



expelee

A Secure Place For Web3

SMART CONTRACT AUDIT OF

Artex Token Fair Launch



Contract Address

0x8Af33e39214c3CE3c367ccc923Ee74b49CD4bC05

www.expelee.com Page 1 |





Audit Summary

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

Ownership: NOT RENOUNCED

KYC Verification: Done

Audit Date: 26/07/2022

Audit Team: EXPELEE

Be aware that smart contracts deployed on the blockchain aren't resistant to internal exploit, external vulnerability, or hack. For a detailed understanding of risk severity, source code vulnerability, functional hack, and audit disclaimer, kindly refer to the audit.

www.expelee.com | Page 2 |





DISCLAMER

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 guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect 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. Always 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.

www.expelee.com Page 3 |



Contract Review

Contract Name	Artex Token
Compiler Version	v0.8.15+commit.e14f2714
Optimization	Yes with 200 runs
License	MIT License
Explorer	https://bscscan.com/address/0x8Af33 e39214c3CE3c367ccc923Ee74b49CD4bC 05#code
Symbol	ARTEX
Decimals	18
Total Supply	100,000,000
Domain	https://artex.app/

www.expelee.com | Page 4 |





Project Review

Token Name: ArtexToken

Web Site: https://artex.app/

Twitter: https://twitter.com/artexcommunity

Telegram: https://t.me/artexcommunity

Contract Address:

0x8Af33e39214c3CE3c367ccc923Ee74b49CD4bC05

Platform: Binance Smart Chain

Token Type: BEP 20

Language: SOLIDITY

www.expelee.com | Page 5 |





Audit Methodology

The scope of this report is to audit the smart contract source code. We have scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract

Vulnerabilities

- Unhandled Exceptions
- Transaction Order Dependency
- Integer Overflow
- Unrestricted Action
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation

Source Code Review

- Gas Limit and Loops
- Deployment Consistency
- Repository Consistency
- Data Consistency
- Token Supply Manipulation

Functional Assessment

- Operations Trail & Event Generation
- Assets Manipulation
- Liquidity Access

www.expelee.com | Page 6 |





Vulnerability Checklist

Νō	Description.	Result
1	Compiler warnings.	Passed
2	Race conditions and Re-entrancy. Cross-function raceconditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

www.expelee.com | Page 7 |

Manual Audit

- Low-Risk
- 3 low-risk code issues found
- Medium-Risk
- 0 medium-risk code issues found
 - High-Risk
 - 0 high-risk code issues found

www.expelee.com Page 8 |



Audit Summary

Number of lines: 1405 (+ 0 in dependencies, + 0 in tests)

Number of assembly lines: 0

Number of contracts: 18 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 28

Number of informational issues: 47

Number of low issues: 3

Number of medium issues: 0

Number of high issues: 0

ERCs: ERC2612, ERC20

+	+		+		+		-+-		 +	+
Name	#	functions	 	ERCS		ERC20 info	'	Complex code	Features	
' SafeMath	i L	8	I		I		i	No	' 	· I
SafeMathInt	1	7	L		I		1	No	I	١
SafeMathUint	1	1	I		ı		l	No	l	Ī
IterableMapping	1	6	I		- 1		T	No	I	Ī
IUniswapV2Factory		8	l		I		1	No	l	ı
IUniswapV2Pair		27	E	RC20,ERC26	512	∞ Minting	1	No	l	ı
	1		l		- 1	Approve Race Cond.	1		I	I
I	1		l		ı		1		I	I
IUniswapV2Router02	1	24	l		ı		1	No	Receive ETH	I
DividendTracker	1	66	l	ERC20		No Minting	1	Yes	Tokens interaction	I
	\mathbb{Z}^{2}		L		- 1	Approve Race Cond.	1		I	I
	1				ı		1		I	I
ArtexToken		78	I	ERC20		No Minting	١	Yes	Receive ETH	I
			N		١	Approve Race Cond.	١		Send ETH	I
	I		I		١		I		Tokens interaction	I
+	+		+		+		-+-		+	+

www.expelee.com | Page 9 |





1) Functions that send Ether to arbitrary destinations

Unprotected call to a function sending Ether to an arbitrary address.

Recommendation

Ensure that an arbitrary user cannot withdraw unauthorized funds.

www.expelee.com Page 10 |





2) Reentrancy vulnerabilities

Detection of the reentrancy bug. Do not report reentrancies that don't involve Ether (see reentrancy-no-eth)

Recommendation

Rename Apply the check-effects-interactions pattern.

www.expelee.com | Page 11 |



3) Unchecked transfer

The return value of an external transfer/transferFrom call is not checked.

```
function claimStuckTokens(address token) external onlyOwner {
    require(token != address(this), "Owner cannot claim native tokens");
    if (token == address(0x0)) {
        payable(msg.sender).transfer(address(this).balance);
        return;
    }
    IERC20 ERC20token = IERC20(token);
    uint256 balance = ERC20token.balanceOf(address(this));
    ERC20token.transfer(msg.sender, balance);
}
```

Recommendation

Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

www.expelee.com | Page 13 |





Manual Audit (Contract Function)

```
contract ArtexToken is ERC20, Ownable {
   uint256 public buyFee = 10;
   uint256 public sellFee = 10;
   uint256 public liquidityShare = 25;
   uint256 public marketingShare = 25;
   uint256 public developmentShare = 25;
   uint256 public rewardShare
   address public marketingWallet = 0x9fC06187cAeA6eD69665Ee4Fb6484Ef38dA6D7DB;
   address public developmentWallet = 0xc828F7db4C59B6f61239FbF659eDa8B421A07DBC;
   bool
           public walletToWalletTransferWithoutFee = false;
   IUniswapV2Router02 public uniswapV2Router;
   address public uniswapV2Pair;
   private swapping;
   hoo1
   uint256 public swapTokensAtAmount;
   mapping (address => bool) private _isExcludedFromFees;
   mapping (address => bool) public automatedMarketMakerPairs;
   DividendTracker public dividendTracker;
   address public rewardToken = 0x55d398326f99059fF775485246999027B3197955;
   uint256 public gasForProcessing = 300000;
   // AntiBot
   mapping (address => bool) private _isBot;
          public antiBotSystemEnabled = true;
   uint256 private _launchTime;
   uint256 private _timeAntiBot
   uint256 private _botFeeIncrease = 3;
   event ExcludeFromFees(address indexed account, bool isExcluded);
   event FeesUpdated(uint256 buyFee, uint256 sellFee);
   event FeeSharesUpdated(uint256 marketingShare, uint256 developmentShare, uint256
liquidityShare, uint256 rewardShare);
   event MarketingWalletChanged(address marketingWallet);
   event DevelopmentWalletChanged(address developmentWallet);
   event LiquidityWalletChanged(address liquidityWallet);
```

www.expelee.com Page 13 |





Important Points To Consider

- ✓ Verified contract source
- √ Token is sellable (not a honeypot) at this time
- X Ownership renounced or source does not contain an owner contract
 - X Source does not contain a mint function
 - X Source does not contain a fee modifier
 - X Buy fee is less than 5% (30%)
 - X Sell fee is less than 10% (29%)
- ✓ Owner/creator wallet contains less than 10% of circulating token supply (0%)

www.expelee.com Page 14 |





About Expelee

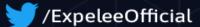
Expelee is a community driven organisation dedicated to fostering an antirug movement. We're here to keep investment safe from fraudsters. We've encountered several rug pulls and know how it feels to be duped, which is why we don't want anybody else to go through the same experience. We are here to raise awareness through our services so that the future of cryptocurrency can be rug-free.

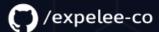
The auditing process focuses to the following considerations with collaboration of an expert team:

- Functionality test of the Smart Contract to determine if proper logic has been followed throughout the whole process.
- Manually detailed examination of the code line by line by experts.
- Live test by multiple clients using Test net.
- Analysing failure preparations to check how the Smart
- Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.

Social Media







www.expelee.com | Page 15 |