TL;DR

Lido has not undergone an annual infrastructure audit (aka pen test) yet this year. Of the top 50 hacks, 40% have occurred beyond the confines of smart contracts, with hackers identifying vulnerabilities in web apps, wallets, bridges, and other points of intrusion. Annual infrastructure auditing is a critical feature of comprehensive protocol security and will allow Lido to take a proactive stance in identifying and addressing potential vulnerabilities.

Halborn is an award-winning, elite cybersecurity company for blockchain organizations founded in 2019 by renowned ethical hacker Steven Walbroehl and growth hacker Rob Behnke. We’ve been trusted by organizations such as Uniswap, Matter Labs, Circle, Solana, Dapper Labs, Polygon, Animoca Brands, Sushi, and many more.

We are seeking a grant to perform a comprehensive infrastructure audit for the Lido protocol.

Purpose & Motivation

The vast majority of companies perform an annual infrastructure audit as a critical part of their security planning. In conversations with the Lido team this month we realized that the protocol has not yet undergone an infrastructure audit this year.

Infrastructuring auditing, also known as pen testing, is a critical feature of a robust and comprehensive cybersecurity plan. While many DAOs and Web3 companies are (rightly) focused on smart contract auditing as a key pillar of their security, infrastructure auditing is just as important, particularly for large protocols.

Whereas smart contract auditing focuses on the contracts themselves, infrastructure auditing targets the various “non-smart contract” surface areas - web apps, mobile apps, bridges, cryptocurrency wallets, cloud infrastructure and more. Proactively identifying vulnerabilities in these areas allows Lido to repair potential weaknesses before they can be exploited by malicious actors.

According to our research, off-chain attacks are a growing threat and a significant source of losses. A closer examination of the top 50 attacks by loss reveals that off-chain attacks accounted for a staggering 40% of the total losses. This percentage has been steadily increasing over time, reaching 61% of losses and 70% of all attacks by type (on-chain vs. off-chain) in 2023 alone.

One notable example illustrating off-chain vulnerabilities was the Badger hack in 2021, resulting in $120mm of losses. This breach was facilitated by a script injection on their website. Another common vulnerability lies in private key theft or leakage, which can result from attacks on protocol servers and databases, social engineering, or other attack vectors. For instance, the Mixin Network hack in September of this year exploited a vulnerability in their cloud service provider’s database, resulting in losses totaling $200mm. However, perhaps the most significant case is the Ronin Bridge attack, which led to a staggering $624mm in losses. A comprehensive audit of the entire ecosystem might have potentially thwarted these attacks.

In this regard, Halborn has played a significant role in enhancing the off-chain security of various protocols. While many of the reports remain confidential, some of our critical finds include detecting unauthorized access to sensitive data in the project database; secret exposure of the database’s admin secret key; potential SQL injection vulnerabilities in other databases and misconfigurations on a Firebase database that could allow an attacker mostly free range on it.

Among our public reports, we would like to highlight:

- The Aptos Wallet WebApp pentest.
- We found a total of 6 critical vulnerabilities, including the possibility for an attacker to obtain the mnemonic passphrase from the clipboard storage; the ability of an attacker to execute malicious code using the exported wallet functions, triggering a Denial of Service on the extension and the Browser; race condition in the function used to sign messages as well as no confirmation required from the user and the possibility for an attacker who has compromised a user’s machine can exfiltrate and steal their mnemonic phrase as well as the password

- We found a total of 6 critical vulnerabilities, including the possibility for an attacker to obtain the mnemonic passphrase from the clipboard storage; the ability of an attacker to execute malicious code using the exported wallet functions, triggering a Denial of Service on the extension and the Browser; race condition in the function used to sign messages as well as no confirmation required from the user and the possibility for an attacker who has compromised a user’s machine can exfiltrate and steal their mnemonic phrase as well as the password

- HBarSuite WebApp and SmartNode FrontEnd and BackEnd pentest
- In this case, Halborn engineers discovered two critical vulnerabilities, which allowed an attacker to perform a Denial Of Service to the smart nodes and a vulnerability that caused a user to not be able to claim back the liquidity or observe the liquidity added into the different pools of the protocol.

- In this case, Halborn engineers discovered two critical vulnerabilities, which allowed an attacker to perform a Denial Of Service to the smart nodes and a vulnerability that caused a user to not be able to claim back the liquidity or observe the liquidity added into the different pools of the protocol.

Infrastructure auditing also provides valuable insights into how well Lido's security controls are functioning. It's not just about finding vulnerabilities, but about understanding how effectively the protocol's defenses can resist and respond to different attack scenarios. This hands-on testing allows Lido to fine-tune its security measures and ensure they can stand up to real-world threats.

Critically, infrastructure auditing is an iterative process, most effective when performed annually so that prior vulnerabilities can be re-tested (to determine the effectiveness of fixes) and new vulnerabilities identified.

Scope of Work

Halborn will conduct penetration testing of Lido's non-smart contract threat surfaces such as web apps, cloud, infrastructure, and more. Halborn will use an active hands-on approach using deep security inspection to identify vulnerabilities. The penetration test will simulate the activities and tactics typically performed by threat actors. During the test, Halborn will update Lido with necessary details or findings.

Halborn will perform the infrastructure audit following these steps or phases:

- Mapping Content and Functionality
- Configuration and deployment
- Identity Management flaws
- Authentication/Authorization Flaws
- Session handling
- Business logic flaws
- Rate Limitations tests
- Brute Force Attempts
- Input Handling
- Fuzzing of all input parameters
- Multiple Type of Injection (SQL/JSON/HTML/Command)
- Client-side testing
- Error handling
- Weak Cryptography
- Source Code Review

Deliverables

After testing, Halborn will create a report that provides details of all service areas covered, with risks, vulnerabilities, steps taken, and remediation recommendations.

Halborn will exercise due care in removing testing tools, payloads, and other files or artifacts used during the assessment after the completion of testing. Halborn will make every attempt to avoid business interruption during the course of the penetration test.

Team

Halborn is an award-winning, elite cybersecurity company for blockchain organizations founded in 2019 by renowned ethical hacker Steven Walbroehl and growth hacker Rob Behnke. We've been trusted by organizations such as Uniswap, Matter Labs, Circle, Solana, Dapper Labs, Polygon, Animoca Brands, Sushi, and many more.

Fees & Payment

Team will need to complete a scoping exercise in order to determine an accurate price, as projects are based on time & complexity. For context however, an average infrastructure audit project costs approximately $50k.