



August 13, 2023

# Express Audit Report for **BigToe [BTO]**

DISCLAIMER: This is an automatically generated audit performed with De.Fi Scanner tool. De.Fi smart contract auditing tool is intended to assist in identifying potential vulnerabilities or malicious functions in smart contracts. While this is done to our best effort and knowledge, please notice that no tool can guarantee complete accuracy or comprehensiveness in detecting all possible vulnerabilities.



## Project Summary


Project Name	TaxableTeamToken(BigToe)
Address	<a href="#">0x013f29ffcceda635f434c1c539c23b6be84201c0</a>
Network	56

Issue ID	103
Severity	 High
Status	Informational
Description Code	<b>pragma solidity</b> >=0.6.2 <0.8.0;
Location	<p>Different versions of Solidity is used:</p> <ul style="list-style-type: none"><li>- Version used: ['0.6.12', '&gt;=0.6.0&lt;0.8.0', '&gt;=0.6.2&lt;0.8.0']</li><li>- &gt;=0.6.2&lt;0.8.0 (Address.sol#4)</li><li>- &gt;=0.6.0&lt;0.8.0 (Context.sol#3)</li><li>- &gt;=0.6.0&lt;0.8.0 (IERC20.sol#3)</li><li>- &gt;=0.6.0&lt;0.8.0 (Ownable.sol#4)</li><li>- &gt;=0.6.0&lt;0.8.0 (SafeMath.sol#3)</li><li>- 0.6.12 (TaxableTeamToken.sol#3)</li></ul>

Issue ID	179
Severity	🔴 Medium
Status	Informational
Description Code	<pre><b>function includeAccount</b>(address account) <b>external onlyOwner</b>() {   <b>require</b>(!_isExcluded[account], "Account is already   excluded");   <b>for</b> (<b>uint256</b> i = 0; i &lt; _excluded.length; i++) {     <b>if</b> (_excluded[i] == account) {       _excluded[i] = _excluded[_excluded.length - 1];       _tOwned[account] = 0;       _isExcluded[account] = <b>false</b>;       _excluded.pop();       <b>break</b>;     }   } }</pre>
Location	<p>TaxableTeamToken.includeAccount(address) (TaxableTeamToken.sol#180-191) has costly operations inside a loop: - _excluded.pop() (TaxableTeamToken.sol#187)</p>

Issue ID	184
Severity	🎯 High
Status	Optimization
Description Code	<b>function name() public view returns (string memory) { return _name; }</b>
Location	name() should be declared external: - TaxableTeamToken.name() (TaxableTeamToken.sol#78-80)

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<b>function symbol() public view returns (string memory) { return _symbol; }</b>
Location	symbol() should be declared external: - TaxableTeamToken.symbol() (TaxableTeamToken.sol#82-84)

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<b>function decimals() public view returns (uint8) { return _decimals; }</b>
Location	decimals() should be declared external: - TaxableTeamToken.decimals() (TaxableTeamToken.sol#86-88)

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<b>function totalSupply() public view override returns (uint256) { return _tTotal; }</b>
Location	totalSupply() should be declared external: - TaxableTeamToken.totalSupply() (TaxableTeamToken.sol#90-92)






Issue ID	184
Severity	🎯 High
Status	Optimization
Description Code	<b>function fees() public view returns (uint256) { return _feesPercentage; }</b>
Location	fees() should be declared external: - TaxableTeamToken.fees() (TaxableTeamToken.sol#94-96)

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function balanceOf</b>(address account) <b>public view</b> <b>override returns</b> (uint256) {   <b>if</b> (_isExcluded[account]) <b>return</b> _tOwned[account];   <b>return</b> tokenFromReflection(_rOwned[account]); }</pre>
Location	<p>balanceOf(address) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.balanceOf(address)</li></ul> <p>(TaxableTeamToken.sol#98-101)</p>

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function</b> <b>transfer</b>(<b>address</b> recipient, <b>uint256</b> amount) <b>public override returns</b> (<b>bool</b>) {   _transfer(_msgSender(), recipient, amount);   <b>return</b> <b>true</b>; }</pre>
Location	<p>transfer(address,uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.transfer(address,uint256) (TaxableTeamToken.sol#103-106)</li></ul>

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<b>function allowance</b> (address owner, address spender) <b>public view override returns</b> (uint256) { <b>return</b> _allowances[owner][spender]; }
Location	allowance(address,address) should be declared external: - TaxableTeamToken.allowance(address,address) (TaxableTeamToken.sol#108-110)


Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function approve</b>(address spender, uint256 amount) <b>public override returns (bool)</b> {   _approve(_msgSender(), spender, amount);   <b>return true</b>; }</pre>
Location	<p>approve(address,uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.approve(address,uint256) (TaxableTeamToken.sol#112-115)</li></ul>

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre><b>function transferFrom</b>(address sender, address recipient, uint256 amount) <b>public override returns</b> <b>(bool)</b> {   _transfer(sender, recipient, amount);   _approve(sender, _msgSender(), _allowances[sender]     [_msgSender()]).sub(amount, "ERC20: transfer amount exceeds allowance");   <b>return true</b>; }</pre>
Location	<p>transferFrom(address,address,uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.transferFrom(address,address,uint256) (TaxableTeamToken.sol#117-121)</li></ul>


Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function</b> <b>increaseAllowance</b>(<b>address</b> spender, <b>uint256</b> addedValue) <b>public virtual returns</b> (<b>bool</b>) {   _approve(_msgSender(), spender,     _allowances[_msgSender()])   [spender].add(addedValue);   <b>return</b> <b>true</b>; }</pre>
Location	<p>increaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.increaseAllowance(address,uint256) (TaxableTeamToken.sol#123-126)</li></ul>

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function decreaseAllowance</b>(<b>address</b> spender, <b>uint256</b> subtractedValue) <b>public virtual returns</b> <b>(bool)</b> {     _approve(_msgSender(), spender,     _allowances[_msgSender()])     [spender].sub(subtractedValue, "ERC20: decreased allowance below zero");     <b>return true</b>; }</pre>
Location	<p>decreaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.decreaseAllowance(address,uint256) (TaxableTeamToken.sol#128-131)</li></ul>



Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre><b>function isExcluded(address account) public view returns (bool) {     return _isExcluded[account]; }</b></pre>
Location	<p>isExcluded(address) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.isExcluded(address)</li></ul> <p>(TaxableTeamToken.sol#133-135)</p>

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<b>function totalFees() public view returns (uint256) { return _tFeeTotal; }</b>
Location	totalFees() should be declared external: - TaxableTeamToken.totalFees() (TaxableTeamToken.sol#137-139)

Issue ID	184
Severity	 High
Status	Optimization
Description Code	<pre><b>function reflect</b>(uint256 tAmount) <b>public</b> {   <b>address</b> sender = _msgSender();   <b>require</b>((!_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>reflect(uint256) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.reflect(uint256)</li></ul> <p>(TaxableTeamToken.sol#141-148)</p>

Issue ID	184
Severity	🔴 High
Status	Optimization
Description Code	<pre><b>function reflectionFromToken(uint256 tAmount, bool deductTransferFee) public view returns(uint256) {   require(tAmount &lt;= _tTotal, "Amount must be less than supply");   if (!deductTransferFee) {     (uint256 rAmount,,,,) = _getValues(tAmount);     return rAmount;   } else {     (uint256 rTransferAmount,,,,) = _getValues(tAmount);     return rTransferAmount;   } }</b></pre>
Location	<p>reflectionFromToken(uint256,bool) should be declared external:</p> <ul style="list-style-type: none"><li>- TaxableTeamToken.reflectionFromToken(uint256,bool) (TaxableTeamToken.sol#150-159)</li></ul>



De.Fi


Issue ID	177
Severity	🎯 High
Status	Informational
Description Code	<b>pragma solidity</b> >=0.6.2 <0.8.0;
Location	Pragma version>=0.6.2<0.8.0 (Address.sol#4) is too complex



**De.Fi**


Issue ID	177
Severity	🎯 High
Status	Informational
Description Code	<b>pragma solidity</b> >=0.6.0 <0.8.0;
Location	Pragma version>=0.6.0<0.8.0 (Context.sol#3) is too complex

Issue ID	173
Severity	🔴 High
Status	Informational
Description Code	<pre>function <b>sendValue</b>(address payable recipient, uint256 amount) <b>internal</b> {   <b>require</b>(address(this).balance &gt;= amount, "Address: insufficient balance");   // solhint-disable-next-line avoid-low-level-calls,   avoid-call-value   (bool success, ) = recipient.call{ value: amount }("");   <b>require</b>(success, "Address: unable to send value, recipient may have reverted"); }</pre>
Location	<p>Low level call in Address.sendValue(address,uint256) (Address.sol#54-60):</p> <ul style="list-style-type: none"><li>- (success) = recipient.call{value: amount}() (Address.sol#58)</li></ul>

Issue ID	173
Severity	 High
Status	Informational
Description Code	<pre>function <b>functionCallWithValue</b>(address target, <b>bytes memory</b> data, <b>uint256</b> value, <b>string memory</b> errorMessage) <b>internal returns</b> (<b>bytes memory</b>) {   <b>require</b>(address(this).balance &gt;= value, "Address:   insufficient balance for call");   <b>require</b>(isContract(target), "Address: call to non-   contract");   // solhint-disable-next-line avoid-low-level-calls   (<b>bool</b> success, <b>bytes memory</b> returndata) =   target.call{ value: value }(data);   <b>return</b> _verifyCallResult(success, returndata,   errorMessage); }</pre>
Location	<p>Low level call in Address.functionCallWithValue(address,bytes,uint256, string) (Address.sol#115-122): - (success,returndata) = target.call{value: value}(data) (Address.sol#120)</p>



Issue ID	173
Severity	🔴 High
Status	Informational
Description Code	<pre><b>function functionStaticCall</b>(address target, <b>bytes</b> <b>memory</b> data, <b>string memory</b> errorMessage) <b>internal view returns</b> (<b>bytes memory</b>) {     <b>require</b>(isContract(target), "Address: static call to non-     contract");     // solhint-disable-next-line avoid-low-level-calls     (<b>bool</b> success, <b>bytes memory</b> returndata) =     target.<b>staticcall</b>(data);     <b>return</b> _verifyCallResult(success, returndata,     errorMessage); }</pre>
Location	<p>Low level call in Address.functionStaticCall(address,bytes,string) (Address.sol#140-146): - (success,returndata) = target.staticcall(data) (Address.sol#144)</p>

Issue ID	173
Severity	 High
Status	Informational
Description Code	<pre><b>function functionDelegateCall</b>(<b>address</b> target, <b>bytes memory</b> data, <b>string memory</b> errorMessage) <b>internal returns</b> (<b>bytes memory</b>) {     <b>require</b>(isContract(target), "Address: delegate call to     non-contract");     // solhint-disable-next-line avoid-low-level-calls     (<b>bool</b> success, <b>bytes memory</b> returndata) =     target.<b>delegatecall</b>(data);     <b>return</b> _verifyCallResult(success, returndata,     errorMessage); }</pre>
Location	<p>Low level call in Address.functionDelegateCall(address,bytes,string) (Address.sol#164-170): - (success,returndata) = target.delegatecall(data) (Address.sol#168)</p>

Issue ID	167-a
Severity	🔴 Medium
Status	Low
Description Code	<b>function setFeesPercentage(uint256</b> feesPercentage) <b>external onlyOwner()</b> <b>checksFeesValid</b> (feesPercentage) { _feesPercentage = feesPercentage; }
Location	TaxableTeamToken.setFeesPercentage(uint256) (TaxableTeamToken.sol#176-178) should emit an event for: - _feesPercentage = feesPercentage (TaxableTeamToken.sol#177)

Issue ID	209
Severity	🔴 High
Status	Critical
Description Code	<b>function transfer</b> (address recipient, uint256 amount) <b>public override returns (bool)</b> { _transfer(_msgSender(), recipient, amount); <b>return true;</b> }
Location	Transfer Fee: TaxableTeamToken.transfer(address,uint256) (TaxableTeamToken.sol#103-106) - in nested function: _getTVValues - in expression: tFee = tAmount.mul(_feesPercentage).div(100)



**De.Fi**

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

Issue ID	237
Severity	🔴 High
Status	Low
Description Code	<pre><b>function transferFrom</b>(address sender, address recipient, uint256 amount) <b>public override returns (bool)</b> {     _transfer(sender, recipient, amount);     _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount, "ERC20: transfer amount exceeds allowance"));     <b>return true</b>; }</pre>
Location	<p>whitelisted function: TaxableTeamToken.transferFrom(address,address,uint256) (TaxableTeamToken.sol#117-121) - in internal call: TaxableTeamToken._transfer(address,address,uint256) (TaxableTeamToken.sol#201-216) - in expression _isExcluded[sender] &amp;&amp; !_isExcluded[recipient]</p>

Issue ID	237
Severity	🔴 High
Status	Low
Description Code	<pre>function transfer(address recipient, uint256 amount) public override returns (bool) {   _transfer(_msgSender(), recipient, amount);   return true; }</pre>
Location	<p>whitelisted function: TaxableTeamToken.transfer(address,uint256) (TaxableTeamToken.sol#103-106)</p> <p>- in internal call: TaxableTeamToken._transfer(address,address,uint256) (TaxableTeamToken.sol#201-216)</p> <p>- in expression _isExcluded[sender] &amp;&amp; !_isExcluded[recipient]</p>