Security Audit Criteria

This page documents all of the things we ask of third party security auditors when bidding and contracting for an independent review of Hyperledger projects.

Requirements

- Static and hand analysis of sensitive areas of the code, specifically the code that interacts with cryptography libraries, network interfaces, and the file system.
- Fuzzing of both network API's and library API's.
- Static analysis and best practice enforcement with a linter over the entire code base.
- Malicious node attacks on the network.

Optional

- Dependency checks looking for known vulnerabilities and/or updates.
- License audit to ensure all dependency licenses are properly followed.

Other Criteria

- Early reporting of issues as they are found by the auditing team so that fixes can be made in parallel.
- The team conducting the audit also has the capability to do PCI/GDPR/HIPPA/etc compliance auditing that we can offer to integrators building applications.
- A written report with detailed analysis.