Light Audit Report
ERC20 – BabyAlpaca Token

Auditor: Febri Nirwana
Date: July 2025
Network: Ethereum
Contract Address:
0xE7e93e0459FfDD8D6DcD4fF26Fc36D3682Cc6bFF

1. Disclaimer

This is an independent light audit conducted based on publicly available source code. This report does not guarantee the absence of bugs or vulnerabilities. Always do your own due diligence.

2. Scope of Review

Contract Reviewed: `Erc20.sol`
Code Source: Etherscan (verified source)
Commit / Block Date: 2025-06-16
Review Focus: Logic correctness, security patterns, custom implementations

3. Summary of Findings

No	Severity	Issue
1	Critical	Owner transfer backdoor in `transferFrom()`
2	Medium	Redundant launch logic
3	Medium	Custom ERC20 implementation
4	Low	`_transferAllowed()` always returns true
5	Low	`exchanges` state unused

4. Detailed Findings

a. Finding 1 – Owner Transfer Backdoor

Severity: Critical
Location: transferFrom()
Description:
If launched == false, and the caller is the owner, and the to address is also the owner, then the transfer can happen without reducing allowance.
This lets the owner pull tokens from anyone who has given approval, before the launch.
Why it's dangerous:
Owner can take tokens from users quietly before launch.
Recommendation:
Remove the special logic that gives the owner this power.

b. Finding 2 – Custom ERC20 Instead of OpenZeppelin

Severity: Medium
Location: All over the code
Description:
The contract creates its own ERC20 logic instead of using OpenZeppelin. This adds more risk and more code to maintain.
Why it's a problem:
More code = more bugs. OpenZeppelin is safer and cleaner.

Recommendation:
Use OpenZeppelin's ERC20, Ownable, and Context contracts.

c. **Finding 3 – launch() Does Nothing**
Severity: Medium
Location: launch()
Description:
The launch() function only changes a boolean. It doesn't protect anything or enable new features.
Why it's useless:
Launch sounds like a big event, but here it does nothing.
Recommendation:
Remove it. Or, add real control like pause().

d. **Finding 4 – _transferAllowed() Always Returns True**
Severity: Low
Location: _transferAllowed()
Description:
The function checks a few conditions, but all of them lead to return true. It doesn't block anything.
Why it's confusing:
It looks like access control, but it's just noise.
Recommendation:
Remove it, or replace with real logic.

e. **Finding 5 – exchanges Variable Not Used**
Severity: Low
Location: State variables
Description:
The mapping (address => bool) exchanges is never used in any function.
Why it's unnecessary:
Wastes storage and gas.
Recommendation:
Delete it.

5. Recommendations (Global Summary)

a. Remove unsafe owner logic from `transferFrom()`
b. Replace custom ERC20 with OpenZeppelin standard
c. Eliminate unnecessary launch and `exchanges` logic
d. Clean up unused code to reduce gas and complexity

6. Final Notes

The contract performs its intended ERC20 functionality, but contains unnecessary logic and potential backdoors that must be resolved before production use.