

Smart Contract Audit Report - GZilla

1. Audit Summary

The smart contract 'GZilla' was subjected to a simulated security audit performed by our team for educational purposes. The audit process reviewed the contract's source code, deployment parameters, and on-chain behavior.

The evaluated contract has a score of 85/100, indicating a good level of security with minor issues addressed. The audit was completed on March 23, 2025 and no critical vulnerabilities were found.

2. Contract Overview

Contract Address: 0x9A8f3B784CDe1F21372e21e1F453a0a4201f92b3

The contract implements a standard ERC-20/BEP-20 token with custom fee mechanisms, ownership management, and liquidity handling. It includes features such as automatic liquidity injection, token burning mechanisms, and a marketing wallet allocation.

3. Vulnerability Assessment

	Type	Details
	Critical Issues	None found
	High Severity Issues	None found
	Medium Severity Issue	1 (Resolved)
	Low Severity Issues	2 (Resolved)
	Informational Notes	3

The medium severity issue related to access control for liquidity withdrawals was patched by implementing a multi-sig safeguard. Low severity issues were related to input validation and non-critical gas optimization opportunities.

4. Final Assessment

The 'GZilla' smart contract shows a solid implementation pattern with adequate protections against

Smart Contract Audit Report - GZilla

the most common vulnerabilities. Although minor issues were present initially, they were addressed. The contract is deemed safe for deployment in academic or testing environments.