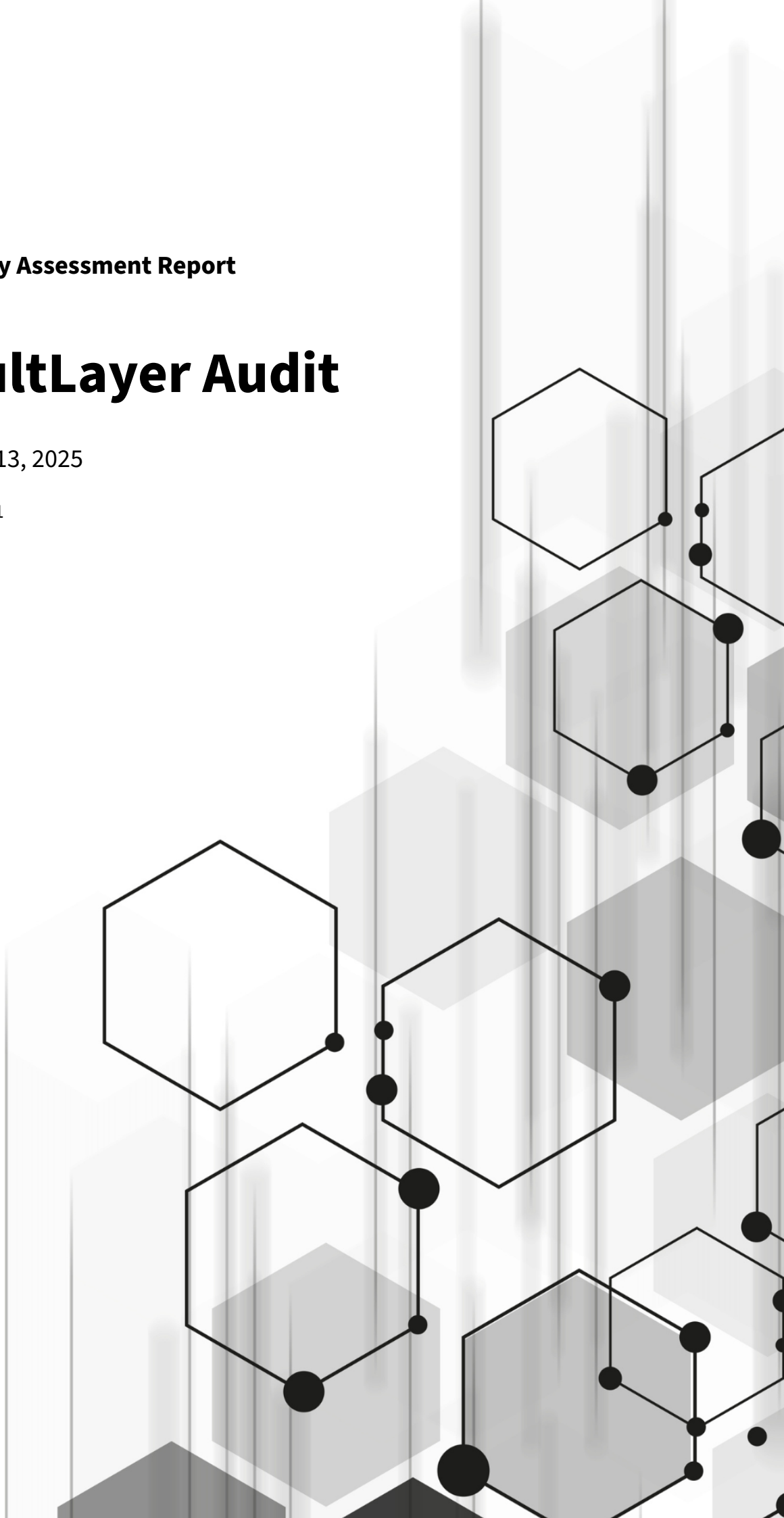
Security Assessment Report

VaultLayer Audit

August 13, 2025

Version 0.1



sub7

Contents

1 Confidentiality statement

This document is the exclusive property of VaultLayer and Sub7 Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both VaultLayer and Sub7 Security.

2 Disclaimer

This report, analysis, or any information provided by Sub7 Security is subject to the terms and conditions outlined in the agreement with our clients, including but not limited to limitations of liability, confidentiality clauses, and terms of use. The contents of this report or information provided may only be utilized in accordance with the agreed-upon scope of services and are intended solely for the recipient's internal use as stipulated in the engagement agreement.

This report is not, and should not be construed as, an endorsement or disapproval of any project, product, or team associated with the assessed technology. Sub7 Security does not provide financial, investment, or legal advice, nor does this report serve as a guarantee or certification of the security, legality, or operational integrity of the analyzed technology.

While Sub7 Security strives to identify and mitigate vulnerabilities through rigorous assessments, no technology can be deemed entirely free of risks. This report does not warrant the absolute bug-free nature or risk-free operation of the audited code or systems. Sub7 Security disclaims any responsibility for future vulnerabilities, exploits, or operational failures that may arise post-assessment.

The recipient of this report or any information provided by Sub7 Security is responsible for conducting their own due diligence and maintaining robust security practices. Cryptographic and blockchain technologies present a high level of ongoing risk due to their evolving nature. Sub7 Security advises all stakeholders to remain vigilant and adapt to emerging threats.

By utilizing our services, the recipient acknowledges that Sub7 Security's role is to reduce attack vectors and enhance the security posture of the analyzed systems to the best of our abilities within the agreed scope. Sub7 Security does not claim or assume any liability for the ultimate functionality, performance, or security of the technology reviewed.

For further inquiries or clarification, please contact Sub7 Security at hello@sub7.tech

3 About Sub7

Founded in 2022, Sub7 Security is a pioneering cybersecurity company dedicated to creating innovative and efficient solutions for a secure digital future. In 2023, we established our presence in Luxembourg after a successful pitch of our cutting-edge platform, SecHub. Our solutions earned us the prestigious recognition of being named one of the top three cybersecurity solutions in Luxembourg, further cementing our position as a leader in the field.

We are the creators of SecHub, a transformative platform designed to deliver fast, transparent, and secure cybersecurity management. SecHub empowers clients by providing direct access to top-tier security researchers, real-time findings, and rapid issue resolution. Our services include smart contract audits, penetration testing, and a range of tailored security solutions. By significantly reducing audit timelines while

maintaining robust security, SecHub is revolutionizing the way organizations manage their digital risks.

Our team brings together a wealth of expertise spanning banking, finance, cybersecurity, law, and business management. We also work closely with a dedicated lawyer, ensuring compliance with regulatory standards and providing a comprehensive approach to security and legal considerations.

Our team members have professional experience at leading organizations such as ServiceNow, Polygon, Tokeny, Bitstamp, Kreditech, Mash, Deloitte, and Bitflyer, bringing invaluable insights from diverse industries.

At Sub7 Security, we are committed to innovation, trust, and resilience. By combining cutting-edge technology, industry expertise, and legal acumen, we deliver solutions that empower businesses and build a safer, more secure digital ecosystem.

Join us as we shape the future of cybersecurity.

4 Project Overview

We are building the simplest, self-custodial way to grow BTC on L1, and get rewards in L2:

Stake from your Smart Vault

Maximize yield from CoreDAO Protocol

Get Liquidity using your Vault as Collateral

Simplify your Bitcoin DeFi journey with AI

With VaultLayer, users grow their BTC and rewards easier, without losing custody

vaultlayer-sdk: A toolkit for developers to offer better Bitcoin DeFi UX.

Smart Vaults: A new decentralized derivative asset of staked Bitcoin.

5 Executive Summary

Sub7 Security has been engaged to what is formally referred to as a Security Audit of Solidity Smart Contracts, a combination of automated and manual assessments in search for vulnerabilities, bugs, unintended outputs, among others inside deployed Smart Contracts.

The goal of such a Security Audit is to assess project code (with any associated specification, and documentation) and provide our clients with a report of potential security-related issues that should be addressed to improve security posture, decrease attack surface and mitigate risk.

As well general recommendations around the methodology and usability of the related project are also included during this activity

1 (One) Security Auditors/Consultants were engaged in this activity.

5.1 Scope

Vault Layer Pentest

5.2 Timeline

from 20 May 2025 to 27 May 2025

5.3 Summary of Findings Identified

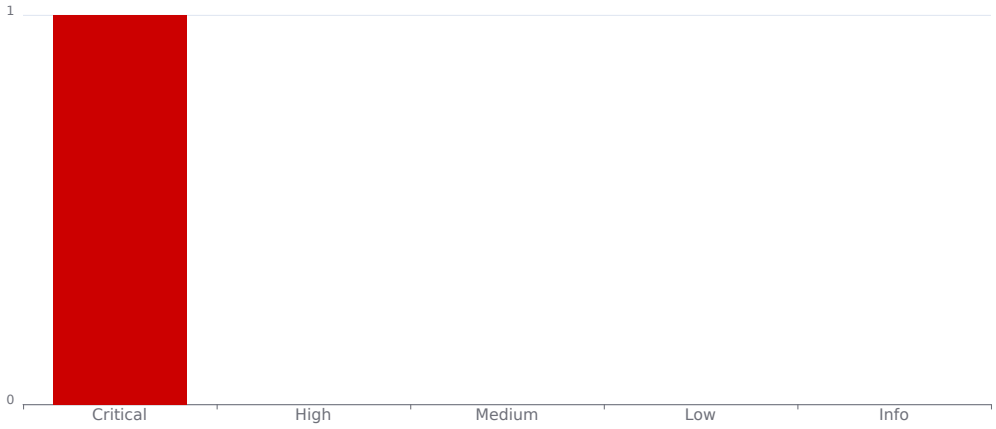


Figure 1: Executive Summary

 # 1 Critical It is possible rug the new smart vault NFT owner. – ***Fixed***

5.4 Methodology

SUB7's audit methodology involves a combination of different assessments that are performed to the provided code, including but not limited to the following:

Specification Check

Manual assessment of the assets, where they are held, who are the actors, privileges of actors, who is allowed to access what and when, trust relationships, threat model, potential attack vectors, scenarios, and mitigations. Well-specified code with standards such as NatSpec is expected to save time.

Documentation Review

Manual review of all and any documentation available, allowing our auditors to save time in inferring the architecture of the project, contract interactions, program constraints, asset flow, actors, threat model, and risk mitigation measures

Automated Assessments

The provided code is submitted via a series of carefully selected tools to automatically determine if the code produces the expected outputs, attempt to highlight possible vulnerabilities within non-running code (Static Analysis), and providing invalid, unexpected, and/or random data as inputs to a running code, looking for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.

Examples of such tools are Slither, MythX, 4naly3er, Sstan, Natspec-smells, and custom bots built by partners that are actively competing in Code4rena bot races.

Manual Assessments

Manual review of the code in a line-by-line fashion is the only way today to infer and evaluate business logic and application-level constraints which is where a majority of the serious vulnerabilities are being found. This intensive assessment will check business logics, intended functionality, access control & authorization issues, oracle issues, manipulation attempts and multiple others.

Security Consultants make use of checklists such as SCSVS, Solcurity, and their custom notes to ensure every attack vector possible is covered as part of the assessment

6 Findings and Risk Analysis

6.1 It is possible rug the new smart vault NFT owner.

Severity: Critical
Status: Fixed

Description

In VaultLayer there is an Admin & Delegatee. Admins are those who owns the Smart Vault NFT & Delegatee is chosen by the Admin to run those action scripts. Here Admin & Delegatee can be same address & the issue is here. If they are same address then they can rug the new NFT owner even after ERC-721 ownership check. Let see it how: For ex I am agent owner or Admin. I choosed my address as Delegatee. Now I will use my address to execute actions. 1. I staked BTC. 2. I sold my NFT in marketplace. 3. Just after timelock ends I executed the redeem action, as I am the Delegatee too I can execute the txn successfully, even without the ownership of the Smart Vault NFT, you can find the related code After executing the redeem action I got back my all staked BTC whereas the new NFT owner, who is real owner of those staked BTC, did not get those BTC. i.e I rugged that new NFT owner.

Location

lib/lit-actions/tool.ts

L65-L86

Recommendation

Finally, added 2 new scripts: * checkSmartVault.mjs - Script to verify PKP creation with expected tools and check current delegations. * pentestWithLoan.mjs - Script to test that a PKP cannot execute delegated actions if it is currently been listed on VaultLayer's P2P Lending market.

Comments

FOLLOW US