



Advanced Manual Smart Contract Audit



Project: Reward Token

Website: <https://rewardtokenbsc.com>

● Low-risk

9 low-risk code
issues found

● Medium-risk

1 medium-risk code
issues found

● High-risk

1 high-risk code
issues found

Contract address

0x048ab6dbfa7444de1d77a4970b6ed19d7495db36

Disclaimer: SureProtector is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

Disclaimer

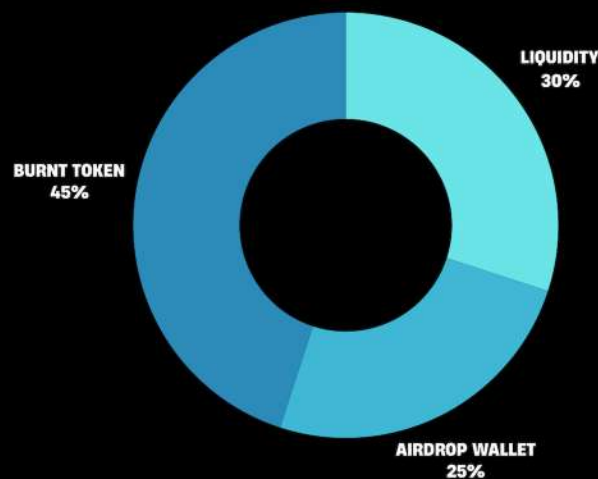
SureProtector is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

SureProtector is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

SureProtector can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics



Source code

SureProtector was commissioned by Reward Token to perform an audit based on the following smart contract:

<https://bscscan.com/address/0x048ab6dbfa7444de1d77a4970b6ed19d7495db36#code>

Manual Code Review



Low-risk

9 low-risk code issues found.




Medium-risk

1 medium-risk code issues found.



High-risk

1 medium-risk code issues found.

Issue ID	103
Severity	 Informational
Status	High
Description Code	<code>pragma solidity ^0.8.0;</code>
Location	<p>Different versions of Solidity is used:</p> <ul style="list-style-type: none">- Version used: ['=0.8.19', '>=0.5.0', '>=0.6.2', '^0.8.0', '^0.8.1']- ^0.8.0 (RWD.sol#27)- ^0.8.0 (RWD.sol#103)- ^0.8.0 (RWD.sol#129)- ^0.8.0 (RWD.sol#208)- ^0.8.1 (RWD.sol#421)- >=0.6.2 (RWD.sol#665)- >=0.5.0 (RWD.sol#803)- =0.8.19 (RWD.sol#823)



Issue ID	179
Severity	🎯 Informational
Status	Medium
Description Code	<pre>function includeInReward(address account) external onlyOwner { require(!_isExcluded[account], "Account is already included"); for (uint256 i = 0; i < _excluded.length; i++) { if (_excluded[i] == account) { _excluded[i] = _excluded[_excluded.length - 1]; _tOwned[account] = 0; _isExcluded[account] = false; _excluded.pop(); break; } } }</pre>
Location	RWD.includeInReward(address) (RWD.sol#1090-1101) has costly operations inside a loop: - _excluded.pop() (RWD.sol#1097)



Issue ID	156
Severity	🔴 Low
Status	Medium
Description Code	<pre>constructor(string memory _name_, string memory _symbol_, uint256 totalSupply_, address router_, address charityAddress_, address user, uint16 taxFeeBps_, uint16 liquidityFeeBps_, uint16 charityFeeBps_) Ownable() { if (charityAddress_ == address(0)) { require(charityFeeBps_ == 0, "Cant set both charity address to address 0 and charity percent more than 0"); } require(taxFeeBps_ + liquidityFeeBps_ + charityFeeBps_ <= MAX_FEE, "Total fee is over 25%"); _name = _name_; _symbol = _symbol_; _decimals = 9; _tTotal = totalSupply_; _rTotal = (MAX - (MAX % _tTotal)); _previousTaxFee = taxFeeBps_; _previousLiquidityFee = liquidityFeeBps_; _charityAddress = charityAddress_; _previousCharityFee = charityFeeBps_; numTokensSellToAddToLiquidity = totalSupply_.div(10**3); // 0.1% swapAndLiquifyEnabled = true; uint256 quarter = _rTotal / 4; _rOwned[charityAddress_] = quarter; _rOwned[user] = _rTotal - quarter; IUniswapV2Router _uniswapV2Router =</pre>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	function name() public view returns (string memory) { return _name; }
Location	name() should be declared external: - RWD.name() (RWD.sol#938-940)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	function symbol() public view returns (string memory) { return _symbol; }
Location	symbol() should be declared external: - RWD.symbol() (RWD.sol#942-944)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	function decimals() public view returns (uint8) { return _decimals; }
Location	decimals() should be declared external: - RWD.decimals() (RWD.sol#946-948)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function transfer(address recipient, uint256 amount) public override returns (bool) _transfer(msgSender(), recipient, amount); return true; }</pre>
Location	<p>transfer(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- RWD.transfer(address,uint256) (RWD.sol#959-966)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function allowance(address owner, address spender) public view override returns (uint256) return _allowances[owner][spender]; }</pre>
Location	<p>allowance(address,address) should be declared external:</p> <ul style="list-style-type: none">- RWD.allowance(address,address) (RWD.sol#968-975)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function approve(address spender, uint256 amount) public override returns (bool) _approve(_msgSender(), spender, amount); return true; }</pre>
Location	<p>approve(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- RWD.approve(address,uint256) (RWD.sol#977-984)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function transferFrom(address sender, address recipient, uint256 amount) public override returns (bool) { _transfer(sender, recipient, amount); _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "ERC20: transfer amount exceeds allowance")); return true; }</pre>
Location	<p>transferFrom(address,address,uint256) should be declared external:</p> <ul style="list-style-type: none">- RWD.transferFrom(address,address,uint256) <p>(RWD.sol#986-1001)</p>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool) _approve(_msgSender(), spender, _allowances[_msgSender()] [spender].add(addedValue)); return true; }</pre>
Location	<p>increaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- RWD.increaseAllowance(address,uint256) <p>(RWD.sol#1003-1014)</p>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool) _approve(_msgSender(), spender, _allowances[_msgSender()][spender].sub(subtractedValue, "ERC20: decreased allowance below zero")); return true; }</pre>
Location	<p>decreaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- RWD.decreaseAllowance(address,uint256) <p>(RWD.sol#1016-1030)</p>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function isExcludedFromReward(address account) public view returns (bool) { return _isExcluded[account]; }</pre>
Location	<p>isExcludedFromReward(address) should be declared external:</p> <ul style="list-style-type: none">- RWD.isExcludedFromReward(address) <p>(RWD.sol#1032-1034)</p>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	function totalFees() public view returns (uint256) { return _tFeeTotal; }
Location	totalFees() should be declared external: - RWD.totalFees() (RWD.sol#1036-1038)



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function deliver(uint256 tAmount) public { address sender = _msgSender(); require(!_isExcluded[sender], "Excluded addresses cannot call this function"); (uint256 rAmount, , , , ,) = _getValues(tAmount); _rOwned[sender] = _rOwned[sender].sub(rAmount); _rTotal = _rTotal.sub(rAmount); _tFeeTotal = _tFeeTotal.add(tAmount); }</pre>
Location	<p>deliver(uint256) should be declared external: - RWD.deliver(uint256) (RWD.sol#1040-1050)</p>



Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function reflectionFromToken(uint256 tAmount, bool deductTransferFee) public view returns (uint256) require(tAmount <= _tTotal, "Amount must be less than supply"); if (!deductTransferFee) { (uint256 rAmount, , , ,) = _getValues(tAmount); return rAmount; } else { (, uint256 rTransferAmount, , ,) = _getValues(tAmount); return rTransferAmount; } }</pre>
Location	<p>reflectionFromToken(uint256,bool) should be declared external:</p> <ul style="list-style-type: none">- RWD.reflectionFromToken(uint256,bool) <p>(RWD.sol#1052-1065)</p>



Issue ID	177
Severity	🎯 Informational
Status	High
Description Code	<code>pragma solidity ^0.8.0;</code>
Location	Pragma version^0.8.0 (RWD.sol#27) allows old versions



Issue ID	177
Severity	 Informational
Status	High
Description Code	<code>pragma solidity ^0.8.1;</code>
Location	Pragma version^0.8.1 (RWD.sol#421) allows old versions



Issue ID	177
Severity	🎯 Informational
Status	High
Description Code	<code>pragma solidity >=0.6.2;</code>
Location	Pragma version>=0.6.2 (RWD.sol#665) allows old versions




Issue ID	177
Severity	🎯 Informational
Status	High
Description Code	<code>pragma solidity >=0.5.0;</code>
Location	Pragma version>=0.5.0 (RWD.sol#803) allows old versions



Issue ID	177
Severity	 Informational
Status	High
Description Code	<code>pragma solidity =0.8.19;</code>
Location	Pragma version=0.8.19 (RWD.sol#823) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7



Issue ID	177
Severity	 Informational
Status	High
Description Code	
Location	solc-0.8.19 is not recommended for deployment



Issue ID	173
Severity	🕒 Informational
Status	High
Description Code	<pre>function sendValue(address payable recipient, uint256 amount) internal { require(address(this).balance >= amount, "Address: insufficient balance"); (bool success,) = recipient.call{value: amount}(""); require(success, "Address: unable to send value, recipient may have reverted"); }</pre>
Location	<p>Low level call in Address.sendValue(address,uint256) (RWD.sol#481-486):</p> <p>- (success) = recipient.call{value: amount}() (RWD.sol#484)</p>




Issue ID	173
Severity	🕒 Informational
Status	High
Description Code	<pre>function functionCallWithValue(address target, bytes memory data, uint256 value, string memory errorMessage) internal returns (bytes memory) { require(address(this).balance >= value, "Address: insufficient balance for call"); (bool success, bytes memory returndata) = target.call{value: value}(data); return verifyCallResultFromTarget(target, success, returndata, errorMessage); }</pre>
Location	<p>Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (RWD.sol#545-554): - (success,returndata) = target.call{value: value}(data) (RWD.sol#552)</p>



Issue ID	173
Severity	🕒 Informational
Status	High
Description Code	<pre>function functionStaticCall(address target, bytes memory data, string memory errorMessage) internal view returns (bytes memory) { (bool success, bytes memory returndata) = target.staticcall(data); return verifyCallResultFromTarget(target, success, returndata, errorMessage); }</pre>
Location	<p>Low level call in Address.functionStaticCall(address,bytes,string) (RWD.sol#572-579): - (success,returndata) = target.staticcall(data) (RWD.sol#577)</p>



Issue ID	173
Severity	 Informational
Status	High
Description Code	<pre>function functionDelegateCall(address target, bytes memory data, string memory errorMessage) internal returns (bytes memory) { (bool success, bytes memory returndata) = target.delegatecall(data); return verifyCallResultFromTarget(target, success, returndata, errorMessage); }</pre>
Location	<p>Low level call in Address.functionDelegateCall(address,bytes,string) (RWD.sol#597-604): - (success,returndata) = target.delegatecall(data) (RWD.sol#602)</p>



Issue ID	167-a
Severity	🔴 Low
Status	Medium
Description Code	<pre>function setTaxFeePercent(uint256 taxFeeBps) external onlyOwner { _taxFee = taxFeeBps; require(_taxFee + _liquidityFee + _charityFee <= MAX_FEE, "Total fee is over 25%"); }</pre>
Location	<p>RWD.setTaxFeePercent(uint256) (RWD.sol#1143-1149) should emit an event for:</p> <ul style="list-style-type: none">- _taxFee = taxFeeBps (RWD.sol#1144)




Issue ID	167-a
Severity	🔴 Low
Status	Medium
Description Code	<pre>function setLiquidityFeePercent(uint256 liquidityFeeBps) external onlyOwner _liquidityFee = liquidityFeeBps; require(_taxFee + _liquidityFee + _charityFee <= MAX_FEE, "Total fee is over 25%"); }</pre>
Location	<pre>RWD.setLiquidityFeePercent(uint256) (RWD.sol#1151-1160) should emit an event for: - _liquidityFee = liquidityFeeBps (RWD.sol#1155)</pre>




Issue ID	167-a
Severity	🔴 Low
Status	Medium
Description Code	<pre>function setCharityFeePercent(uint256 charityFeeBps) external onlyOwner { _charityFee = charityFeeBps; require(_taxFee + _liquidityFee + _charityFee <= MAX_FEE, "Total fee is over 25%"); }</pre>
Location	<p>RWD.setCharityFeePercent(uint256) (RWD.sol#1162-1168) should emit an event for:</p> <ul style="list-style-type: none">- _charityFee = charityFeeBps (RWD.sol#1163)



Issue ID	209
Severity	 Critical
Status	High
Description Code	<pre>function transfer(address recipient, uint256 amount) public override returns (bool) _transfer(_msgSender(), recipient, amount); return true; }</pre>
Location	<p>Transfer Fee: RWD.transfer(address,uint256) (RWD.sol#959-966)</p> <ul style="list-style-type: none">- in nested function: _getTValues- in expression: _amount.mul(_taxFee).div(10 ** 4)- in expression: _amount.mul(_liquidityFee).div(10 ** 4)- in expression: _amount.mul(_charityFee).div(10 ** 4)



Issue ID	7
Severity	 Data
Status	High
Description Code	
Location	Transfer fee variables



Issue ID	237
Severity	🔴 Low
Status	High
Description Code	<pre>function transferFrom(address sender, address recipient, uint256 amount) public override returns (bool) { _transfer(sender, recipient, amount); _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "ERC20: transfer amount exceeds allowance")); return true; }</pre>
Location	<p>whitelisted function: RWD.transferFrom(address,address,uint256) (RWD.sol#986-1001)</p> <p>- in internal call: RWD._transfer(address,address,uint256) (RWD.sol#1359-1397)</p> <p>- in expression _isExcluded[account]</p>



Issue ID	237
Severity	🎯 Low
Status	High
Description Code	<pre>function transfer(address recipient, uint256 amount) public override returns (bool) _transfer(_msgSender(), recipient, amount); return true; }</pre>
Location	<p>whitelisted function: RWD.transfer(address,uint256) (RWD.sol#959-966)</p> <p>- in internal call: RWD._transfer(address,address,uint256) (RWD.sol#1359-1397)</p> <p>- in expression _isExcluded[account]</p>

Website Review

 Reward Token

[Buy](#)

Earn continuous rewards by holding **Reward Token**.





A community-driven token built on the **BNB** smart chain to reward loyalty and engagement in the Web3 space

 [Copy contract address](#)

[Join community](#) 



SureProtector checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.

-  Mobile Friendly
-  Contains no jQuery errors
-  SSL Secured
-  No major spelling errors

Loading speed: 91%

Rug-pull Review

Based on the available information analyzed by us, we come to the following conclusions:

● Tax Modifiable

● No doxxed Team

Honeypot Review

Based on the available information analyzed by us, we come to the following conclusions:

● There is not enough data

Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.