



Smart Contract Audit

FOR
PARTY

DATED : 22 MAY 23'



AUDIT SUMMARY

Project name – PARTY

Date: 22 May, 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1. Manual Review: The code has undergone a line-by-line review by the **Ace** team.

2. ETH Test Network: All tests were conducted on the ETH Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3. Slither: The code has undergone static analysis using Slither.

Testnet version:

Contract has been tested on binance smart chain testnet which can be found in below link:

<https://testnet.bscscan.com/token/0x11bDC05dd64Ee6BBBfB6D8bFF8d711aF3dC2c7F2>



Token Information

Name : Party Parrot

Symbol : PARTY

Decimals: 18

Network: Binance smart chain

Token Type: BEP20

Token Address:

0x3D2e1334E5FaeB6Ab630DFEd455a34bFC600756
a

Owner:

0x15B43A006e8d3cD5a459CE2d603f4c2B22a0b816
(at time of writing the audit)

Deployer: 0x5dD1721Bb020118d5A0602e5dD83631E
3A50F698



Token Information

Fees:

Buy Fees: 0-12%

Sell Fees: 0-12%

Transfer Fees: 0%

Fees Privilege: Owner

Ownership :

0x56d7db7cE1128Cf8cB288650Cf614b8EBa03256b

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges:- - Enabling trades

- initial distribution of the tokens



AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
 - Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
 - Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
 - Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
 - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-

VULNERABILITY CHECKLIST

- | | |
|------------------------------------|-------------------------------|
| ✓ Return values of low-level calls | ✓ Gasless Send |
| ✓ Private modifier | ✓ Using block.timestamp |
| ✓ Multiple Sends | ✓ Re-entrancy |
| ✓ Using Suicide | ✓ Tautology or contradiction |
| ✓ Gas Limitand Loops | ✓ Timestamp Dependence |
| ✓ Address hardcoded | ✓ Revert/require functions |
| ✓ Exception Disorder | ✓ Use of tx.origin |
| ✓ Using inline assembly | ✓ Integer overflow/underflow |
| ✓ Divide before multiply | ✓ Dangerous strict equalities |
| ✓ Missing Zero Address Validation | ✓ Using SHA3 |
| ✓ Compiler version not fixed | ✓ Using throw |
-



CLASSIFICATION OF RISK

Severity

Description

◆ Critical

These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.

◆ High-Risk

A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.

◆ Medium-Risk

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

◆ Low-Risk

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

◆ Gas Optimization /Suggestion

A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity

Found

◆ Critical

0

◆ High-Risk

0

◆ Medium-Risk

0

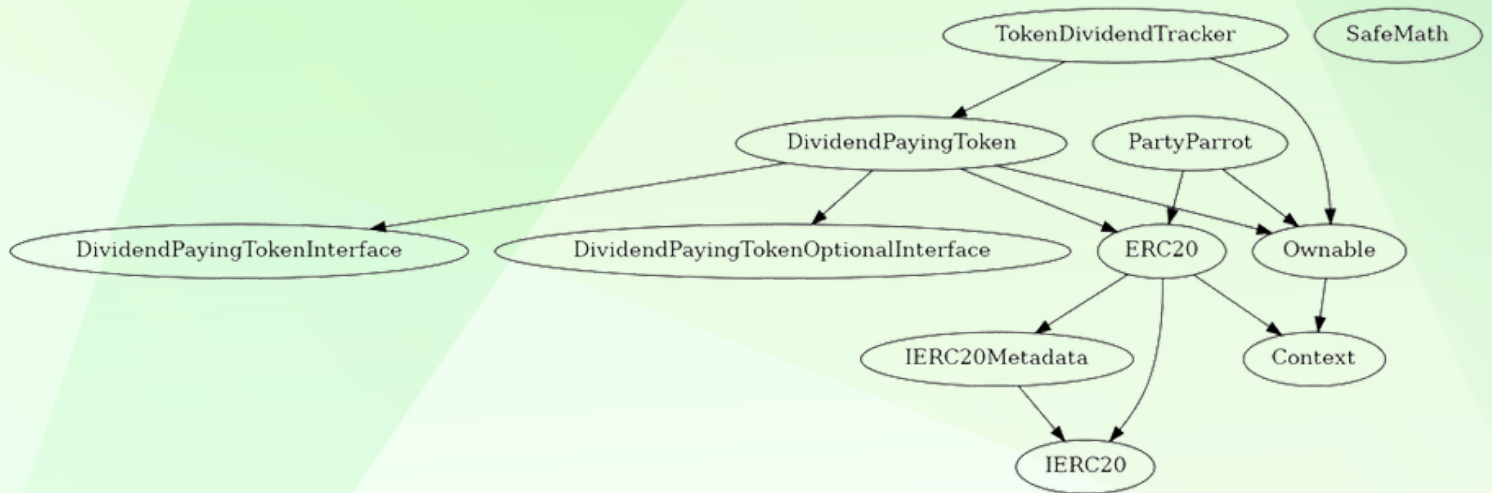
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

0

INHERITANCE TREE



POINTS TO NOTE

- Owner is not able to set buy/sell fees over 12% each
 - Owner is not able to set fee on transfers
 - Owner is not able to blacklist an arbitrary address.
 - Owner is able to disable trades but not directly
 - Owner is able to burn tokens from any wallet
 - Owner is not able to limit buy/sell/transfer/wallet amounts
 - Owner is not able to mint new tokens
-



CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
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	_transferOwnership	Internal	🔒		●
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 !
IERC20Metadata Interface IERC20					
L	name	External	!		NO !
L	symbol	External	!		NO !
L	decimals	External	!		NO !
SafeMath Library					
L	add	Internal	🔒		
L	sub	Internal	🔒		
L	sub	Internal	🔒		
L	mul	Internal	🔒		
L	div	Internal	🔒		
L	div	Internal	🔒		
L	mod	Internal	🔒		
L	mod	Internal	🔒		
SafeMathInt Library					
L	mul	Internal	🔒		
L	div	Internal	🔒		
L	sub	Internal	🔒		
L	add	Internal	🔒		

CONTRACT ASSESMENT

```

|  | abs | Internal | | | |
|  | toUint256Safe | Internal | | |
|||||
|  | **SafeMathUint** | Library | |||
|  | toInt256Safe | Internal | | |
|||||
|  | **Clones** | Library | |||
|  | clone | Internal | | |
|  | cloneDeterministic | Internal | | |
|  | predictDeterministicAddress | Internal | | |
|  | predictDeterministicAddress | Internal | | |
|||||
|  | **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 | | |
|  | _cast | Internal | | |
|  | _burn | Internal | | |
|  | _approve | Internal | | |
|  | _beforeTokenTransfer | Internal | | |
|||||
|  | **IUniswapV2Router01** | Interface | |||
|  | factory | External | | NO |
|  | WETH | External | | NO |
|  | 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 |

```



CONTRACT ASSESMENT

```
| L | swapTokensForExactETH | External ! | ● | NO ! |
| L | swapExactTokensForETH | External ! | ● | NO ! |
| L | swapETHForExactTokens | External ! | 🟢 | NO ! |
| L | quote | External ! | | NO ! |
| L | getAmountOut | External ! | | NO ! |
| L | getAmountIn | External ! | | NO ! |
| L | getAmountsOut | External ! | | NO ! |
| L | getAmountsIn | External ! | | NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🟢 | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
|||||
| **IUniswapV2Factory** | Interface | |||
| L | feeTo | External ! | | NO ! |
| L | feeToSetter | External ! | | NO ! |
| L | getPair | External ! | | NO ! |
| L | allPairs | External ! | | NO ! |
| L | allPairsLength | External ! | | NO ! |
| L | createPair | External ! | ● | NO ! |
| L | setFeeTo | External ! | ● | NO ! |
| L | setFeeToSetter | External ! | ● | NO ! |
|||||
| **IUniswapV2Pair** | Interface | |||
| L | name | External ! | | NO ! |
| L | symbol | External ! | | NO ! |
| L | decimals | External ! | | NO ! |
| L | totalSupply | External ! | | NO ! |
| L | balanceOf | External ! | | NO ! |
| L | allowance | External ! | | NO ! |
| L | approve | External ! | ● | NO ! |
| L | transfer | External ! | ● | NO ! |
| L | transferFrom | External ! | ● | NO ! |
| L | DOMAIN_SEPARATOR | External ! | | NO ! |
| L | PERMIT_TYPEHASH | External ! | | NO ! |
| L | nonces | External ! | | NO ! |
| L | permit | External ! | ● | NO ! |
| L | MINIMUM_LIQUIDITY | External ! | | NO ! |
| L | factory | External ! | | NO ! |
```

CONTRACT ASSESMENT

```

└─ token0 | External ! | |NO ! |
└─ token1 | External ! | |NO ! |
└─ getReserves | External ! | |NO ! |
└─ price0CumulativeLast | External ! | |NO ! |
└─ price1CumulativeLast | External ! | |NO ! |
└─ kLast | External ! | |NO ! |
└─ burn | External ! | ● |NO ! |
└─ swap | External ! | ● |NO ! |
└─ skim | External ! | ● |NO ! |
└─ sync | External ! | ● |NO ! |
└─ initialize | External ! | ● |NO ! |
|||||
**DividendPayingTokenInterface** | Interface | |||
└─ dividendOf | External ! | |NO ! |
└─ withdrawDividend | External ! | ● |NO ! |
|||||
**DividendPayingTokenOptionalInterface** | Interface | |||
└─ withdrawableDividendOf | External ! | |NO ! |
└─ withdrawnDividendOf | External ! | |NO ! |
└─ accumulativeDividendOf | External ! | |NO ! |
|||||
**DividendPayingToken** | Implementation | ERC20, Ownable, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface |||
└─ <Constructor> | Public ! | ● |ERC20 |
└─ distributeCAKEDividends | Public ! | ● |onlyOwner |
└─ withdrawDividend | Public ! | ● |NO ! |
└─ _withdrawDividendOfUser | Internal 🔒 | ● ||
└─ dividendOf | Public ! | |NO ! |
└─ withdrawableDividendOf | Public ! | |NO ! |
└─ withdrawnDividendOf | Public ! | |NO ! |
└─ accumulativeDividendOf | Public ! | |NO ! |
└─ _transfer | Internal 🔒 | ● ||
└─ _cast | Internal 🔒 | ● ||
└─ _burn | Internal 🔒 | ● ||
└─ _setBalance | Internal 🔒 | ● ||
|||||
**TokenDividendTracker** | Implementation | Ownable, DividendPayingToken |||
└─ <Constructor> | Public ! | ● |DividendPayingToken |
└─ _transfer | Internal 🔒 | ||
└─ withdrawDividend | Public ! | |NO ! |
└─ setMinimumTokenBalanceForDividends | External ! | ● |onlyOwner |
└─ excludeFromDividends | External ! | ● |onlyOwner |
└─ updateClaimWait | External ! | ● |onlyOwner |

```

CONTRACT ASSESMENT

```

└─ getLastProcessedIndex | External ! | |NO ! |
└─ getNumberOfTokenHolders | External ! | |NO ! |
└─ isExcludedFromDividends | Public ! | |NO ! |
└─ getAccount | Public ! | |NO ! |
└─ getAccountAtIndex | Public ! | |NO ! |
└─ canAutoClaim | Private 🔒 | |
└─ setBalance | External ! | ● | onlyOwner |
└─ process | Public ! | ● |NO ! |
└─ processAccount | Public ! | ● | onlyOwner |
└─ MAPGet | Public ! | |NO ! |
└─ MAPGetIndexOfKey | Public ! | |NO ! |
└─ MAPGetKeyAtIndex | Public ! | |NO ! |
└─ MAPSize | Public ! | |NO ! |
└─ MAPSet | Public ! | ● |NO ! |
└─ MAPRemove | Public ! | ● |NO ! |
|||||
**PartyParrot** | Implementation | ERC20, Ownable |||
└─ <Constructor> | Public ! | 🟢 | ERC20 |
└─ <Receive Ether> | External ! | 🟢 |NO ! |
└─ updateMinimumTokenBalanceForDividends | Public ! | ● | onlyOwner |
└─ updateUniswapV2Router | Public ! | ● | onlyOwner |
└─ excludeFromFees | Public ! | ● | onlyOwner |
└─ excludeMultipleAccountsFromFees | Public ! | ● | onlyOwner |
└─ setMarketingWallet | External ! | ● | onlyOwner |
└─ setAutomatedMarketMakerPair | Public ! | ● | onlyOwner |
└─ burn | External ! | ● | onlyOwner |
└─ _setAutomatedMarketMakerPair | Private 🔒 | ● |
└─ updateGasForProcessing | Public ! | ● | onlyOwner |
└─ updateClaimWait | External ! | ● | onlyOwner |
└─ getClaimWait | External ! | |NO ! |
└─ getTotalDividendsDistributed | External ! | |NO ! |
└─ isExcludedFromFees | Public ! | |NO ! |
└─ withdrawableDividendOf | Public ! | |NO ! |
└─ dividendTokenBalanceOf | Public ! | |NO ! |
└─ excludeFromDividends | External ! | ● | onlyOwner |
└─ isExcludedFromDividends | Public ! | |NO ! |
└─ getAccountDividendsInfo | External ! | |NO ! |
└─ getAccountDividendsInfoAtIndex | External ! | |NO ! |
└─ processDividendTracker | External ! | ● |NO ! |
└─ claim | External ! | ● |NO ! |
└─ getLastProcessedIndex | External ! | |NO ! |

```

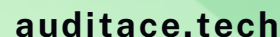


CONTRACT ASSESMENT

	└		getNumberOfDividendTokenHolders		External	!			NO	!	
	└		swapManual		Public	!		●		onlyOwner	
	└		setSwapTokensAtAmount		Public	!		●		onlyOwner	
	└		setDeadWallet		Public	!		●		onlyOwner	
	└		setBuyTaxes		External	!		●		onlyOwner	
	└		setSelTaxes		External	!		●		onlyOwner	
	└		_transfer		Internal	🔒		●			
	└		swapAndSendToFee		Private	🔒		●			
	└		swapAndLiquify		Private	🔒		●			
	└		swapTokensForEth		Private	🔒		●			
	└		swapTokensForToken		Private	🔒		●			
	└		addLiquidity		Private	🔒		●			
	└		swapAndSendDividends		Private	🔒		●			

Legend

	Symbol		Meaning	
	:-----:		-----	
	●		Function can modify state	
	💰		Function is payable	

[illegible]

an static analysis of the code were performed using
slither. No issues were found



FUNCTIONAL TESTING

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0x1b5336ae33e6330d78026f54035944a42091c68203ddecaee8930b327d54c588>

2- Buying when excluded from fees (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x98762dedff86acac0fed2dab020fcb425f3ba80ca21204844f82d39d71905817>

3- Selling when excluded from fees (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x3248b538e987952a7338695a536a6ef338214a7e5c504973f042bfa2e50dc711>

4- Transferring when excluded from fees (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x9c961b63585da76e0c05db544a94b790b44fc99621298ffb0fd10e0311fd5aad>

5- Buying when not excluded from fees (0-12% tax) (passed):

<https://testnet.bscscan.com/tx/0x2e139e79d47f6c5251491bd7704352dd1282bc3a77f5b1d8f0300312d239b3be>

6- Selling from a regular wallet (0-12% tax) (passed):

<https://testnet.bscscan.com/tx/0x58eeca44ad8acc4f28bbec7597f212287ba99444edf61d93ed724fc711c9af17>

7- Transferring from a regular wallet (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x18f603de450d35f7dda0df904806157b03a586e946e2d67a5c7debf00afdd1fb>



FUNCTIONAL TESTING

**7- Internal swap + rewards distirbution + auto liquidity + burn
(passed):**

<https://testnet.bscscan.com/tx/0x58eeca44ad8acc4f28bbec7597f212287ba99444edf61d93ed724fc711c9af17>



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 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 Auditace 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 Auditace 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 Auditace team disclaims any liability for the resulting losses.



ABOUT AUDITACE

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



<https://auditace.tech/>



https://t.me/Audit_Ace



https://twitter.com/auditace_



<https://github.com/Audit-Ace>
