Xennium Token Security Audit Report

1. Introduction

Contract Name: Xennium Token
Symbol: XENX
Compiler Version: 0.8.20
Libraries Used: OpenZeppelin (ERC20, Ownable, ERC20Permit)
Audit Date: 14-02-2025

Scope

This audit focuses on the **Xennium Token** smart contract, which implements an ERC-20 token with:

- A total supply of 19 billion tokens.
- A Last Coin Transfer Restriction (LCTR) rule.
- Reserved allocations for community and development.

2. Executive Summary

Findings Summary:

- Critical Issues: **0**
- High-Risk Issues: **1**
- Medium-Risk Issues: **0**
- Low-Risk Issues:**1**

Overall, the contract follows best practices but has some security and usability concerns that need attention.

3. Methodology

The audit was conducted using:

- Automated Analysis Tools: Slither, Mythril, and Securify.
- Manual Code Review: Reviewing business logic, security vulnerabilities, and adherence to best practices.
- Testing: Running simulations and edge-case scenarios.

4. Findings & Issues

🔴 High-Risk Issue: Contract Owns Initial Supply

Description: The contract initially mints the entire total supply to itself and then transfers the development reserve to the owner. However, the remaining 15 billion tokens remain locked inside the contract with no function to distribute or allow access.

Impact: The contract may be unusable unless additional functions are added to release the supply.

Recommendation: Since the owner will distribute tokens via DEXs, ensure a clear distribution plan and potentially add a function to withdraw tokens securely if needed.

🔵 Low-Risk Issue: No Event Emission for Transfers

Description: The `transfer` and `transferFrom` functions override ERC-20 methods but do not emit additional events for logging restricted transfers.

Impact: This reduces transparency and makes tracking LCTR-related failures more difficult.

Recommendation: Implement a custom event (e.g.,`TransferRestricted(address sender, uint256 amount)) to log failed transfer attempts due to LCTR.

5. Recommendations

1. **Ensure a secure mechanism** for distributing the initial supply via DEXs.
2. **Improve logging and event emission** for transparency.
3. **Implement unit tests** covering edge cases for LCTR logic.

6. Conclusion

The **Xennium Token contract** is well-structured but has some **high-risk issues** related to **token accessibility**. Addressing these will improve security and usability.

Final Security Rating: 8.0/10 (Minor Adjustments Recommended)