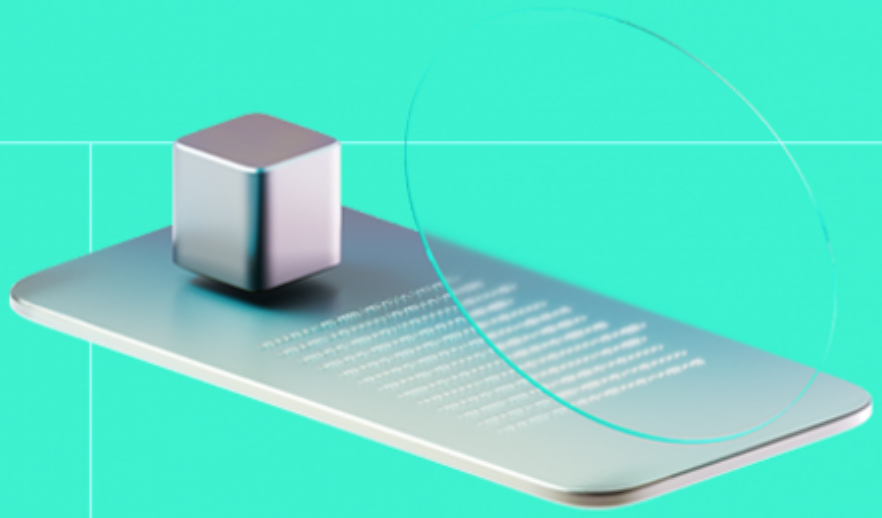
HACKEN

Smart Contract Code Review And Security Analysis Report

Customer: L7

Date: 19/02/2024



We express our gratitude to the L7 team for the collaborative engagement that enabled the execution of this Smart Contract Security Assessment.

LSD is a simple BEP-20 token which implements burning functionalities and whose total supply is fixed at 210m of token units.

Platform: EVM

Language: Solidity

Tags: BEP-20

Timeline: 06/02/2024 - 07/02/2024

Methodology: https://hackenio.cc/sc_methodology

Review

Scope

Repository	https://bscscan.com/address/0xcd1b51b87a8a7137d6421ba5a976225187a26777#code
Commit	-

Audit Summary

10/10	7/10	100%	0/10
Security Score	Code quality score	Test coverage	Documentation quality score

Total 8.4/10

The system users should acknowledge all the risks summed up in the risks section of the report

0	0	0	0
Total Findings	Resolved	Accepted	Mitigated

Findings by severity

Critical	0
High	0
Medium	0
Low	0

This report may contain confidential information about IT systems and the intellectual property of the Customer, as well as information about potential vulnerabilities and methods of their exploitation.

The report can be disclosed publicly after prior consent by another Party. Any subsequent publication of this report shall be without mandatory consent.

Document

Name	Smart Contract Code Review and Security Analysis Report for L7
Audited By	Giovanni Franchi
Approved By	Turgay Arda Usman
Website	N/A
Changelog	07/02/2024 - Preliminary Report && 19/02/2024 -Final Report

Table of Contents

System Overview **6**

Executive Summary **7**

Documentation Quality 7

Code Quality 7

Test Coverage 7

Security Score 7

Summary 7

Risks **8**

Findings **9**

Vulnerability Details 9

Observation Details 9

Disclaimers 11

Appendix 1. Severity Definitions **12**

Appendix 2. Scope **13**

System Overview

LSD is a BEP-20 that also implements OpenZeppelin burnable functionalities:

LSD Token — simple BEP-20 token that mints all initial supply to an address which is passed as a constructor parameter. Additional minting is not allowed.

It has the following attributes:

- Name: LSD
- Symbol: LSD
- Decimals: 18
- Total supply: 210m tokens.

Executive Summary

This report presents an in-depth analysis and scoring of the customer's smart contract project. Detailed scoring criteria can be referenced in the scoring methodology.

Documentation quality

The total Documentation Quality score is **0** out of **10**.

- Functional requirements are not provided.
- Technical description is not provided.
- NatSpecs are absent.

Code quality

The total Code Quality score is **7** out of **10**.

- Some best practises such as readability conventions and locked pragma are missed.
- The development environment is not provided.

Test coverage

Code coverage of the project is **100%** (branch coverage).

- Code coverage is not required under 250 locs.

Security score

Upon auditing, the code was found to contain **0** critical, **0** high, **0** medium, and **0** low severity issues, leading to a security score of **10** out of **10**.

All identified issues are detailed in the “Findings” section of this report.

Summary

The comprehensive audit of the customer's smart contract yields an overall score of **8.4**. This score reflects the combined evaluation of documentation, code quality, test coverage, and security aspects of the project.

Risks

- No risks are identified

Findings

Vulnerability Details

Observation Details

F-2024-0794 - Floating pragma - Info

Description:

The project uses floating pragma ^0.8.0.

This may result in the contracts being deployed using the wrong pragma version, which is different from the one they were tested with. For example, they might be deployed using an outdated pragma version which may include bugs that affect the system negatively.

Assets:

- LSDToken.sol [https://bscscan.com/token/0xcD1B51b87a8a7137D6421bA5A976225187a26777]

Status: Accepted

Recommendations

Recommendation:

Consider locking the pragma version whenever possible and avoid using a floating pragma in the final deployment. Consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

External References:

- Solidity Documentation

F-2024-0795 - Obscure Numerical Notation in Token Supply - Info

Description: In the reviewed smart contract, specifically within the token minting function, the numerical notation used to define the initial token supply presents a concern regarding clarity. The expression **21 * 10**25** is employed to denote the total supply of tokens to be minted. While mathematically accurate, this representation may not immediately convey the intended magnitude of the token supply to readers unfamiliar with parsing such expressions, especially given the common practice of specifying token amounts in relation to the **decimals** function, typically set at 18 for ERC-20 tokens.

Assets:

- LSDToken.sol [https://bscscan.com/token/0xcD1B51b87a8a7137D6421bA5A976225187a26777]

Status: Accepted

Recommendations

Recommendation: To address the concerns raised by the obscure numerical notation and enhance the readability and accessibility of the smart contract code, it is recommend adopting a more descriptive and universally understood format for representing large numbers, particularly for crucial parameters such as token supply.

- Current format:

```
_mint(addr_, 21 * 10**25);
```

- Suggested format:

```
_mint(addr_, 210_000_000 * 10 ** decimals());
```

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed based on best industry practices at the time of the writing of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the Consultant cannot guarantee the explicit security of the audited smart contracts.

Appendix 1. Severity Definitions

When auditing smart contracts, Hacken is using a risk-based approach that considers **Likelihood**, **Impact**, **Exploitability** and **Complexity** metrics to evaluate findings and score severities.

Reference on how risk scoring is done is available through the repository in our Github organization:

hknio/severity-formula

Severity	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation.
High	High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation.
Medium	Medium vulnerabilities are usually limited to state manipulations and, in most cases, cannot lead to asset loss. Contradictions and requirements violations. Major deviations from best practices are also in this category.
Low	Major deviations from best practices or major Gas inefficiency. These issues will not have a significant impact on code execution, do not affect security score but can affect code quality score.

Appendix 2. Scope

The scope of the project includes the following smart contracts from the provided repository:

Scope Details

Repository	https://bscscan.com/address/0xcd1b51b87a8a7137d6421ba5a976225187a26777#code
Commit	N/A
Whitepaper	N/A
Requirements	N/A
Technical Requirements	N/A

Contracts in Scope

LSD.sol