



Building the Futuristic **Blockchain** Ecosystem

SECURITY AUDIT REPORT

AKITAKAI

TOKEN OVERVIEW

Risk Findings

Severity	Found
● High	0
● Medium	2
● 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

02	Token Overview	
03	Table of Contents	
04	Overview	
05	Contract Details	
06	Audit Methodology	
07	Vulnerabilities Checklist	
08	Risk Classification	
09	Inheritance Trees & Risk Overview	
10	Testnet Version	
12	Function Details	
15	Manual Review	
16	Findings	
18	About Expelee	
19	Disclaimer	

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	23 June 2023

CONTRACT DETAILS

Token Name: AKITAKAI

Symbol: \$AKIKA

Network: Binance smart chain

Language: Solidity

Contract Address:

0xD7fC8A3a10cbb0bA6a6Ebc6C3AA8B406a22Fc571

Total Supply: 1,000,000,000,000

Owner's Wallet:

0x0aBef54dd435E0414926E00b17361875e8ec8C61

Deployer's Wallet:

0x0aBef54dd435E0414926E00b17361875e8ec8C61

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

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access 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.

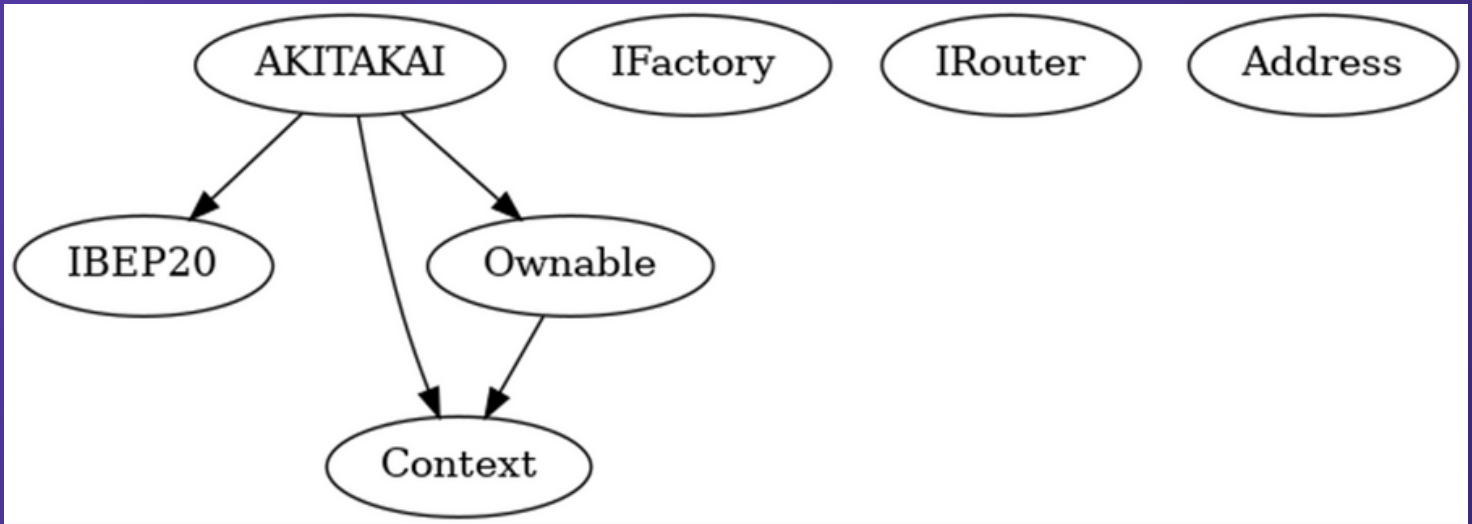
Low Risk

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

Informational

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

INHERITANCE TREES



TESTNET VERSION

Adding Liquidity ✓

Tx:

<https://testnet.bscscan.com/tx/0x4d6aadca352159f4ddb3103e11ede88b15b9eac9b700fcb9c617562591db9a45>

=====

Buying when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x6fbec81c2a299c4ea78f190801f7074329e05e65457118f6dc326a4189f3b676>

=====

Selling when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x3de118e0cf8e2ccc8b5bdf4e4bb046afb6a88b08c42cdd724b2ee773b292eae5>

=====

Transferring when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xd114a5a2e0e8750f5b14cb363dcf1246334b230a803615bd5aedc4ded6f52adc>

=====

TESTNET VERSION

Buying ✓

Tx (5% tax):

<https://testnet.bscscan.com/tx/0x1e3de8d7b7fb4809232e87361bc896ec271b675151db97f6b204675879891830>

=====

Selling ✓

Tx (5% tax):

<https://testnet.bscscan.com/tx/0x0434bcfeb153c303d3e4d090f5bc2766db4540da3afdb8a5525fab7146282ba8>

=====

Transferring ✓

Tx (5% tax):

<https://testnet.bscscan.com/tx/0x9fe122baceb964a96d371e00406dd9b5dbe5349e5215ed8d440e4417361ae8f7>

=====

Internal swap (marketing wallet received BNB) ✓

Tx :

<https://testnet.bscscan.com/address/0x01a3e9f8c45c767499d00aadaaf13266a3f3c89e4#internaltx>

=====

FUNCTION DETAILS

Contract	Type	Bases			
----- ----- ----- ----- -----					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
IBEP20 Interface					
L	totalSupply	External !	NO !		
L	balanceOf	External !	NO !		
L	transfer	External !	● NO !		
L	allowance	External !	NO !		
L	approve	External !	● NO !		
L	transferFrom	External !	● NO !		
Context Implementation					
L	_msgSender	Internal 🔒			
L	_msgData	Internal 🔒			
Ownable Implementation Context					
L	<Constructor>	Public !	● NO !		
L	owner	Public !	NO !		
L	renounceOwnership	Public !	● onlyOwner		
L	transferOwnership	Public !	● onlyOwner		
L	_setOwner	Private 🔒	●		
IFactory Interface					
L	createPair	External !	● NO !		
IRouter Interface					
L	factory	External !	NO !		
L	WETH	External !	NO !		
L	addLiquidityETH	External !	🇺🇸 NO !		
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External !	● NO !		

FUNCTION DETAILS

```

#####
| **Address** | Library | |||
| L | sendValue | Internal | 🔒 | ● | |
#####
| **AKITAKAI** | Implementation | Context, IBEP20, Ownable ||| |
| L | <Constructor> | Public | ! | ● | NO ! |
| L | name | Public | ! | | NO ! |
| L | symbol | Public | ! | | NO ! |
| L | decimals | Public | ! | | NO ! |
| L | totalSupply | Public | ! | | NO ! |
| L | balanceOf | Public | ! | | NO ! |
| L | allowance | Public | ! | | NO ! |
| L | approve | Public | ! | ● | NO ! |
| L | transferFrom | Public | ! | ● | NO ! |
| L | increaseAllowance | Public | ! | ● | NO ! |
| L | decreaseAllowance | Public | ! | ● | NO ! |
| L | transfer | Public | ! | ● | NO ! |
| L | isExcludedFromReward | Public | ! | | NO ! |
| L | reflectionFromToken | Public | ! | | NO ! |
| L | tokenFromReflection | Public | ! | | NO ! |
| L | excludeFromReward | Public | ! | ● | onlyOwner |
| L | includeInReward | External | ! | ● | onlyOwner |
| L | excludeFromFee | Public | ! | ● | onlyOwner |
| L | includeInFee | Public | ! | ● | onlyOwner |
| L | isExcludedFromFee | Public | ! | | NO ! |
| L | _reflectRfi | Private | 🔒 | ● | |
| L | _takeMarketing | Private | 🔒 | ● | |
| L | _getValues | Private | 🔒 | | |
| L | _getTValues | Private | 🔒 | | |
| L | _getRValues | Private | 🔒 | | |
| L | _getRate | Private | 🔒 | | |
| L | _getCurrentSupply | Private | 🔒 | | |
| L | _approve | Private | 🔒 | ● | |
| L | _transfer | Private | 🔒 | ● | |
| L | _tokenTransfer | Private | 🔒 | ● | |
| L | swapAndLiquify | Private | 🔒 | ● | lockTheSwap |
| L | swapTokensForBNB | Private | 🔒 | ● | |
| L | bulkExcludeFee | External | ! | ● | onlyOwner |
| L | updateMarketingWallet | External | ! | ● | onlyOwner |
| L | updateSwapTokensAtAmount | External | ! | ● | onlyOwner |
| L | rescueBNB | External | ! | ● | onlyOwner |
| L | rescueAnyBEP20Tokens | Public | ! | ● | onlyOwner |
| L | <Receive Ether> | External | ! | 🟢 | NO ! |

```

Legend

FUNCTION DETAILS

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 standards.

Vulnerabilities are divided into three primary risk categories:

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: Numerical

Subject: Invalid input validation for updating numTokensSellToAddToLiquidity

Status: Open

Severity : Medium

Overview

updateSwapTokensAtAmount validates amount to be less than $1e15$ (1,000,000,000,000,000), but this amount is not 1% of total supply.

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner
{
    require(amount <= 1e15, "Cannot set swap threshold amount higher than 1%
of tokens");
    swapTokensAtAmount = amount * 10 ** _decimals;
}
```

Suggestion

Ensure that inputs are validated correctly:

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(amount <= 1e10, "Cannot set swap threshold amount higher than 1% of
tokens");
    swapTokensAtAmount = amount * 10 ** _decimals;
}
```


HIGH RISK FINDING

Category: Configuration

Subject: Upgrading marketing wallet to an ETH rejector

Status: Open

Severity : Medium

Overview

if marketing wallet is set to a contract that doesn't accept ether (rejects ether upon receiving), internal swap could be failed resulting in sell failure.

```
function swapAndLiquify() private lockTheSwap {
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForBNB(contractBalance);
    uint256 deltaBalance = address(this).balance;

    if (deltaBalance > 0) {
        payable(marketingWallet).sendValue(deltaBalance);
    }
}
```

Suggestion

Adjust sendValue function to ignore "success".

```
function sendValue(address payable recipient, uint256 amount) internal {
    require(address(this).balance >= amount, "Address: insufficient balance");

    (bool success,) = recipient.call{value: amount}("");
}
```

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



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.

The logo for Expelee, featuring the word "expelee" in a stylized font. The "ex" is in white, and "pelee" is in orange. The letters are bold and modern.

Building the Futuristic **Blockchain Ecosystem**