RugFreeCoins Audit

PurityAI 2.0 Token
Smart Contract Security Audit

July 08th ,2023

Overview

✅ No mint function found, the owner cannot mint tokens after initial deployment.

✅ The owner can’t pause trading once it’s enabled

✅ The owner can't blacklist wallets.

✅ The owner can't set a max wallet limit

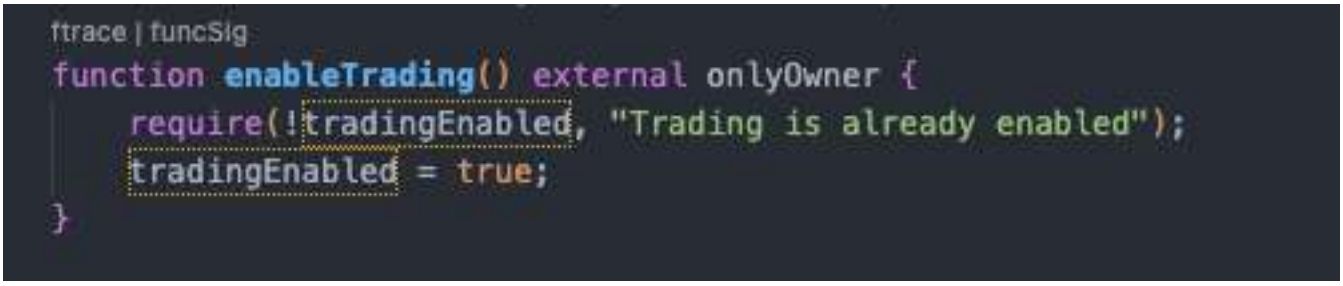
✅ The owner can't claim the contract’s balance of its own token.

✅ The owner can't change fees by more than 20%.

✅ The owner can't set a max transaction limit

- **High severity issues**

The owner must enable trade for the holders, if trading remains disabled, no one would be able to buy and sell.



Contents

Audit details

Audited project
PurityAI 2.0 Token

Contract Address
0x28B984E14eC4CAfEc28724b4673a0C613AE22243

Client contact
PurityAI 2.0 Token Team

Blockchain
Binance Smart chain

Project website
https://purity-ai.live/

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Rugfreecoins hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

Rugfreecoins was commissioned by the PurityAI 2.0 Token Team to perform an audit of the smart contract.

https://bscscan.com/token/0x28B984E14eC4CAfEc28724b4673a0C613AE22243

This audit focuses on verifying that the smart contract is secure, resilient, and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, and long-term sustainability, and as a guide to improving the smart contract's security posture by remediating the identified issues.

Tokenomics

0% tax when buying

5% tax when selling

- 5% of trade goes to the marketing wallet in BNB

Target market and the concept

Target market

- Anyone who’s interested in the Crypto space with long-term investment plans.
- Anyone who’s ready to earn a passive income by holding tokens.
- Anyone who’s interested in trading tokens.
- Anyone who’s interested in taking part in the PurityAI token ecosystem.
- Anyone who’s interested in taking part in the future plans of PurityAI Token.
- Anyone who’s interested in making financial transactions with any other party using PurityAI Token as the currency.

Potential to grow with score points

1.	Project efficiency	8/10
2.	Project uniqueness	8/10
3	Information quality	8/10
4	Service quality	8/10
5	System quality	8/10
6	Impact on the community	8/10
7	Impact on the business	9/10
8	Preparing for the future	8/10
9	Smart contract security	9/10
10	Smart contract functionality assessment	10/10
Total Points		**8.4/10**

Contract details

Token contract details for 8th of July 2023

Contract name	PurityAI 2.0
Contract address	0x28B984E14eC4CAfEc28724b4673a0C613AE22243
Token supply	1,000,000,000
Token ticker	PURITY
Decimals	9
Token holders	3
Transaction count	9
Contract deployer address	0x000c0686E40d9c608251e72bddb097E033e6DD70
Contract's current owner address	0x000c0686E40d9c608251e72bddb097E033e6DD70
Marketing wallet	0x3d5444f328da47b0bf6ca5e94ec4ad954497efcb

Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security & centralization	Access control of owners	HIGH
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass

13	**Event security**		**pass**

Contract description table

The below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions, and implementations with their visibility and mutability.

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
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 🔒		
Address	**Library**			
L	isContract	Internal 🔒		
L	sendValue	Internal 🔒	🛑	
L	functionCall	Internal 🔒	🛑	
L	functionCall	Internal 🔒	🛑	
L	functionCallWithValue	Internal 🔒	🛑	

└	functionCallWithValue	Internal 🔒	🛑	
└	_functionCallWithValue	Private 🔐	🛑	
Context	**Implementation**			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	**Implementation**	**Context**		
└		Public ❗	🛑	NO ❗
└	owner	Public ❗		NO ❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
IERC20	**Interface**			
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	transfer	External ❗	🛑	NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
IUniswapV2 Factory	**Interface**			
└	feeTo	External ❗		NO ❗

└	feeToSetter	External ❗		NO ❗
└	getPair	External ❗		NO ❗
└	allPairs	External ❗		NO ❗
└	allPairsLength	External ❗		NO ❗
└	createPair	External ❗	🛑	NO ❗
└	setFeeTo	External ❗	🛑	NO ❗
└	setFeeToSetter	External ❗	🛑	NO ❗
IUniswapV2 Pair	**Interface**			
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	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 ❗
IUniswapV2 Router01	**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 !
└	getAmountIn	External !		NO !
└	getAmountsOut	External !		NO !
└	getAmountsIn	External !		NO !
IUniswapV2 Router02	**Interface**	**Iuniswap V2 Router01**		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External !	🛑	NO !
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External !	🛑	NO !
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External !	🛑	NO !
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External !	💵	NO !

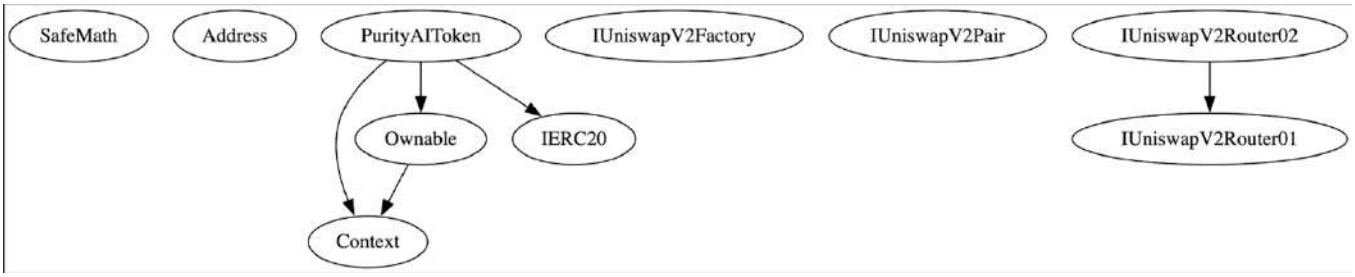
└	swapExactTokensForETHSupportingFee OnTransferTokens	External !	🛑	NO !
PurityAI Token	**Implementation**	**Context, IERC20, Ownable**		
└		Public !	🛑	NO !
└	name	Public !		NO !
└	symbol	Public !		NO !
└	decimals	Public !		NO !
└	totalSupply	Public !		NO !
└	balanceOf	Public !		NO !
└	allowance	Public !		NO !
└	increaseAllowance	Public !	🛑	NO !
└	decreaseAllowance	Public !	🛑	NO !
└	minimumTokensBeforeSwapAmount	Public !		NO !
└	approve	Public !	🛑	NO !
└	_approve	Private 🔐	🛑	
└	setIsFeeExempt	External !	🛑	onlyOwner
└	enableTrading	External !	🛑	onlyOwner
└	setSwapAndLiquifyEnabled	Public !	🛑	onlyOwner
└	getCirculatingSupply	Public !		NO !
└	transferToAddressETH	Private 🔐	🛑	
└		External !	💵	NO !

└	transfer	Public !	🛑	NO !
└	transferFrom	Public !	🛑	NO !
└	_transfer	Private 🔐	🛑	
└	_basicTransfer	Internal 🔒	🛑	
└	swapAndLiquify	Private 🔐	🛑	lockThe Swap
└	swapTokensForEth	Private 🔐	🛑	
└	takeFee	Internal 🔒	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Inheritance Hierarchy



Security issue checking status

- **High severity issues**

The owner must enable trade for the holders, if trading remains disabled, no one would be able to buy and sell.

```
ftrace | funcSig
function enableTrading() external onlyOwner {
    require(!tradingEnabled, "Trading is already enabled");
    tradingEnabled = true;
}
```

- **Medium severity issues**
  No medium severity issues found

- **Low severity issues**

Owner can not transfer ownership, can only renounce

```
abstract contract Ownable is Context {
    address private _owner;
    event OwnershipTransferred(address indexed prevOwner, address indexed newOwner);
    ftrace
    constructor () {
        _owner = 0x000c0686E40d9c608251e72bddb097E033e6DD70;
        emit OwnershipTransferred(address(0), _owner);
    }
    ftrace | funcSig
    function owner() public view virtual returns (address) {
        return _owner;
    }
    modifier onlyOwner() {
        require(owner() == _msgSender(), "Ownable: caller is not the owner");
        _;
    }
    ftrace | funcSig
    function renounceOwnership() public virtual onlyOwner {
        emit OwnershipTransferred(_owner, address(0));
        _owner = address(0);
    }
}
```

- **Centralization Risk**
  No centralization risks found

Owner privileges

- Owner can include/exclude wallets from fees

```
ftrace | funcSig
function setIsFeeExempt(address holder⬆, bool exempt⬆) external onlyOwner {
    isExcludedFromFee[holder⬆] = exempt⬆;
}
```

- Owner can enable trading, once enabled can not disable again

```
ftrace | funcSig
function enableTrading() external onlyOwner {
    require(!tradingEnabled, "Trading is already enabled");
    tradingEnabled = true;
}
```

- Owner can enable/disable swapping

```
ftrace | funcSig
function setSwapAndLiquifyEnabled(bool _enabled⬆) public onlyOwner {
    swapAndLiquifyEnabled = _enabled⬆;
    emit SwapAndLiquifyEnabledUpdated(_enabled⬆);
}
```

Audit conclusion

RugFreeCoins team has performed in-depth testings, line-by-line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASS**

Number of risk issues: **2**

Solidity code functional issue level: **PASS**

Number of owner privileges: **3**

Centralization risk correlated to the active owner: **HIGH**

Smart contract active ownership: **ACTIVE**