expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

Venom CEO

expelee

TOKEN OVERVIEW

Risk Findings

Severity	Found
🔴 High	0
🟠 Medium	0
🟡 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	**16 July 2023**

CONTRACT DETAILS

Token Name: Venom CEO

Symbol: VCEO

Network: Binance Smart Chain

Language: Solidity

Contract Address:
0xFff3382E667863770dCbeb66a7C30A1E6F3deD06

Total Supply: 3,000,000

Owner's Wallet:
0xDbCdD6ce039Dbe46FC9CB949d44f153F63edE719

Deployer's Wallet:
0xDbCdD6ce039Dbe46FC9CB949d44f153F63edE719

Testnet.
https://testnet.bscscan.com/token/0x6C1deea6f8156eDc7D
da26e9d0E065bb53F971d1

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.
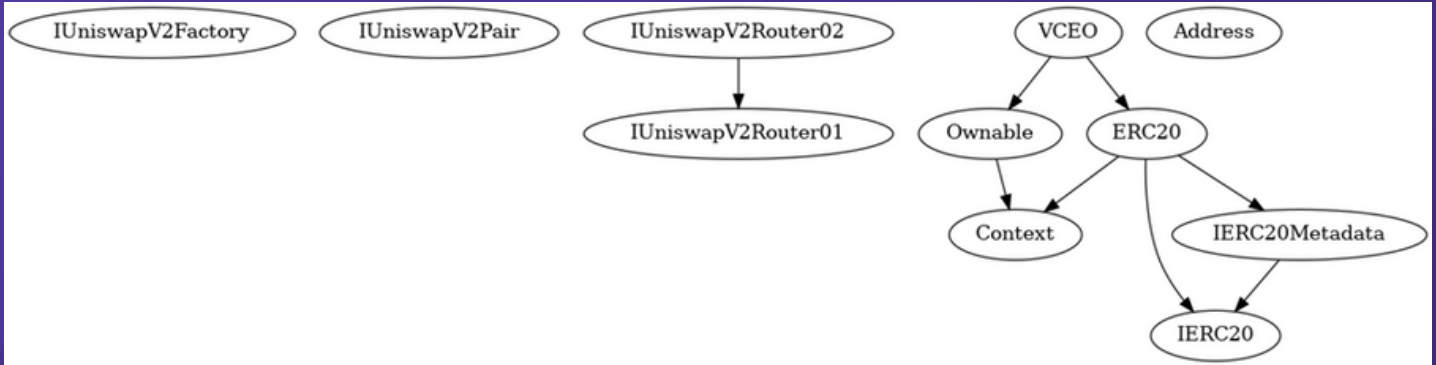
Low Risk

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

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**

IUniswapV2Factory	Interface	|||	
└	feeTo	External ❗	|NO ❗	
└	feeToSetter	External ❗	|NO ❗	
└	getPair	External ❗	|NO ❗	
└	allPairs	External ❗	|NO ❗	
└	allPairsLength	External ❗	|NO ❗	
└	createPair	External ❗	🔴 |NO ❗	
└	setFeeTo	External ❗	🔴 |NO ❗	
└	setFeeToSetter	External ❗	🔴 |NO ❗	

IUniswapV2Pair	Interface	|||	
└	name	External ❗	|NO ❗	
└	symbol	External ❗	|NO ❗	
└	decimals	External ❗	|NO ❗	
└	totalSupply	External ❗	|NO ❗	
└	balanceOf	External ❗	|NO ❗	
└	allowance	External ❗	|NO ❗	
└	approve	External ❗	🔴 |NO ❗	
└	transfer	External ❗	🔴 |NO ❗	
└	transferFrom	External ❗	🔴 |NO ❗	
└	DOMAIN_SEPARATOR	External ❗	|NO ❗	
└	PERMIT_TYPEHASH	External ❗	|NO ❗	
└	nonces	External ❗	|NO ❗	
└	permit	External ❗	🔴 |NO ❗	
└	MINIMUM_LIQUIDITY	External ❗	|NO ❗	
└	factory	External ❗	|NO ❗	
└	token0	External ❗	|NO ❗	
└	token1	External ❗	|NO ❗	
└	getReserves	External ❗	|NO ❗	
└	price0CumulativeLast	External ❗	|NO ❗	
└	price1CumulativeLast	External ❗	|NO ❗	
└	kLast	External ❗	|NO ❗	
└	mint	External ❗	🔴 |NO ❗	
└	burn	External ❗	🔴 |NO ❗	
└	swap	External ❗	🔴 |NO ❗	
└	skim	External ❗	🔴 |NO ❗	
└	sync	External ❗	🔴 |NO ❗	
└	initialize	External ❗	🔴 |NO ❗	

IUniswapV2Router01	Interface	|||	
└	factory	External ❗	|NO ❗	
└	WETH	External ❗	|NO ❗	

FUNCTION DETAILS

```
| └ | addLiquidity | External ! | ● |NO ! |
| └ | addLiquidityETH | External ! | 🔳 |NO ! |
| └ | removeLiquidity | External ! | ● |NO ! |
| └ | removeLiquidityETH | External ! | ● |NO ! |
| └ | removeLiquidityWithPermit | External ! | ● |NO ! |
| └ | removeLiquidityETHWithPermit | External ! | ● |NO ! |
| └ | swapExactTokensForTokens | External ! | ● |NO ! |
| └ | swapTokensForExactTokens | External ! | ● |NO ! |
| └ | swapExactETHForTokens | External ! | 🔳 |NO ! |
| └ | swapTokensForExactETH | External ! | ● |NO ! |
| └ | swapExactTokensForETH | External ! | ● |NO ! |
| └ | swapETHForExactTokens | External ! | 🔳 |NO ! |
| └ | quote | External ! | |NO ! |
| └ | getAmountOut | External ! | |NO ! |
| └ | getAmountIn | External ! | |NO ! |
| └ | getAmountsOut | External ! | |NO ! |
| └ | getAmountsIn | External ! | |NO ! |
||||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| └ | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
| └ | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|
| └ | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● |NO ! |
| └ | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🔳 |NO ! |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
||||||
| **IERC20** | Interface | |||
| └ | totalSupply | External ! | |NO ! |
| └ | balanceOf | External ! | |NO ! |
| └ | transfer | External ! | ● |NO ! |
| └ | allowance | External ! | |NO ! |
| └ | approve | External ! | ● |NO ! |
| └ | transferFrom | External ! | ● |NO ! |
||||||
| **IERC20Metadata** | Interface | IERC20 |||
| └ | name | External ! | |NO ! |
| └ | symbol | External ! | |NO ! |
| └ | decimals | External ! | |NO ! |
||||||
| **Address** | Library | |||
| └ | isContract | Internal 🔒 | ||
| └ | sendValue | Internal 🔒 | ● ||
| └ | functionCall | Internal 🔒 | ● ||
| └ | functionCall | Internal 🔒 | ● ||
| └ | functionCallWithValue | Internal 🔒 | ● ||
| └ | functionCallWithValue | Internal 🔒 | ● ||
```

FUNCTION DETAILS

```
| └ | functionStaticCall | Internal 🔒 | ||
| └ | functionStaticCall | Internal 🔒 | ||
| └ | functionDelegateCall | Internal 🔒 | 🔴 ||
| └ | functionDelegateCall | Internal 🔒 | 🔴 ||
| └ | verifyCallResultFromTarget | Internal 🔒 | ||
| └ | verifyCallResult | Internal 🔒 | ||
| └ | _revert | Private 🔒 | ||
||||||
| **Context** | Implementation | |||
| └ | _msgSender | Internal 🔒 | ||
| └ | _msgData | Internal 🔒 | ||
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗ | 🔴 |NO ❗ |
| └ | owner | Public ❗ | |NO ❗ |
| └ | renounceOwnership | Public ❗ | 🔴 | onlyOwner |
| └ | transferOwnership | Public ❗ | 🔴 | onlyOwner |
||||||
| **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 ❗ |
| └ | allowance | Public ❗ | |NO ❗ |
| └ | approve | Public ❗ | 🔴 |NO ❗ |
| └ | transferFrom | Public ❗ | 🔴 |NO ❗ |
| └ | increaseAllowance | Public ❗ | 🔴 |NO ❗ |
| └ | decreaseAllowance | Public ❗ | 🔴 |NO ❗ |
| └ | _transfer | Internal 🔒 | 🔴 ||
| └ | _mint | Internal 🔒 | 🔴 ||
| └ | _burn | Internal 🔒 | 🔴 ||
| └ | _approve | Internal 🔒 | 🔴 ||
| └ | _beforeTokenTransfer | Internal 🔒 | 🔴 ||
| └ | _afterTokenTransfer | Internal 🔒 | 🔴 ||
||||||
| **VCEO** | Implementation | ERC20, Ownable |||
| └ | <Constructor> | Public ❗ | 🔴 | ERC20 |
| └ | <Receive Ether> | External ❗ | 💵 |NO ❗ |
| └ | claimStuckTokens | External ❗ | 🔴 | onlyOwner |
| └ | excludeFromFees | External ❗ | 🔴 | onlyOwner |
| └ | isExcludedFromFees | Public ❗ | |NO ❗ |
| └ | updateBuyFees | External ❗ | 🔴 | onlyOwner |
| └ | updateSellFees | External ❗ | 🔴 | onlyOwner |
```

FUNCTION DETAILS

└	updateWalletToWalletTransferFee	External ❗	🔴	onlyOwner
└	changeMarketingWallet	External ❗	🔴	onlyOwner
└	_transfer	Internal 🔒	🔴	
└	setSwapTokensAtAmount	External ❗	🔴	onlyOwner
└	swapAndLiquify	Private 🔐	🔴	
└	swapAndSendMarketing	Private 🔐	🔴	

Legend

Symbol	Meaning
🔴	Function can modify state
💵	Function is payable

TESTNET VERSION

Adding Liquidity ✅
Tx:
https://testnet.bscscan.com/tx/0x2e0372b682009fd6f8a85c558a31a73ab96cee43d7138c1a4305af730863cef1

==

Buying when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xaeed26320e0518f9ae7ddac290d893b0e029715b614ced6c1a2ad5a31c9e2727

==

Selling when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x4119d1895bad1fc00922b4ee165bf72224c5300c15bc321fbf03cc95ed571a61

==

Transferring when exclduded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x800b1efd22a9030509013fe5b84a6067f3cead1da8c4ffc23a92f1f1cdd71bc7

==

Buying ✅
Tx (0-20% tax):
https://testnet.bscscan.com/tx/0x654788e4f9aad8649c30a875f948d25992baff987eb454d58c0b9d6e31eb5aac

TESTNET VERSION

Selling ✅
Tx (0-20% tax):
https://testnet.bscscan.com/tx/0x89c9316342292c5b6ff37bf81d956190126c1987441a27442dcef88164bdda20
==

Transferring ✅
Tx (0-15% tax):
https://testnet.bscscan.com/tx/0x4aa97fd6e831241601e6b08c285595db2223d6e888cae22bac10eb3fe6dc1607

==

Internal swap (auto-liquidity | BNB to marketing wallet) ✅
Tx:
https://testnet.bscscan.com/address/0xdbcdd6ce039dbe46fc9cb949d44f153f63ede719#internaltx
https://testnet.bscscan.com/token/0xb20df51eb662a2f426f72009a8e9efb5fbef0069?a=0x000000000000000000000000000000000000dead

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		

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.

expelee

Building the Futuristic Blockchain Ecosystem