



Smart Contract Audit

FOR
XRP 2.0

DATED : 14 July 23'



AUDIT SUMMARY

Project name – XRP 2.0

Date: 14 July, 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:

A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC 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:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0xC04484fE4251474091839831F6bABff657be4A67>



Token Information

Token Name : XRP 2.0

Token Symbol: XRP 2.0

Decimals: 9

Token Supply: 420,000,000,000,000,000

Token Address:

0x5571afbBC852a12A001bce4D70DEc7eC0AF24751

Checksum:

fa17c9f5736affaf74cb2b9343cf49e4888f335b

Owner:

0xFe5AEc0AFc2812Dc4BfCb7F695e92fc047aADF3
(at time of writing the audit)

Deployer:

0xFe5AEc0AFc2812Dc4BfCb7F695e92fc047aADF3



TOKEN OVERVIEW

Fees:

Buy Fees: 0-6%

Sell Fees: 0-6%

Transfer Fees: 0-6%

Fees Privilege: no fees

Ownership: owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: no

Blacklist: No

Other Privileges: Initial distribution of the tokens
modifying fees



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

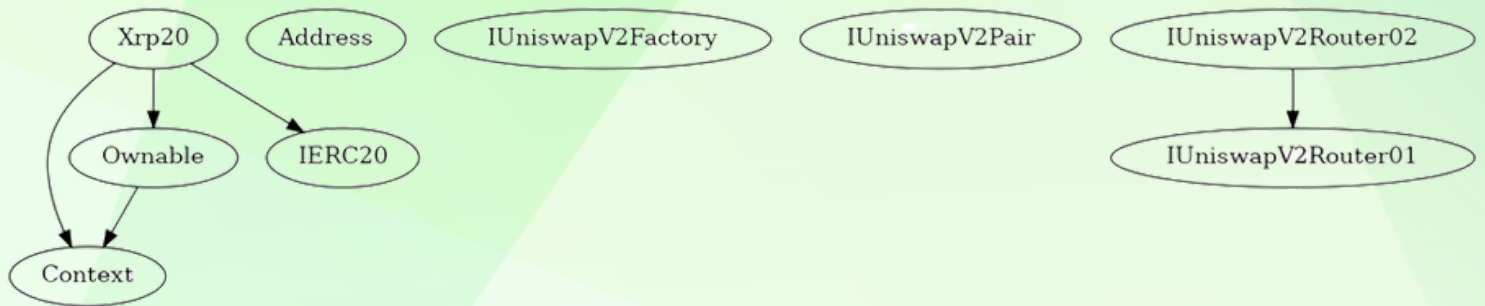
Severity

Found

◆ Critical	0
◆ High-Risk	0
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0



INHERITANCE TREE



POINTS TO NOTE

- Owner is able to change fees in range 0-6% for buy and sells (0% transfer tax)
 - Owner is not able to blacklist an arbitrary address.
 - Owner is not able to disable trades
 - 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
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 !
Address Library					
L	isContract	Internal	🔒		
L	sendValue	Internal	🔒	●	
L	functionCall	Internal	🔒	●	
L	functionCall	Internal	🔒	●	
L	functionCallWithValue	Internal	🔒	●	
L	functionCallWithValue	Internal	🔒	●	
L	_functionCallWithValue	Private	🔒	●	
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 !



CONTRACT ASSESMENT

```
| 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 ! |
| burn | External ! | ● |NO ! |
| swap | External ! | ● |NO ! |
| skim | External ! | ● |NO ! |
| sync | External ! | ● |NO ! |
| initialize | External ! | ● |NO ! |
|||||
| **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 ! |
| swapTokensForExactETH | External ! | ● |NO ! |
| swapExactTokensForETH | External ! | ● |NO ! |
| swapETHForExactTokens | External ! | 💰 |NO ! |
| quote | External ! | |NO ! |
| getAmountOut | External ! | |NO ! |
```

CONTRACT ASSESMENT







































```

└─| 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 ! |
|||||
**Xrp20** | Implementation | Context, IERC20, Ownable |||
└─| <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 ! |
└─| isExcludedFromReward | Public ! | |NO ! |
└─| totalReflectionDistributed | Public ! | |NO ! |
└─| deliver | Public ! | ● |NO ! |
└─| reflectionFromToken | Public ! | |NO ! |
└─| tokenFromReflection | Public ! | |NO ! |
└─| excludeFromReward | Public ! | ● |onlyOwner |
└─| includeInReward | External ! | ● |onlyOwner |
└─| <Receive Ether> | External ! | $ |NO ! |
└─| clearStuckTokens | External ! | ● |NO ! |
└─| updateFeeBuy | Public ! | ● |onlyOwner |
└─| updateFeeSell | Public ! | ● |onlyOwner |
└─| _reflectFee | Private 🔒 | ● |
└─| _getValues | Private 🔒 |
└─| _getTValues | Private 🔒 |
└─| _getRValues | Private 🔒 |
└─| _getRate | Private 🔒 |
└─| _getCurrentSupply | Private 🔒 |
└─| _takeLiquidity | Private 🔒 | ● |

```



CONTRACT ASSESMENT

```

|  | _takeMarketing | Private |  |  | |
|  | calculateTaxFee | Private |  | | |
|  | calculateLiquidityFee | Private |  | | |
|  | calculateMarketingFee | Private |  | | |
|  | removeAllFee | Private |  |  | |
|  | setBuyFee | Private |  |  | |
|  | setSellFee | Private |  |  | |
|  | isExcludedFromFee | Public |  | | NO  |
|  | _approve | Private |  |  | |
|  | _transfer | Private |  |  | |
|  | swapAndLiquify | Private |  |  | |
|  | swapAndSendMarketing | Private |  |  | |
|  | setSwapTokensAtAmount | External |  |  | onlyOwner |
|  | setSwapEnabled | External |  |  | onlyOwner |
|  | _tokenTransfer | Private |  |  | |
|  | _transferStandard | Private |  |  | |
|  | _transferToExcluded | Private |  |  | |
|  | _transferFromExcluded | Private |  |  | |
|  | _transferBothExcluded | Private |  |  | |
|  | excludeFromFees | External |  |  | onlyOwner |
|  | isContract | Internal |  | | |

```

Legend

Symbol	Meaning
	Function can modify state
	Function is payable



STATIC ANALYSIS

```
Variable Xrp20._getValues(uint256).rTransferAmount (contracts/Token.sol#646) is too similar to Xrp20._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#887)
Variable Xrp20._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#922) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#563) is too similar to Xrp20._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#924)
Variable Xrp20._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#922) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#563) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#563) is too similar to Xrp20._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#943)
Variable Xrp20._getValues(uint256).rTransferAmount (contracts/Token.sol#646) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#655)
Variable Xrp20._getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#655)
Variable Xrp20._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#885) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#655)
Variable Xrp20._getValues(uint256).rTransferAmount (contracts/Token.sol#646) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#941) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#655)
Variable Xrp20._getValues(uint256).rTransferAmount (contracts/Token.sol#646) is too similar to Xrp20._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#924)
Variable Xrp20._getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20._getValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#887)
Variable Xrp20._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#885) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#941) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20._getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#924)
Variable Xrp20._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#885) is too similar to Xrp20._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#924)
Variable Xrp20._getValues(uint256).rTransferAmount (contracts/Token.sol#646) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#563) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#655)
Variable Xrp20._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#941) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#941) is too similar to Xrp20._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#924)
Variable Xrp20._getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#885) is too similar to Xrp20._getValues(uint256).tTransferAmount (contracts/Token.sol#645)
Variable Xrp20.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#563) is too similar to Xrp20._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#905)
Variable Xrp20._getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#668) is too similar to Xrp20._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#943)
Variable Xrp20._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#885) is too similar to Xrp20._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#943)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

Xrp20.DEAD (contracts/Token.sol#416) should be constant
Xrp20._decimals (contracts/Token.sol#391) should be constant
Xrp20._name (contracts/Token.sol#389) should be constant
Xrp20._symbol (contracts/Token.sol#390) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

Xrp20.DEV (contracts/Token.sol#417) should be immutable
Xrp20._tTotal (contracts/Token.sol#394) should be immutable
Xrp20._mk (contracts/Token.sol#414) should be immutable
Xrp20.totalBuyFees (contracts/Token.sol#411) should be immutable
Xrp20.totalSellFees (contracts/Token.sol#412) should be immutable
Xrp20.uniswapV2Pair (contracts/Token.sol#420) should be immutable
Xrp20.uniswapV2Router (contracts/Token.sol#419) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

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

No major issues were found in the output



FUNCTIONAL TESTING

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0x07f57be61e54c9ef3415ba87e6db177638ca6ca5977e5ffbeede3bb6c577d505>

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

<https://testnet.bscscan.com/tx/0x027db45c7a6e848ca099abac3824c27f93694a619953440dab03e66084b401d9>

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

<https://testnet.bscscan.com/tx/0x8a39e027e64672cf64186519dc375027ad9689449e760631ea18173940c1eec0>

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

<https://testnet.bscscan.com/tx/0x13d8edce4578d8e4f649bf0776af0b7d292ad60f0ca9b28d2f16af3454cc88c6>

5- Buying from a regular wallet (0-6% tax) (passed):

<https://testnet.bscscan.com/tx/0x539b540fb69a1f5ffecdff4880fc9362125be2067e09c436db09b986a9184dc7>

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

<https://testnet.bscscan.com/tx/0x0b3f59ba33a295c9c2c3432c54ae34838d0a9f3960712f7c6ebc5d3ac3e6e050>



FUNCTIONAL TESTING

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

<https://testnet.bscscan.com/tx/0x92365e4bae74459cba7679e6e2fb9d61f3b62d7a301e0655027f0ea97a482b1d>

7- Internal swap (marketing and development wallets received BNB) (passed):

<https://testnet.bscscan.com/address/0xFe5AEc0AFc2812Dc4BfCb7F695e92fc047aADF3#internaltx>



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>
