

- Any Contributors from countries that have trade restrictions or export sanctions with the Republic of Korea will not be able to receive bounty payments.
- Minors are welcome to participate; however, bounty payments can only be claimed by the minor's parent or legal guardian.
- All payments will be made in HYC at the current market price in U.S. dollars (USD). As a result, a Hycon wallet is required for the payment to take place.
- All rewards are subject to applicable law and taxation.
- Testing made by the Contributor must not violate any law or compromise any data that is not yours.

6. Addendum

6.1 Scope of Security Issues

6.1.a Protocol Security

6.1.b Implementation Security

Client Application Security
Client Protocol Implementation
Cryptographic Primitives Security
Database Implementation
Database Security
Network Security
Node Security

7. Revision History

This chapter describes changes to the Bounty$_{code}$ Program Handbook for the Hycon Project from previous revision.

Updated Content

- 2018/06/29_19:19 – Received review and suggestions. Added email guidelines for Custom Projects and Vulnerabilities. Fixed typos.
- 2018/06/29_16:39 – Revision of Introduction, Rules, Ways to Contribution, and Legal Information.
- 2018/06/04_00:00 – First draft of the Handbook, not including Bounty$_{code}$.