AuditAce
FROM INCEPTION TO SUCCESS

auditace.tech

Smart Contract Audit

FOR

White Rabbit

DATED : 4 June 23'

AUDIT SUMMARY

Project name – White Rabbit

Date: 4 June, 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	1
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:
a line by line code review has been performed by audit ace team.

2- BSC Test Network:
all tests were done on BSC Test network, each test has its transaction has attached to it.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

https://testnet.bscscan.com/token/0xe31faedd1fe0180f174a7ce540fba77d814ea911

Token Information

Token Name : White Rabbit

Token Symbol: WRB

Decimals: 18

Token Supply:100,000,000,000

Token Address:
0x55D004a30b4958f84df134a8082C0082c1923551

Checksum:
ba62deaafd161d4c3f54796e67e2c279bb97307d

Owner: -
0xf46e65701d892Bd3a67B5Fe909C50359394d0415

TOKEN OVERVIEW

Fees:

Buy Fees: 0-8%

Sell Fees: 0-8 %

Transfer Fees: 0%

Fees Privilige: Owner

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: none

Blacklist: No

Other Priviliges: - changing swap threshold

- changing fees
- modifying swap settings
- enabling trades
- initial distribution of 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 isexercised 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
- ✓ Private modifier
- ✓ Multiple Sends
- ✓ Using Suicide
- ✓ Gas Limitand Loops
- ✓ Address hardcoded
- ✓ Exception Disorder
- ✓ Using inline assembly
- ✓ Divide before multiply
- ✓ Missing Zero Address Validation
- ✓ Compiler version not fixed
- ✓ **Gasless Send**
- ✓ Using block.timestamp
- ✓ Re-entrancy
- ✓ Tautology or contradiction
- ✓ Timestamp Dependence
- ✓ Revert/require functions
- ✓ Use of tx.origin
- ✓ Integer overflow/underflow
- ✓ Dangerous strict equalities
- ✓ Using SHA3
- ✓ Using throw

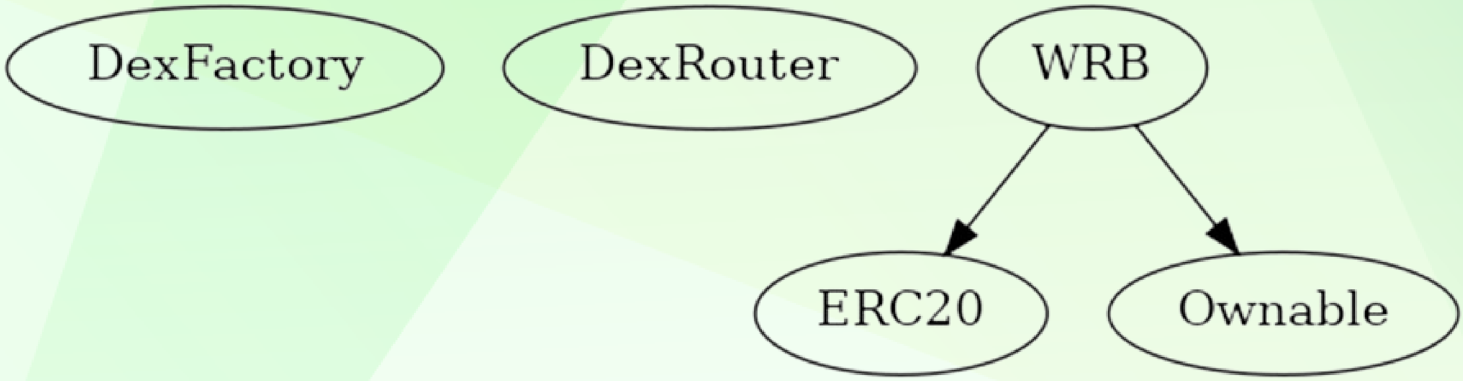
CLASSIFICATION OF RISK

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	1

INHERITANCE TREE



POINTS TO NOTE

- Owner is not able to set buy/sell taxes over 8%
- Owner is not ablet o set transfer taxes (0% forever)
- Owner is not able to set max buy/sell/transfer/hold amount
- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to mint new tokens
- Owner is not able to disable trades

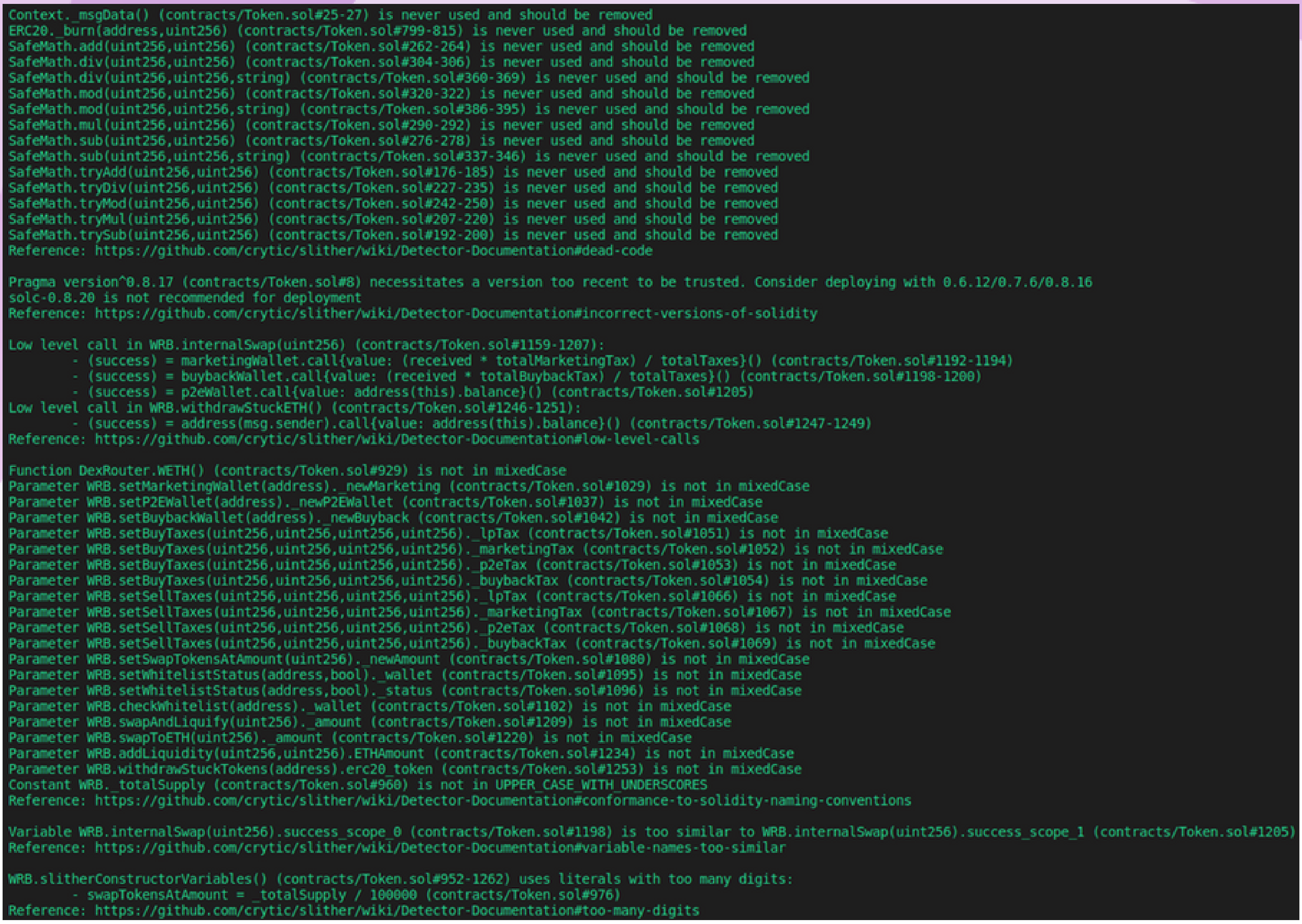
CONTRACT ASSESMENT

```
|  Contract  |        Type        |       Bases      |                  |                 |
|:----------:|:-------------------:|:----------------:|:----------------:|:---------------:|
|     └      |  **Function Name**  |  **Visibility**  |  **Mutability**  |  **Modifiers**  |
||||||
| **DexFactory** | Interface |  |||
| └ | createPair | External ❗️ | 🛑  |NO❗️ |
||||||
| **DexRouter** | Interface |  |||
| └ | factory | External ❗️ |   |NO❗️ |
| └ | WETH | External ❗️ |   |NO❗️ |
| └ | addLiquidityETH | External ❗️ |  💵 |NO❗️ |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ❗️ | 🛑  |NO❗️ |
||||||
| **WRB** | Implementation | ERC20, Ownable |||
| └ | <Constructor> | Public ❗️ | 🛑  | ERC20 |
| └ | enableTrading | External ❗️ | 🛑  | onlyOwner |
| └ | setMarketingWallet | External ❗️ | 🛑  | onlyOwner |
| └ | setP2EWallet | External ❗️ | 🛑  | onlyOwner |
| └ | setBuybackWallet | External ❗️ | 🛑  | onlyOwner |
| └ | setBuyTaxes | External ❗️ | 🛑  | onlyOwner |
| └ | setSellTaxes | External ❗️ | 🛑  | onlyOwner |
| └ | setSwapTokensAtAmount | External ❗️ | 🛑  | onlyOwner |
| └ | toggleSwapping | External ❗️ | 🛑  | onlyOwner |
| └ | setWhitelistStatus | External ❗️ | 🛑  | onlyOwner |
| └ | checkWhitelist | External ❗️ |   |NO❗️ |
| └ | _takeTax | Internal 🔒 | 🛑  | |
| └ | _transfer | Internal 🔒 | 🛑  | |
| └ | internalSwap | Internal 🔒 | 🛑  | |
| └ | swapAndLiquify | Internal 🔒 | 🛑  | |
| └ | swapToETH | Internal 🔒 | 🛑  | |
| └ | addLiquidity | Private 🔐 | 🛑  | |
| └ | withdrawStuckETH | External ❗️ | 🛑  | onlyOwner |
| └ | withdrawStuckTokens | External ❗️ | 🛑  | onlyOwner |
| └ | <Receive Ether> | External ❗️ |  💵 |NO❗️ |

### Legend

|  Symbol  |  Meaning  |
|:--------:|-----------|
|    🛑    | Function can modify state |
|    💵    | Function is payable |
```

STATIC ANALYSIS



```
Context._msgData() (contracts/Token.sol#25-27) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#799-815) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#262-264) is never used and should be removed
SafeMath.div(uint256,uint256) (contracts/Token.sol#304-306) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#360-369) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#320-322) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#386-395) is never used and should be removed
SafeMath.mul(uint256,uint256) (contracts/Token.sol#290-292) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#276-278) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#337-346) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#176-185) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#227-235) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#242-250) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#207-220) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#192-200) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#8) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in WRB.internalSwap(uint256) (contracts/Token.sol#1159-1207):
        - (success) = marketingWallet.call{value: (received * totalMarketingTax) / totalTaxes}() (contracts/Token.sol#1192-1194)
        - (success) = buybackWallet.call{value: (received * totalBuybackTax) / totalTaxes}() (contracts/Token.sol#1198-1200)
        - (success) = p2eWallet.call{value: address(this).balance}() (contracts/Token.sol#1205)
Low level call in WRB.withdrawStuckETH() (contracts/Token.sol#1246-1251):
        - (success) = address(msg.sender).call{value: address(this).balance}() (contracts/Token.sol#1247-1249)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function DexRouter.WETH() (contracts/Token.sol#929) is not in mixedCase
Parameter WRB.setMarketingWallet(address)._newMarketing (contracts/Token.sol#1029) is not in mixedCase
Parameter WRB.setP2EWallet(address)._newP2EWallet (contracts/Token.sol#1037) is not in mixedCase
Parameter WRB.setBuybackWallet(address)._newBuyback (contracts/Token.sol#1042) is not in mixedCase
Parameter WRB.setBuyTaxes(uint256,uint256,uint256,uint256)._lpTax (contracts/Token.sol#1051) is not in mixedCase
Parameter WRB.setBuyTaxes(uint256,uint256,uint256,uint256)._marketingTax (contracts/Token.sol#1052) is not in mixedCase
Parameter WRB.setBuyTaxes(uint256,uint256,uint256,uint256)._p2eTax (contracts/Token.sol#1053) is not in mixedCase
Parameter WRB.setBuyTaxes(uint256,uint256,uint256,uint256)._buybackTax (contracts/Token.sol#1054) is not in mixedCase
Parameter WRB.setSellTaxes(uint256,uint256,uint256,uint256)._lpTax (contracts/Token.sol#1066) is not in mixedCase
Parameter WRB.setSellTaxes(uint256,uint256,uint256,uint256)._marketingTax (contracts/Token.sol#1067) is not in mixedCase
Parameter WRB.setSellTaxes(uint256,uint256,uint256,uint256)._p2eTax (contracts/Token.sol#1068) is not in mixedCase
Parameter WRB.setSellTaxes(uint256,uint256,uint256,uint256)._buybackTax (contracts/Token.sol#1069) is not in mixedCase
Parameter WRB.setSwapTokensAtAmount(uint256)._newAmount (contracts/Token.sol#1080) is not in mixedCase
Parameter WRB.setWhitelistStatus(address,bool)._wallet (contracts/Token.sol#1095) is not in mixedCase
Parameter WRB.setWhitelistStatus(address,bool)._status (contracts/Token.sol#1096) is not in mixedCase
Parameter WRB.checkWhitelist(address)._wallet (contracts/Token.sol#1102) is not in mixedCase
Parameter WRB.swapAndLiquify(uint256)._amount (contracts/Token.sol#1209) is not in mixedCase
Parameter WRB.swapToETH(uint256)._amount (contracts/Token.sol#1220) is not in mixedCase
Parameter WRB.addLiquidity(uint256,uint256).ETHAmount (contracts/Token.sol#1234) is not in mixedCase
Parameter WRB.withdrawStuckTokens(address).erc20_token (contracts/Token.sol#1253) is not in mixedCase
Constant WRB._totalSupply (contracts/Token.sol#960) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Variable WRB.internalSwap(uint256).success_scope_0 (contracts/Token.sol#1198) is too similar to WRB.internalSwap(uint256).success_scope_1 (contracts/Token.sol#1205)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

WRB.slitherConstructorVariables() (contracts/Token.sol#952-1262) uses literals with too many digits:
        - swapTokensAtAmount = _totalSupply / 100000 (contracts/Token.sol#976)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

Result => A static analysis of contract’s source code has been performed using slither,

No major issues were found in the output

FUNCTIONAL TESTING

Router (PCS V2):
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

All the functionalities have been tested, no issues were found

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0xd7374804b6b01f35990e4371124d1d71b172ef224613e5e566eacbbb0b1c5841

2- Buying when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x74d36a45811057a36af202d1703bb387b1c4bc2541525f3cd191002eafa05fa3

3- Selling when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xbf1f8fc351efee2710e8415d3aee97c6cca5330d954b4037225adbd4252a4487

4- Transferring when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x76d7d3129209476a0f57fb49329b8775dc6815ef3b0b22973469a9786b00db4e

5- Buying when not excluded from fees (0-8% tax) (passed):
https://testnet.bscscan.com/tx/0x68d7bd4a4174147270d674734e22dbc6ed7387075e735a11116feb6c637b75d3

6- Sellingwhen not excluded from fees (0-8% tax) (passed):
https://testnet.bscscan.com/tx/0x5421199e4778373c1e1b274af54f25104784fc83542f2dc5e401ee84ebd68624

FUNCTIONAL TESTING

7- Transferring from a regular wallet (0% tax) (passed):
https://testnet.bscscan.com/tx/0x3cc7392c984c017632fbd4afa50efbefe542342dcca27cd3149cad15c6ca1280

8-Internal swap (BNB Fees and auto-liquidity) ((passed):
https://testnet.bscscan.com/tx/0x5421199e4778373c1e1b274af54f25104784fc83542f2dc5e401ee84ebd68624

ISSUES FOUND

Centralization – Trades must be enabled

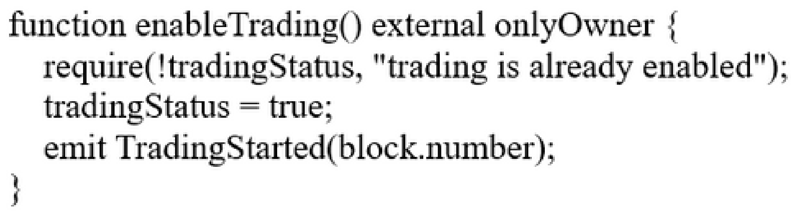
Severity: **Informational**

function: EnableTrading

Status: Not Resolved

Overview:

The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.



```
function enableTrading() external onlyOwner {
    require(!tradingStatus, "trading is already enabled");
    tradingStatus = true;
    emit TradingStarted(block.number);
}
```

Suggestion

To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades

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 specializes 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