

**SECURITY AUDIT REPORT**

Baby Hamster Kombat

**2**

**TOKEN OVERVIEW**

## Risk Findings

**Severity Found**

 High **0**

 **Medium** **0**

 **Low** **0**

 **Informational** **1**

## Centralization Risks

**Owner Privileges Description**



 **Can Owner Set Taxes >25% ?**

 **Owner needs to enable trading ? ** **Can Owner Disable Trades ?**

 **Can Owner Mint ?**

 **Can Owner Blacklist ?**

 **Can Owner set Max Wallet amount ? ** **Can Owner Set Max TX amount ?**

**Not Detected Not Detected Not Detected Not Detected Not Detected Not Detected Not Detected**

**3**



# TABLE OF CONTENTS

**02 Token Overview 03 Table of ContentS 04 Overview**

1. **Contract DetailS**
2. **Audit Methodology**
3. **VulnerabilitieS CheckliSt**
4. **RiSk ClaSSification**
5. **Inheritence TreeS**
6. **TeStnet VerSion**
7. **Manual Review**

**13 About Expelee**

1. **DiSclaimer**

**4**

Audit Result

Audit Date

Passed

20 June 2024



**OVERVIEW**

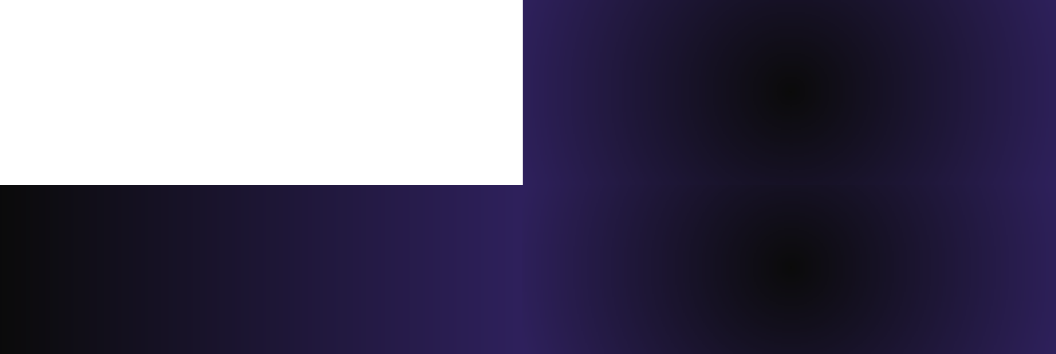
The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

15 March 2025

Audit Date

Passed

Audit Result



**5**



# CONTRACT DETAILS

Token Address: 0x089D91926e43cd7318198922D548189470cA25f2

Name:

Baby Hamster Kombat

Symbol: HMSTR   
Decimals: 18 Network: Base

Type: ERC-20 Owner: -

Deployer: 0xdBc578b0178458cb344bF4179F55dfE14900b9FA

Token Supply: -

Checksum: A17acbefe2a12642d388659dffd20311

Testnet: https://basescan.org/token/0x089D91926e43cd7318198922D548189470cA25f2#code

**6**



# AUDIT METHODOLOGY

### Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

### Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch , that lead to scams and rugpulls.

### Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

Exploits

 Back-doors  Vulnerability  Accuracy

 Readability

### Tools

 Manual Review: The code has undergone a line-by-line review by the Ace team.

 ETH Test Network: All tests were conducted on the ETH Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

 Slither: The code has undergone static analysis using Slither.

**7**



# VULNERABILITY CHECKS

**Design Logic Compiler warnings**

**Private user data leaks Timestamps dependence Integer overflow and underflow**

**Race conditions & reentrancy. Cross-function race conditions Possible delays in data delivery**

**Oracle calls Front Running DoS with Revert**

**DoS with block gas limit Methods execution permissions Economy model**

**Impact of the exchange rate on the logic Malicious event log**

**Scoping and declarations Uninitialized storage pointers Arithmetic accuracy**

**Cross-function race conditions**

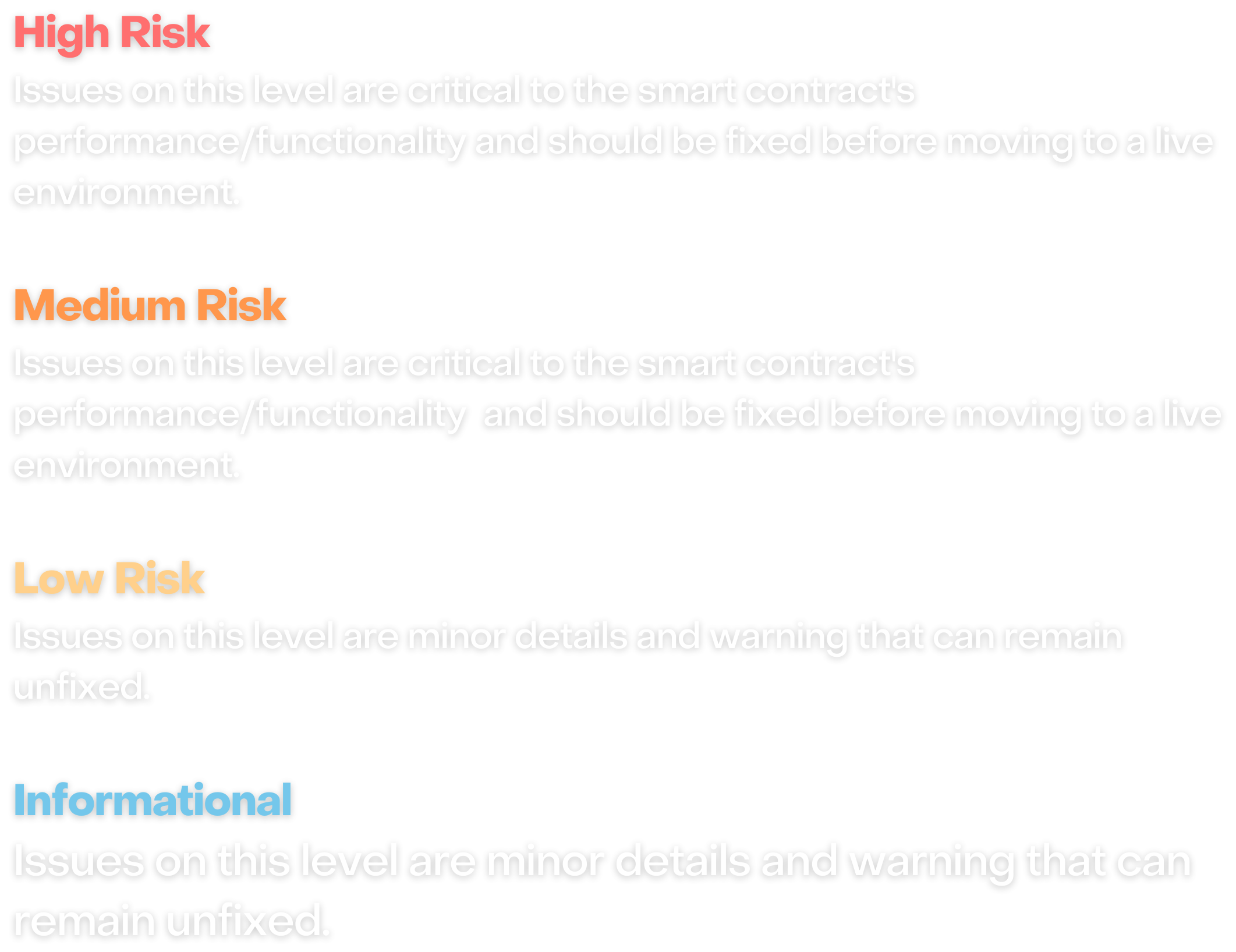
**Safe Zepplin module**

Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed Passed

Passed



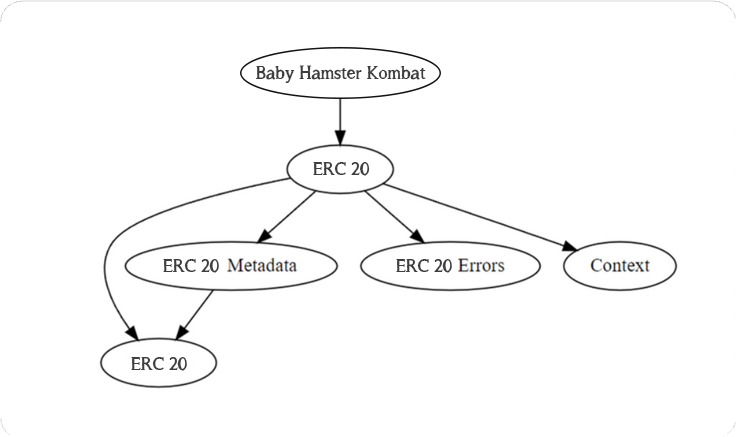
**8**



# RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

**9**



# INHERITANCE TREE

**10**



# TESTNET VERSION

1. **Approve (passed):** https://basescan.org/token/0x089D91926e43cd7318198922D548189470cA25f2#code
2. **Transfer (passed):** https://basescan.org/token/0x089D91926e43cd7318198922D548189470cA25f2#code

**11**



# MANUAL REVIEW

### Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk categroies: High

Medium Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

Malicious input handling Escalation of privileges Arithmetic

Gas use

**12**



**INFORMATIONAL FINDINGS**

Optimization

Severity: Informational

Subject: Floating Pragma Solidity version Status: Open

Overview:

It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

pragma solidity ^0.8.26;

Suggestion:

Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

**13**



# ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.



**14**



# DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

