



Building the Futuristic **Blockchain** Ecosystem

SECURITY AUDIT REPORT

UNIVEL

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	29 June 2023

CONTRACT DETAILS

Token Name: Univel

Symbol: VEL

Network: Ethereum

Language: Solidity

Contract Address:

0x7691e5cA3977168a9CE8ec434Ea54A81032Ed86c

Total Supply: 500,000,000

Owner's Wallet:

0xa28DF9e14fa8560ADb0a2D74e5094c8b902d3C7b

Deployer's Wallet:

0xa28DF9e14fa8560ADb0a2D74e5094c8b902d3C7b

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 Zeppelin 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.

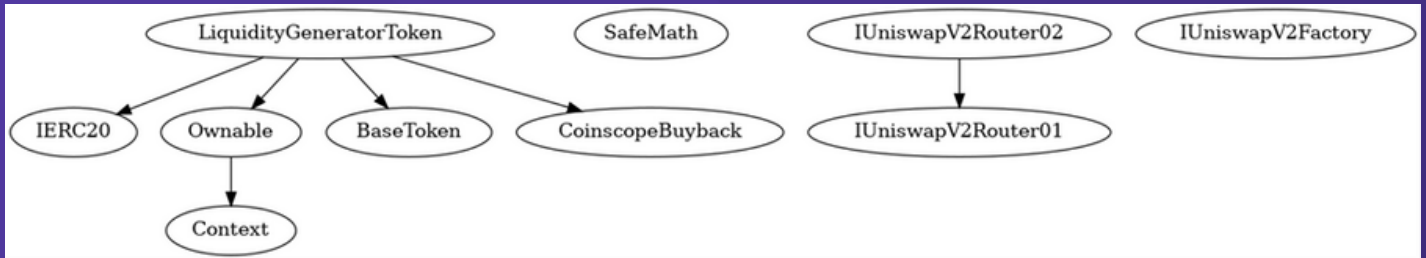
Low Risk

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/0x8f1f06c1691637b6d348ad2506b5e8adb67effa20dd61e09085a13e8965eb4cf>

=====

Buying when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x4e03af4237bed203abd59ce4fc7cdb3b6f42199be793974d523542d80e6e4404>

=====

Selling when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xa0ca408976230273ecb8f7689bbd267f91185789a901f1c75839b812761571a4>

=====

Transferring when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x3fecf9264c1f497a09d510dc34f846eccc76318ff72d64934d74854661742505>

=====

TESTNET VERSION

Adding Liquidity ✓

Tx:

<https://testnet.bscscan.com/tx/0x8f1f06c1691637b6d348ad2506b5e8adb67effa20dd61e09085a13e8965eb4cf>

=====

Buying when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x4e03af4237bed203abd59ce4fc7cdb3b6f42199be793974d523542d80e6e4404>

=====

Selling when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xa0ca408976230273ecb8f7689bbd267f91185789a901f1c75839b812761571a4>

=====

Transferring when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x3fecf9264c1f497a09d510dc34f846eccc76318ff72d64934d74854661742505>

=====

FUNCTION DETAILS

Contract	Type	Bases			
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
IERC20	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	🔒		
Ownable	Implementation	Context			
L	<Constructor>	Public	!	●	NO !
L	owner	Public	!		NO !
L	renounceOwnership	Public	!	●	onlyOwner
L	transferOwnership	Public	!	●	onlyOwner
L	_setOwner	Private	🔒	●	
SafeMath	Library				
L	sub	Internal	🔒		
IUniswapV2Router01	Interface				
L	factory	External	!		NO !
L	WETH	External	!		NO !
L	WETC	External	!		NO !
L	WHT	External	!		NO !
L	WROSE	External	!		NO !
L	WAVAX	External	!		NO !
L	addLiquidity	External	!	●	NO !
L	addLiquidityETH	External	!	💰	NO !
L	addLiquidityAVAX	External	!	💰	NO !
L	addLiquidityETC	External	!	💰	NO !

FUNCTION DETAILS

```

| L | addLiquidityROSE | External ! | 44 | NO ! |
| L | swapExactETHForTokens | External ! | 81 | NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | swapExactTokensForETCSupportingFeeOnTransferTokens | External ! | 44 | NO ! |
| L | swapExactTokensForAVAXSupportingFeeOnTransferTokens | External ! | 81 | NO ! |
| L | swapExactTokensForROSESupportingFeeOnTransferTokens | External ! | 81 | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | 81 | NO ! |
|||||
| **IUniswapV2Factory** | Interface | |||
| L | createPair | External ! | 81 | NO ! |
|||||
| **BaseToken** | Implementation | |||
|||||
| **CoinscopeBuyback** | Implementation | |||
| L | coinscopeBuyback | Internal 🔒 | 81 | NO ! |
|||||
| **LiquidityGeneratorToken** | Implementation | IERC20, Ownable, BaseToken,
CoinscopeBuyback |||
| L | <Constructor> | Public ! | 81 | NO ! | | |
| L | getNativeCurrency | Internal 🔒 | |||
| L | name | External ! | NO ! |
| L | symbol | External ! | NO ! |
| L | decimals | External ! | NO ! |
| L | totalSupply | External ! | NO ! |
| L | balanceOf | Public ! | NO ! |
| L | transfer | External ! | 81 | NO ! |
| L | allowance | External ! | NO ! |
| L | approve | External ! | 81 | NO ! |
| L | transferFrom | External ! | 81 | NO ! |
| L | increaseAllowance | External ! | 81 | NO ! |
| L | decreaseAllowance | External ! | 81 | NO ! |
| L | isExcludedFromReward | External ! | NO ! |
| L | totalFees | External ! | NO ! |
| L | deliver | External ! | 81 | NO ! |
| L | reflectionFromToken | External ! | NO ! |
| L | tokenFromReflection | Public ! | NO ! |
| L | excludeFromReward | External ! | 81 | onlyOwner |
| L | includeInReward | External ! | 81 | onlyOwner |
| L | _transferBothExcluded | Private 🔒 | 81 | |||
| L | excludeFromFee | External ! | 81 | onlyOwner |
| L | includeInFee | External ! | 81 | onlyOwner |
| L | setTaxFeePercent | External ! | 81 | onlyOwner |
| L | setLiquidityFeePercent | External ! | 81 | onlyOwner |
| L | setTeamFeePercent | External ! | 81 | onlyOwner |
| L | setTeamAddress | External ! | 81 | onlyOwner |
| L | validateTaxes | Internal 🔒 | |||

```

FUNCTION DETAILS

```

| L | setSwapAndLiquifyEnabled | External ! | ● | onlyOwner |
| L | setTokenSellToLiquify | External ! | ● | onlyOwner |
| L | <Receive Ether> | External ! | 8 | NO ! |
| L | _getValues | Private 🔒 | | |
| L | _getTValues | Private 🔒 | | |
| L | _getRValues | Private 🔒 | | |
| L | _getRate | Private 🔒 | | |
| L | _getCurrentSupply | Private 🔒 | | |
| L | _takeLiquidity | Private 🔒 | ● | |
| L | _takeTeamFee | Private 🔒 | ● | |
| L | _reflectFee | Private 🔒 | ● | |
| L | calculateTaxFee | Private 🔒 | | |
| L | calculateLiquidityFee | Private 🔒 | | |
| L | calculateTeamFee | Private 🔒 | | |
| L | removeAllFee | Private 🔒 | ● | |
| L | restoreAllFee | Private 🔒 | ● | |
| L | getIsExcludedFromFee | Public ! | | NO ! |
| L | _approve | Private 🔒 | ● | |
| L | _transfer | Private 🔒 | ● | |
| L | swapAndLiquify | Private 🔒 | ● | lockTheSwap |
| L | swapTokensForEth | Private 🔒 | ● | |
| L | addLiquidity | Private 🔒 | ● | |
| L | _tokenTransfer | Private 🔒 | ● | |
| L | _transferStandard | Private 🔒 | ● | |
| L | _transferToExcluded | Private 🔒 | ● | |
| L | _transferFromExcluded | Private 🔒 | ● | |

```

Legend

Symbol	Meaning
●	Function can modify state
8	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: Excessive Fees

Status: Open

Impact: Medium

Overview

Owner of the contract is able to set up to 20% fee on buy/sell/transfers

```
function setTaxFeePercent(uint256 taxFeeBps) external onlyOwner {  
    emit UpdatedTaxFeePercent(taxFeeBps, taxFee);  
    taxFee = taxFeeBps;  
    validateTaxes();  
}
```

```
function setLiquidityFeePercent(uint256 liquidityFeeBps) external onlyOwner {  
    emit UpdatedLiquidityFeePercent(liquidityFeeBps, liquidityFee);  
    liquidityFee = liquidityFeeBps;  
    validateTaxes();  
}
```

```
function setTeamFeePercent(uint256 teamFeeBps) external onlyOwner {  
    emit UpdatedTeamFeePercent(teamFeeBps, teamFee);  
    teamFee = teamFeeBps;  
    validateTaxes();  
}
```

Suggestion

Its suggested to keep buy/sell/transfer fees in between 0-10% according to pinksale safu criteria.

MEDIUM RISK FINDING

Category: Centralization

Subject: EOA receiving LP tokens

Status: Open

Severity : Medium

Overview

Owner of the contract received LP tokens generated from auto-liquidity, this LP tokens can be used to remove a portion of liquidity pool.

```
uniswapV2Router.addLiquidityETH{value: ethAmount}(  
address(this), tokenAmount, 0, 0, owner(), block.timestamp  
);
```

Suggestion

Its suggested to either burn or lock new LP tokens.

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**