Security Code Audits

At Hyperledger, we are committed to a trust-but-verify security philosophy for our open source projects. We trust the engineering, change management, and risk reduction processes we use in our software supply chain to greatly reduce the risk of security flaws in the finished product. But to verify that is the case, we are organizing outside, independent security audits of the projects as they reach their 1.0 milestone. In addition to code audits, we also conduct regular crypto audits to comply with the US government regulations on the exportation of strong cryptography. Lastly we also run regular license audits to make sure that all of the code in our projects is properly licensed.

Re-auditing Policy

After our projects reach 1.0 status, the policy for when we do another outside audit of a project is based on a few factors. The primary factor is code "churn" –the amount of code that has changed since the last audit. The secondary factor is major architectural changes (e.g. changing cryptography library implementations). When enough code has changed and/or architectural rework has happened, Hyperledger will invest money into having a follow up audit done to once again establish a baseline for project security.

Hyperledger Besu

Hyperledger Besu joined Hyperledger as a project in the fall of 2019 and with their first major release a security audit was conducted. Below is the report from that audit.

- Q1 2020
    - Hyperledger Besu Penetration Test Report
- Q2 2022
    - Hyperledger Besu Penetration Test Report

Hyperledger Cactus

Hyperledger Cactus

- Q2 2022
    - 2021 Hyperledger Cactus Web Application Pentest Updated

Hyperledger Composer

Hyperledger Composer reached their 1.0 milestone early in 2018. Nettitude conducted the security audit of the source code and all issues found have been resolved.

- Hyperledger Composer - Security Assessment Management Report
- Hyperledger Composer - Security Assessment Technical Report

Hyperledger Fabric

Hyperledger Fabric was the first project to reach the 1.0 milestone. We hired WP Hacked Help to conduct a web security audit of the source code and to work closely with the developers to fix any issues that they found. The audit results were announced in a Hyperledger blog post.

- Hyperledger Fabric - Security Assessment Management Report
- Hyperledger Fabric - Security Assessment Technical Report

For the v2.x release, a subsequent penetration test of Hyperledger Fabric was performed by Tevora Threat Research Group.

- Hyperledger Fabric - Penetration Test Report

Hyperledger Iroha

Hyperledger Iroha is fast approaching their 1.0 milestone. Nettitude conducted the security audit of the source code and all issues found have been resolved. The audit results were announce in a Hyperledger blog post.

- Q3 2020
    - Hyperledger Iroha Application Pentest Report
- Q1 2018
    - Hyperledger Iroha - Security Assessment Management Report
    - Hyperledger Iroha - Security Assessment Technical Report

Hyperledger Indy

Hyperledger Indy reached their 1.0 milestone late in 2018. Nettitude conducted the security audit of the source code and all issues found have been resolved.

- Hyperledger Indy - Security Assessment Management Report

- Hyperledger Indy - Security Assessment Technical Report

Hyperledger Sawtooth

Hyperledger Sawtooth reached 1.0 in the Spring of 2018. Nettitude conducted the security audit of the code base and all reported issues have been addressed. The audit results were announced in a Hyperledger blog post.

- Hyperledger Sawtooth - Security Assessment Management Report
- Hyperledger Sawtooth - Security Assessment Technical Report