SECURI LAB

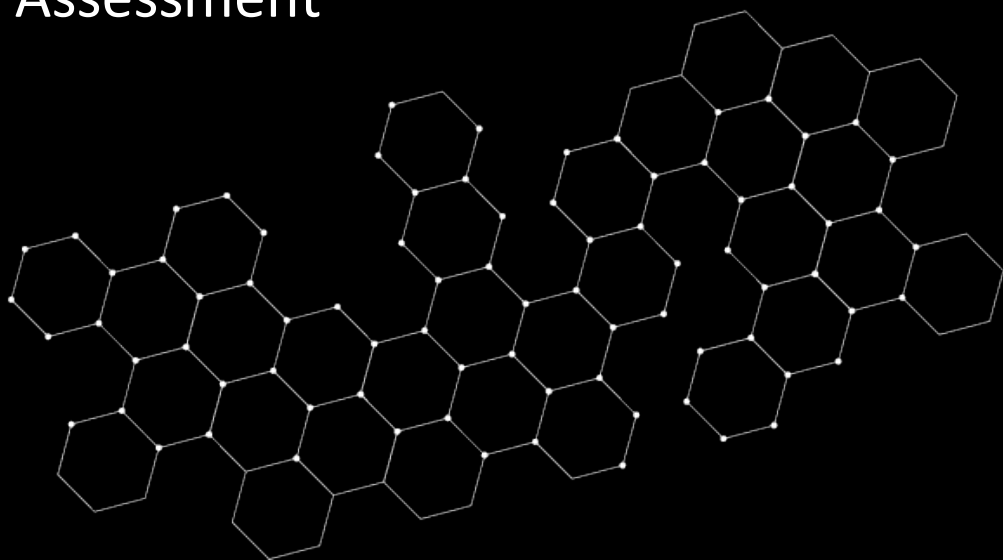
Cybersecurity Audit | KYC | Consultant

Partner Quota

TorkPad

Full Audit report

TorkPad Security Assessment



AUDIT BY SECURI

SECURI contact@securi-lab.com

FULL AUDIT REPORT

Table of Contents

Contact us: contact@securi-lab.com
Website: https://securi-lab.com
Telegram: https://t.me/securi_lab
Twitter: https://twitter.com/SECURI_LAB

FULL AUDIT REPORT

Report Information

About Report	TorkPad Security Assessment
Version	v1.1
Client	TorkPad
Language	Solidity
Confidentiality	Public
Platform	BNB Chain (Previously Binance Smart Chain)
Contract Address	0x77972A1BA3cAb14E1E907b58BBc4971544f4719d
Audit Method	Whitebox

*Audit Method

Whitebox: Securi Team receives all source code from the client to provide the assessment.
Blackbox: Securi Team receives only bytecode from the client to provide the assessment.

Digital Sign (Only Full Audit Report)

Digitally signed by CHIN J
DN: cn=CHIN J, o=SECURI LAB - Cybersecurity | Audit | KYC, ou=CEO, email=contact@securi-lab.com, c=TH
Date: 2022.10.09 18:00:10 +07'00'

Contact us: contact@securi-lab.com
Website: https://securi-lab.com
Telegram: https://t.me/securi_lab
Twitter: https://twitter.com/SECURI_LAB

FULL AUDIT REPORT

Disclaimer

Regarding this security assessment, there are no guarantees about the security of the program instruction received from the client is hereinafter referred to as "**Source code**".
And **SECURI** hereinafter referred to as "**Service Provider**", the **Service Provider** will not be held liable for any legal liability arising from errors in the security assessment. The responsibility will be the responsibility of the **client**, hereinafter referred to as "**Service User**" and the **service user** agrees not to be held liable to the **service provider** in any case. By contract **service provider** to conduct security assessments with integrity with professional ethics, and transparency to deliver security assessments to users The **service provider** has the right to postpone the delivery of the security assessment. If the security assessment is delayed whether caused by any reason and is not responsible for any delayed security assessments. If **the service provider** finds a vulnerability The **service provider** will notify the **service user** via the Preliminary Report, which will be kept confidential for security. The **service provider** disclaims responsibility in the event of any attacks occurring whether before conducting a security assessment. Or happened later All responsibility shall be sole with the **service user**.

Security Assessment Not Financial/Investment Advice Any loss arising from any investment in any project is the responsibility of the investor.

SECURI disclaims any liability incurred. Whether it's Rugpull, Abandonment, Soft Rugpull

FULL AUDIT REPORT

Executive Summary

For this security assessment, SECURI LAB received a request from TorkPad on Wednesday, October 5, 2022.

The SECURI LAB team has conducted a comprehensive security assessment of the vulnerabilities. This assessment is tested with an expert assessment. Using the following test requirements

1. Smart Contract Testing with Expert Analysis By testing the most common and uncommon vulnerabilities.
2. Automated program testing It includes a sample vulnerability test and a sample of the potential vulnerabilities being used for the most frequent attacks.
3. Visibility, Mutability, Modifier function testing, such as whether a function can be seen in general, or whether a function can be changed and if so, who can change it.
4. Function association test It will be displayed through the association graph.
5. This safety assessment is cross-checked prior to the delivery of the assessment results.

Audit Result

Securi evaluated the smart contract security of the Example project and found: **[Total : 6 Issues]**

Critical	High	Medium	Low	Very Low	Informational
0	0	0	5	0	1

Contact us: contact@securi-lab.com
Website: https://securi-lab.com
Telegram: https://t.me/securi_lab
Twitter: https://twitter.com/SECURI_LAB

FULL AUDIT REPORT

Project Introduction

Scope Information:

Project Name	TorkPad
Website	https://torkpad.io/
Chain	BNB Chain (Previously Binance Smart Chain)
Language	Solidity

Audit Information:

Request Date	Wednesday, October 5, 2022
Audit Date	Sunday, October 9, 2022

Audit Version History:

Version	Date	Description
1.0	Sunday, October 9, 2022	Preliminary Report
1.1	Sunday, October 9, 2022	Full Audit Report

FULL AUDIT REPORT

Initial Audit Scope: Contract: 0x77972A1BA3cAb14E1E907b58BBc4971544f4719d

Smart Contract	0x77972A1BA3cAb14E1E907b58BBc4971544f4719d
Contract Name	**TORKPAD**
Compiler Version	**v0.8.16+commit.07a7930e**

FULL AUDIT REPORT

Security Assessment Procedure

Securi has the following procedures and regulations for conducting security assessments:

1.Request Audit Client submits a form request through the Securi channel. After receiving the request, Securi will discuss a security assessment. And drafting a contract and agreeing to sign a contract together with the Client

2.Auditing Securi performs security assessments of smart contracts obtained through automated analysis and expert manual audits.

3.Preliminary Report At this stage, Securi will deliver an initial security assessment. To report on vulnerabilities and errors found under Audit Scope will not publish preliminary reports for safety.

4.Reassessment After Securi has delivered the Preliminary Report to the Client, Securi will track the status of the vulnerability or error, which will be published to the Final Report at a later date with the following statuses:

- **a.Acknowledge** The client has been informed about errors or vulnerabilities from the security assessment.
- **b.Resolved** The client has resolved the error or vulnerability. Resolved is probably just a commit, and Securi is unable to verify that the resolved has been implemented or not.
- **c.Decline** Client has rejected the results of the security assessment on the issue.

5.Final Report Securi providing full security assessment report and public

Risk Rating

Risk rating using this commonly defined: $Risk\ rating\ =\ impact\ *\ confidence$

Impact The severity and potential impact of an attacker attack

Confidence Ensuring that attackers expose and use this vulnerability

Both have a total of 3 levels: **High**, **Medium**, **Low**. By *Informational* will not be classified as a level

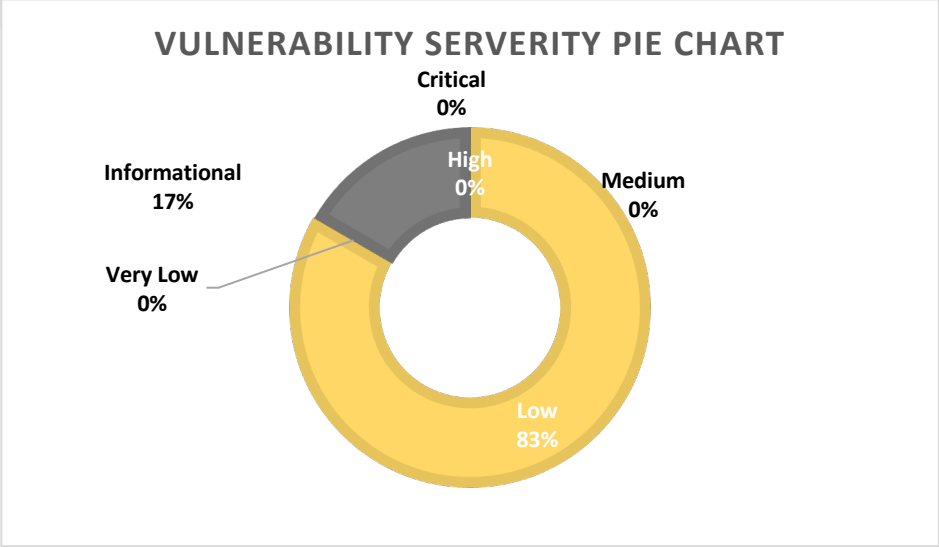
Impact \ Confidence	Low	Medium	High
Low	Very Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Severity is a risk assessment It is calculated from the Impact and Confidence values using the following calculation methods, $Risk\ rating\ =\ impact\ *\ confidence$ It is categorized into **5 categories based** on the **lowest severity**: Very Low , Low , Medium , **High** , Critical .
For **Informational** will not be counted as **severity**

FULL AUDIT REPORT

Vulnerability Severity Summary

Vulnerability Severity Level	Total
Critical	0
High	0
Medium	0
Low	5
Very Low	0
Informational (Non severity level)	1



Vulnerability Findings

ID	Title	Severity	Status
SEC-01	Unchecked tokens transfer	Low	**Acknowledge**
SEC-02	Imprecise arithmetic operations order	Low	**Acknowledge**
SEC-03	Missing Zero Address Validation	Low	**Acknowledge**
SEC-04	Missing Events Arithmetic	Low	**Acknowledge**
SEC-05	Local variables shadowing	Low	**Acknowledge**
SEC-06	Conformance to numeric notation best practices	Informational	**Acknowledge**

SEC-01: Unchecked tokens transfer

Type	Severity	Location	Status
Unchecked tokens transfer (unchecked-transfer)	Low	Line: 901-905	**Acknowledge**

Finding:

❌ TORKPAD.recoverWrongTokens(address) (TORKPAD.sol:901-905) ignores return value by IERC20(_tokenAddress).transfer(address(msg.sender),_tokenAmount) (TORKPAD.sol#904)

Recommendation:

Use `SafeERC20`, or ensure that the transfer/transferFrom return value is checked.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer

Alleviation:

TorkPad Team has acknowledge this issue

SEC-02: Imprecise arithmetic operations order

Type	Severity	Location	Status
Imprecise arithmetic operations order (divide-before-multiply)	Low	Line: Check on finding	**Acknowledge**

Finding:

❌ TORKPAD.swapBack() (TORKPAD.sol:791-827) performs a multiplication on the result of a division:
- devAmount = contractBalance * devAccrued / swapAccrued (TORKPAD.sol#800)
- safeTransferBNB(devWallet,amountEth * devAmount / convertAmount) (TORKPAD.sol#813)

❌ TORKPAD.swapBack() (TORKPAD.sol:791-827) performs a multiplication on the result of a division:
- marketingAmount = contractBalance * marketingAccrued / swapAccrued (TORKPAD.sol#799)
- safeTransferBNB(marketingWallet,amountEth * marketingAmount / convertAmount) (TORKPAD.sol#812)

Recommendation:

Consider ordering multiplication before division.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply

Alleviation:

TorkPad Team has acknowledge this issue

SEC-03: Missing Zero Address Validation

Type	Severity	Location	Status
Missing Zero Address Validation (missing-zero-check)	Low	Line: Check on finding	**Acknowledge**

Finding:

❌ TORKPAD.constructor(address).pair (TORKPAD.sol:668-671) lacks a zero-check on :
- lp_pair = pair (TORKPAD.sol#673)
- initialLiquidityPair = pair (TORKPAD.sol#679)

Recommendation:

Check that the address is not zero.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation

Alleviation:

TorkPad Team has acknowledge this issue

SEC-04: Missing Events Arithmetic

Type	Severity	Location	Status
Missing Events Arithmetic (events-maths)	Low	Line: Check on finding	**Acknowledge**

Finding:

❌ TORKPAD.setBurnTax(uint256,uint256) (TORKPAD.sol:750-754) should emit an event for:
- buyBurnTax = _buyBurnTax (TORKPAD.sol#751)
- sellBurnTax = _sellBurnTax (TORKPAD.sol#752)

❌ TORKPAD.setDevTax(uint256,uint256) (TORKPAD.sol:744-748) should emit an event for:
- buyDevTax = _buyDevTax (TORKPAD.sol#745)
- sellDevTax = _sellDevTax (TORKPAD.sol#746)

❌ TORKPAD.setLiquidityPair(address,bool)._lp (TORKPAD.sol:709) lacks a zero-check on :
- lp_pair = _lp (TORKPAD.sol#712)

❌ TORKPAD.setLiquidityTax(uint256,uint256) (TORKPAD.sol:720-724) should emit an event for:
- buyLiquidityTax = _buyLiquidityTax (TORKPAD.sol#721)
- sellLiquidityTax = _sellLiquidityTax (TORKPAD.sol#722)

❌ TORKPAD.setLpStakingTax(uint256,uint256) (TORKPAD.sol:738-742) should emit an event for:
- buyLpStakingTax = _buyLpStakingTax (TORKPAD.sol#739)
- sellLpStakingTax = _sellLpStakingTax (TORKPAD.sol#740)

❌ TORKPAD.setMarketingTax(uint256,uint256) (TORKPAD.sol:726-730) should emit an event for:
- buyMarketingTax = _buyMarketingTax (TORKPAD.sol#727)
- sellMarketingTax = _sellMarketingTax (TORKPAD.sol#728)

❌ TORKPAD.setMaxWallet(uint256) (TORKPAD.sol:687-690) should emit an event for:
- maxWallet = maxSupply * _maxWalletPercent / 1e4 (TORKPAD.sol#689)

❌ TORKPAD.setNativeStakingTax(uint256,uint256) (TORKPAD.sol:732-736) should emit an event for:
- buyNativeStakingTax = _buyNativeStakingTax (TORKPAD.sol#733)
- sellNativeStakingTax = _sellNativeStakingTax (TORKPAD.sol#734)

❌ TORKPAD.setSwapThreshold(uint256) (TORKPAD.sol:756-759) should emit an event for:

- swapThreshold = _swapThreshold (TORKPAD.sol#758)

Recommendation:

Emit an event for critical parameter changes.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-arithmetic

Alleviation:

TorkPad Team has acknowledge this issue

SEC-05: Local variables shadowing

Type	Severity	Location	Status
Local variables shadowing (shadowing-local)	Low	Line: Check on finding	**Acknowledge**

Finding:

❌ TORKPAD.transfer(address,uint256).owner (TORKPAD.sol:786) shadows:
- Ownable.owner() (TORKPAD.sol#63-65) (function)

Recommendation:

Rename the local variables that shadow another component.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

Alleviation:

TorkPad Team has acknowledge this issue

SEC-06: Conformance to numeric notation best practices

Type	Severity	Location	Status
Conformance to numeric notation best practices (too-many-digits)	Informational	Line: Check on finding	**Acknowledge**

Finding:

❌ TORKPAD.setSwapThreshold(uint256) (TORKPAD.sol:756-759) uses literals with too many digits:
- require(bool,string)(_swapThreshold > totalSupply() / 1000000,SwapThreshold must be greater than 0.0001% of total supply) (TORKPAD.sol#757)

❌ TORKPAD.slitherConstructorVariables() (TORKPAD.sol:609-912) uses literals with too many digits:
- liquidityWallet = 0x000000000000000000000000000000000000dEaD (TORKPAD.sol#615)

Recommendation:

Use:
- [Ether suffix](https://solidity.readthedocs.io/en/latest/units-and-global-variables.html#ether-units),
- [Time suffix](https://solidity.readthedocs.io/en/latest/units-and-global-variables.html#time-units), or
- [The scientific notation](https://solidity.readthedocs.io/en/latest/types.html#rational-and-integer-literals)

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

Alleviation:

TorkPad Team has acknowledge this issue

SWC Findings

ID	Title	Scanning	Result
SWC-100	Function Default Visibility	Complete	No risk
SWC-101	Integer Overflow and Underflow	Complete	No risk
SWC-102	Outdated Compiler Version	Complete	No risk
SWC-103	Floating Pragma	Complete	No risk
SWC-104	Unchecked Call Return Value	Complete	No risk
SWC-105	Unprotected Ether Withdrawal	Complete	No risk
SWC-106	Unprotected SELFDESTRUCT Instruction	Complete	No risk
SWC-107	Reentrancy	Complete	No risk
SWC-108	State Variable Default Visibility	Complete	No risk
SWC-109	Uninitialized Storage Pointer	Complete	No risk
SWC-110	Assert Violation	Complete	No risk
SWC-111	Use of Deprecated Solidity Functions	Complete	No risk
SWC-112	Delegatecall to Untrusted Callee	Complete	No risk

SWC-113	DoS with Failed Call	Complete	No risk
SWC-114	Transaction Order Dependence	Complete	No risk
SWC-115	Authorization through tx.origin	Complete	No risk
SWC-116	Block values as a proxy for time	Complete	No risk
SWC-117	Signature Malleability	Complete	No risk
SWC-118	Incorrect Constructor Name	Complete	No risk
SWC-119	Shadowing State Variables	Complete	No risk
SWC-120	Weak Sources of Randomness from Chain Attributes	Complete	No risk
SWC-121	Missing Protection against Signature Replay Attacks	Complete	No risk
SWC-122	Lack of Proper Signature Verification	Complete	No risk
SWC-123	Requirement Violation	Complete	No risk
SWC-124	Write to Arbitrary Storage Location	Complete	No risk
SWC-125	Incorrect Inheritance Order	Complete	No risk
SWC-126	Insufficient Gas Griefing	Complete	No risk

FULL AUDIT REPORT

SWC-127	Arbitrary Jump with Function Type Variable	Complete	No risk
SWC-128	DoS With Block Gas Limit	Complete	No risk
SWC-129	Typographical Error	Complete	No risk
SWC-130	Right-To-Left-Override control character (U+202E)	Complete	No risk
SWC-131	Presence of unused variables	Complete	No risk
SWC-132	Unexpected Ether balance	Complete	No risk
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Complete	No risk
SWC-134	Message call with hardcoded gas amount	Complete	No risk
SWC-135	Code With No Effects	Complete	No risk
SWC-136	Unencrypted Private Data On-Chain	Complete	No risk

FULL AUDIT REPORT

Visibility, Mutability, Modifier function testing

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	_checkOwner	Internal 🔒		
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	
IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		

FULL AUDIT REPORT

```
| └ | <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❗ |
| └ | _transfer | Internal 🔒 | 🛑 | |
| └ | _mint | Internal 🔒 | 🛑 | |
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _approve | Internal 🔒 | 🛑 | |
| └ | _spendAllowance | Internal 🔒 | 🛑 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfer | Internal 🔒 | 🛑 | |
||||||
| **IDEXRouter** | Interface | ||| |
| └ | factory | External ❗ | |NO❗ |
| └ | WETH | External ❗ | |NO❗ |
| └ | addLiquidityETH | External ❗ | 💵 |NO❗ |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ❗ | 🛑 |NO❗ |
||||||
| **IDEXFactory** | Interface | ||| |
| └ | createPair | External ❗ | 🛑 |NO❗ |
||||||
| **TORKPAD** | Implementation | ERC20, Ownable ||| |
| └ | <Constructor> | Public ❗ | 🛑 | ERC20 |
| └ | setMaxWallet | External ❗ | 🛑 | onlyOwner |
| └ | setTaxWallets | External ❗ | 🛑 | onlyOwner |
| └ | setStakingPools | External ❗ | 🛑 | onlyOwner |
| └ | setLiquidityPair | External ❗ | 🛑 | onlyOwner |
| └ | setWhitelisted | External ❗ | 🛑 | onlyOwner |
| └ | setLiquidityTax | External ❗ | 🛑 | taxUnlocked onlyOwner |
| └ | setMarketingTax | External ❗ | 🛑 | taxUnlocked onlyOwner |
```

FULL AUDIT REPORT

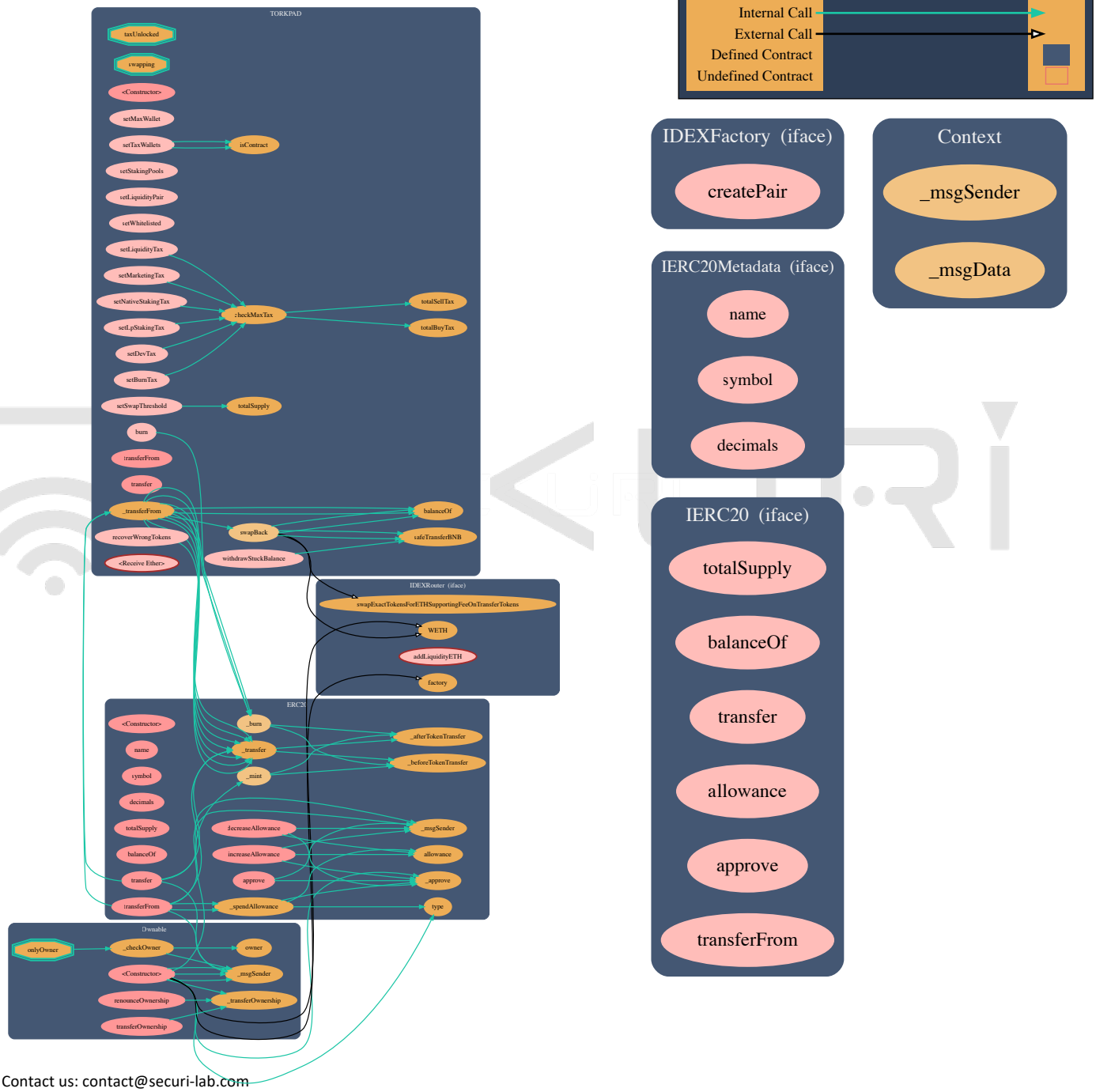
└	setNativeStakingTax	External ❗	🛑	taxUnlocked onlyOwner
└	setLpStakingTax	External ❗	🛑	taxUnlocked onlyOwner
└	setDevTax	External ❗	🛑	taxUnlocked onlyOwner
└	setBurnTax	External ❗	🛑	taxUnlocked onlyOwner
└	setSwapThreshold	External ❗	🛑	onlyOwner
└	totalBuyTax	Internal 🔒		
└	totalSellTax	Internal 🔒		
└	checkMaxTax	Internal 🔒		
└	burn	External ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	transfer	Public ❗	🛑	NO❗
└	swapBack	Internal 🔒	🛑	swapping
└	_transferFrom	Internal 🔒	🛑	
└	isContract	Internal 🔒		
└	withdrawStuckBalance	External ❗	🛑	onlyOwner
└	safeTransferBNB	Internal 🔒	🛑	
└	recoverWrongTokens	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

FULL AUDIT REPORT

Inheritate Function Relation Graph



Contact us: contact@securi-lab.com
Website: https://securi-lab.com
Telegram: https://t.me/securi_lab
Twitter: https://twitter.com/SECURI_LAB

FULL AUDIT REPORT

About Securi

SECURI LAB is a group of cyber security experts providing cyber security consulting, smart contract security audits, and KYC services.

Follow Us On:

Website	https://securi-lab.com/
Twitter	https://twitter.com/SECURI_LAB
Telegram	https://t.me/securi_lab
Medium	https://medium.com/@securi