expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

$ELY

TOKEN OVERVIEW

Risk Findings

Severity	Found
🔴 High	1
🟠 Medium	1
🟡 Low	0
🔵 Informational	0

Centralization Risks

Owner Privileges	Description
🟢 Can Owner Set Taxes >25% ?	Not Detected
🟢 Owner needs to enable trading ?	Not Detected
🟢 Can Owner Disable Trades ?	Not Detected
🟢 Can Owner Mint ?	Not Detected
🟢 Can Owner Blacklist ?	Not Detected
🟢 Can Owner set Max Wallet amount ?	Not Detected
🟢 Can Owner Set Max TX amount ?	Not Detected

TABLE OF CONTENTS

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:

Audit Result	Passed
KYC Verification	-
Audit Date	11 June 2023

CONTRACT DETAILS

Token Name: Elyssa AR

Symbol: $ELY

Network: Ethereum

Language: Solidity

Contract Address: ---

Total Supply: 10,000,000

Owner's Wallet: ---

Deployer's Wallet: ---

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

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zepplin module	Passed

expelee

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:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.
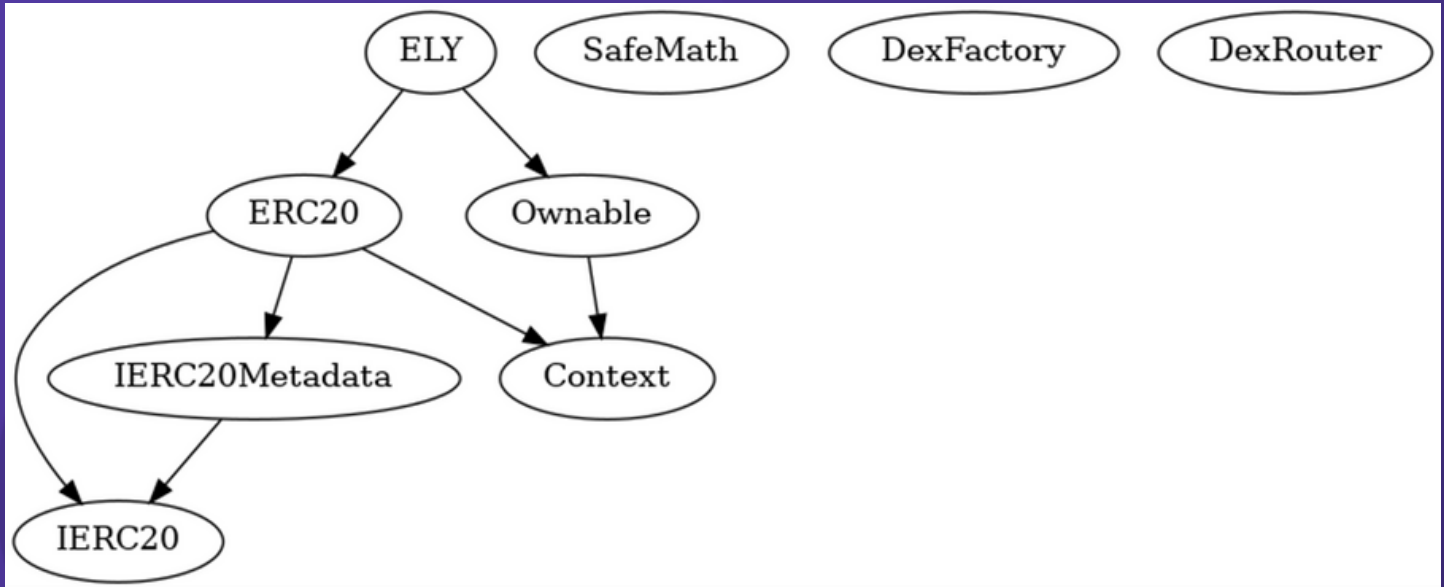
Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Issues on this level are minor details and warning that can remain unfixed.

INHERITANCE TREES

TESTNET VERSION

Adding Liquidity ✓
Tx:
https://testnet.bscscan.com/tx/0x4825926095902a078f0fbe
afb29ba3a606154012f39666fdcb32453b0201e1f6

===

Buying from a fee excluded wallet ✓
Tx (0% tax):
https://testnet.bscscan.com/tx/0x44b4bb4d59e875bb050c2c
65588b2e00333aecf7dc025c737d3d03aceb427da8

===

Selling from a fee excluded wallet ✓
Tx (0% tax):
https://testnet.bscscan.com/tx/0x94d3aead406e48e54dc02b
d2e4141c6055dbf3315d5762854f6561e28adec1da

===

Transferring using a fee excluded wallet ✓
Tx (0% tax):
https://testnet.bscscan.com/tx/0x8ba852648b94a8355d5b9a
3398cf7017b0baf47c732df800371f3b2bd723a16a

===

TESTNET VERSION

Buying from a regular wallet ✓
Tx (0-10% tax):
https://testnet.bscscan.com/tx/0xac9e27b2418d1a1e3c9ae7622cfcaa6819d39ed5b1e778bc6198a35456bee092

===

Selling from a regular wallet ✓
Tx (0-10% tax):
https://testnet.bscscan.com/tx/0x495d09b619806b72f223eb4c0f72a5fec6a6b6b95649784ef825563952ec3853

===

Transferring a regular wallet ✓
Tx (0%):
https://testnet.bscscan.com/tx/0xecd32ecdb0599cbfd2820a27d4154ff87737b9fabad8fec01c0e17cc925612f1

===

Internal swap (marketing BNB) ✓
Tx:
https://testnet.bscscan.com/address/0xaad239ed60773e34b8b1682214f7015c845bfb57#internaltx

===

FUNCTION DETAILS

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface	|||		
└	totalSupply	External ❗	|NO ❗	
└	balanceOf	External ❗	|NO ❗	
└	transfer	External ❗	🔴 |NO ❗	
└	allowance	External ❗	|NO ❗	
└	approve	External ❗	🔴 |NO ❗	
└	transferFrom	External ❗	🔴 |NO ❗	
Context	Implementation	|||		
└	_msgSender	Internal 🔒	||	
└	_msgData	Internal 🔒	||	
IERC20Metadata	Interface	IERC20 |||		
└	name	External ❗	|NO ❗	
└	symbol	External ❗	|NO ❗	
└	decimals	External ❗	|NO ❗	
ERC20	Implementation	Context, IERC20, IERC20Metadata |||		
└	\<Constructor\>	Public ❗	🔴 |NO ❗	
└	name	Public ❗	|NO ❗	
└	symbol	Public ❗	|NO ❗	
└	decimals	Public ❗	|NO ❗	
└	totalSupply	Public ❗	|NO ❗	
└	balanceOf	Public ❗	|NO ❗	
└	transfer	Public ❗	🔴 |NO ❗	

FUNCTION DETAILS

```
| └ | allowance | Public ❗ | | |NO ❗ |
| └ | approve | Public ❗ | 🔴 |NO ❗ |
| └ | transferFrom | Public ❗ | 🔴 |NO ❗ |
| └ | increaseAllowance | Public ❗ | 🔴 |NO ❗ |
| └ | decreaseAllowance | Public ❗ | 🔴 |NO ❗ |
| └ | _transfer | Internal 🔒 | 🔴 ||
| └ | _mint | Internal 🔒 | 🔴 ||
| └ | _burn | Internal 🔒 | 🔴 ||
| └ | _approve | Internal 🔒 | 🔴 ||
| └ | _spendAllowance | Internal 🔒 | 🔴 ||
| └ | _beforeTokenTransfer | Internal 🔒 | 🔴 ||
| └ | _afterTokenTransfer | Internal 🔒 | 🔴 ||
||||||
| **SafeMath** | Library | |||
| └ | tryAdd | Internal 🔒 | ||
| └ | trySub | Internal 🔒 | ||
| └ | tryMul | Internal 🔒 | ||
| └ | tryDiv | Internal 🔒 | ||
| └ | tryMod | Internal 🔒 | ||
| └ | add | Internal 🔒 | ||
| └ | sub | Internal 🔒 | ||
| └ | mul | Internal 🔒 | ||
| └ | div | Internal 🔒 | ||
| └ | mod | Internal 🔒 | ||
| └ | sub | Internal 🔒 | ||
| └ | div | Internal 🔒 | ||
| └ | mod | Internal 🔒 | ||
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗ | 🔴 |NO ❗ |
| └ | owner | Public ❗ | | |NO ❗ |
| └ | _checkOwner | Internal 🔒 | ||
| └ | renounceOwnership | Public ❗ | 🔴 | onlyOwner |
| └ | transferOwnership | Public ❗ | 🔴 | onlyOwner |
| └ | _transferOwnership | Internal 🔒 | 🔴 ||
||||||
| **DexFactory** | Interface | |||
| └ | createPair | External ❗ | 🔴 |NO ❗ |
||||||
| **DexRouter** | Interface | |||
| └ | factory | External ❗ | | |NO ❗ |
| └ | WETH | External ❗ | | |NO ❗ |
| └ | addLiquidityETH | External ❗ | 🟩 |NO ❗ |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ❗ | 🔴 |NO ❗ |
||||||
| **ELY** | Implementation | ERC20, Ownable |||
```

FUNCTION DETAILS

```
| └ | <Constructor> | Public ❗ | 🔴 | ERC20 |
| └ | setmarketingWallet | External ❗ | 🔴 | onlyOwner |
| └ | setSwapTokensAtAmount | External ❗ | 🔴 | onlyOwner |
| └ | toggleSwapping | External ❗ | 🔴 | onlyOwner |
| └ | setWhitelistStatus | External ❗ | 🔴 | onlyOwner |
| └ | checkWhitelist | External ❗ | |NO ❗ | |
| └ | startTrading | External ❗ | 🔴 | onlyOwner |
| └ | updateBuyTax | External ❗ | 🔴 | onlyOwner |
| └ | updateSellTax | External ❗ | 🔴 | onlyOwner |
| └ | _takeTax | Internal 🔒 | 🔴 ||
| └ | _transfer | Internal 🔒 | 🔴 ||
| └ | internalSwap | Internal 🔒 | 🔴 ||
| └ | swapToETH | Internal 🔒 | 🔴 ||
| └ | adjustDeadBlock | External ❗ | 🔴 | onlyOwner |
| └ | removeLimits | External ❗ | 🔴 | onlyOwner |
| └ | _antiBot | Internal 🔒 | 🔴 ||
| └ | withdrawStuckETH | External ❗ | 🔴 | onlyOwner |
| └ | withdrawStuckTokens | External ❗ | 🔴 | onlyOwner |
| └ | <Receive Ether> | External ❗ | 💵 |NO ❗ | |
```

Legend

Symbol	Meaning
🔴	Function can modify state
💵	Function is payable

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

			Overall Risk Severity	
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
			Likelihood	

HIGH RISK FINDING

Category: Centralization

Subject: Blacklisting

Impact : High

Status: Open

Overview

Owner of the contract is able to blacklist one or multiple number of wallets. Blacklisted wallets wont be able to buy/sell/transfer tokens.

```
    function blacklistAddress(address _target, bool _status) external onlyOwner {
        if (_status) {
require(_target != pairAddress, "Can't blacklist liquidity pool");
require(_target != address(this), "Can't blacklisted the token");
        }
isBlacklisted[_target] = _status;
    }

    function blacklistAddresses(address[] memory _targets, bool[] memory
_status) external onlyOwner {
        for (uint256 i = 0; i < _targets.length; i++) {
        if (_status[i]) {
require(_targets[i] != pairAddress, "Can't blacklist liquidity pool");
require(_targets[i] != address(this), "Can't blacklisted the token");
        }
isBlacklisted[_targets[i]] = _status[i];
    }
  }
```

Suggestion:

there are multiple ways to resolve this centralization issue:
- declare all the actions that may blacklist a wallet
- create an automated method to blacklist a bad actor

expelee

MEDIUM RISK FINDING

Category: Centralization
Subject: Excessive sell taxes
Impact : Medium
Status: Open

Overview

Owner of the contract is able to set up to 40% tax on sells.

```
  function updateSellTax(uint256 marketingTax) external onlyOwner {
require(marketingTax <= 40, "can't set buy tax over 30%");
sellTaxes.marketingTax = marketingTax;
  }
```

Overview

Its suggested to keep sell taxes in a more safe and reasonable range which is 0-10%

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.

www.expelee.com

🐦 expeleeofficial   Ⓜ expelee

✈ Expelee   in expelee

📷 expelee_official   ⓞ expelee-co

expelee

Building the Futuristic Blockchain Ecosystem

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.

Building the Futuristic Blockchain Ecosystem