

**Building the Futuristic Blockchain Ecosystem** 

# SECURITY AUDIT REPORT

**Toker Token** 



### **TOKEN OVERVIEW**

### **Risk Findings**

Severity	Found	
High	1	
Medium	0	
Low	0	
Informational	0	

### **Centralization Risks**

Owner Privileges	Description
Can Owner Set Taxes >25%?	Not Detected
Owner needs to enable trading?	Yes, owner needs to enable trades
Can Owner Disable Trades ?	Not Detected
Can Owner Mint?	Not Detected
Can Owner Blacklist?	Not Detected
Can Owner set Max Wallet amount ?	Not Detected
<ul><li>Can Owner Set Max Transfer amount</li></ul>	? Not Detected



# TABLE OF CONTENTS

Token Overview ————————————————————————————————————
Table of Contents
Overview
Contract Details ————————————————————————————————————
Audit Methodology
Vulnerabilities Checklist
Risk Classification
Inheritence Trees
Function Details
Testnet Version
Manual Review ————————————————————————————————————
About Expelee
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 With High Risk
KYC Verification	-
Audit Date	25 June 2023



### **CONTRACT DETAILS**

Token Name: Toker Token

Symbol: THC

**Network: Binance Smart Chain** 

Language: Solidity

**Contract Address:** 

--

Total Supply: 840,000,000,000,000

Owner's Wallet: --

Deployer's Wallet: --

Testnet.

https://testnet.bscscan.com/address/0x776394ebfd85A61e



# 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 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**

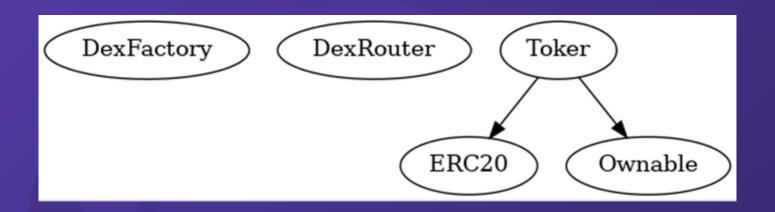
Issues on this level are minor details and warning that can remain unfixed.

#### **Informational**

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



### **INHERITANCE TREES**





### **FUNCTION DETAILS**

```
Type
                     Bases
 Contract
      | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| **DexFactory** | Interface | |||
L | createPair | External | | | NO | |
| **DexRouter** | Interface | |||
L | factory | External | NO | |
 L | WETH | External | | NO | |
 | addLiquidityETH | External | | 1 | NO | |
 **Toker** | Implementation | ERC20, Ownable ||
 └ | <Constructor> | Public | | ● | ERC20 |
 enableTrading | External | | • | onlyOwner |
 └ | setTransferFees | External | | ● | onlyOwner |
 └ | setWhitelistStatus | External | | ● | onlyOwner |
 | checkWhitelist | External | NO | |
L | takeTax | Internal 🔒 | 🛑 | |
 L | transfer | Internal 🔒 | 🛑 | |
 └ | swapToETH | Internal 🔒 | 🛑 | |
 | withdrawStuckETH | External | | | onlyOwner |
 | withdrawStuckTokens | External | | | onlyOwner |
 ### Legend
| Symbol | Meaning
|:-----|
     | Function can modify state |
     | Function is payable |
```



### **TESTNET VERSION**

Adding Liquidity  Tx:
https://testnet.bscscan.com/tx/0xf5b2f50e4ef9547c7af8cb44c26ea101161b38e306l79e8dbd79d40ea4adf23d
Buying when excluded from fees   Tx (0% tax):  https://testnet.bscscan.com/tx/0x98aefa1f19164e4558532fbc8da5386d55be8c5208e6ae0a78c17f93314eed63
Selling when excluded from fees  Tx (0% tax): https://testnet.bscscan.com/tx/0xfe9886c27f9e34228d10ae783c7a4a2a0d3db06460a0ee0d341b08a0c788a2f
Transferring when excluded from fees Tx (0% tax):  https://testnet.bscscan.com/tx/0x9907f252a1e3588a9ea698c02d56c1a23073bf918df31875967c66408beb3b3
Puving 2

Tx (0-5% tax):

https://testnet.bscscan.com/tx/0xf864c749f2639c5ade6ad06e4cdce018bbb1712728b0d6f80418ab7c1302ef6e



### **TESTNET VERSION**

Se	lling 🕻	
Tx	(0-5%	tax):

https://testnet.bscscan.com/tx/0x45b0f5067b96df74ce765f7a94a76271386680e7a0 02eaa760445414d89ce6fb



https://testnet.bscscan.com/tx/0x69d4bd69b91667cf449b07d5753c4b1450b2059c6 7ad4e91d51e71f0df8def07

Burning (fee are sent to dead wallet) 🗸



https://testnet.bscscan.com/token/0x776394ebfd85a61e18f627f4afb65b53cf5816e1? 



### **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**

### **Trades must be enabled manually**

**Category: Centralization** 

Status: Open

**Severity: High** 

**Overview:** 

Owner of the contract must call startTrading function in order for holders to be able to transfer/sell their tokens. If Owner refuse to enable trades for any reason, holders wont be able to transfer/sell their tokens and their assets will be locked in liquidity pool forever.

```
function enableTrading() external onlyOwner {
require(!tradingEnabled, "Trading is already enabled");
  tradingEnabled = true;
  startTradingBlock = block.number;
}
```



### **HIGH RISK FINDING**

### Trades must be enabled manually

### Suggestion:

#### To resolve this issue you can:

- Enable trades prior to presale: this ensures investors about safety of their assets
- Transfer ownreship of the contract to pinksale: this ensures that trades will be enabled eventually at right time
- Create a time lock feature: this ensures that trades will be enabled automatically after a fixed amount of time.



### **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



**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**