Security Audit Report - BabylonXToken

Summary:

Contract Name: BabylonXToken

Network: Ethereum Mainnet

Compiler Version: ^0.8.20

Audit Date: May 27, 2025

Auditor: ChatGPT (AI-assisted manual review)

Key Checks:

Reentrancy: SAFE

Integer Overflow/Underflow: SAFE (Solidity ^0.8+ has built-in checks)

Access Control: SAFE (OnlyOwner pattern used)

Token Minting: SAFE (Only in constructor)

External Calls: SAFE (Staking contract only)

Upgradeability: NOT UPGRADEABLE

Events: MISSING critical events like Minted, RewardDistributed

Gas Efficiency: Can be improved (buyTokens is unimplemented)

Detailed Findings:

1. No Token Mint After Deployment:

   - Only minted in the constructor.

   - Risk: Low

   - Recommendation: Add 'Minted' event.

2. Staking Reward Distribution:

   - Only stakingContract can call it.

   - Risk: Medium

Security Audit Report - BabylonXToken

  - Recommendation: Emit 'RewardDistributed' event.

3. buyTokens() Logic:

  - Empty function.

  - Risk: Medium

  - Recommendation: Remove or safely implement with a cap.

Conclusion:

This is a low-risk contract using well-established OpenZeppelin standards.

Before public launch or listing:

- Add missing events for transparency.

- Implement or remove incomplete functions.

- Consider third-party audit if raising funds.