Full Audit Report

ButcherCoin Security Assessment

Real Cybersecurity
Protecting digital assets

Made in Thailand

SECURI LAB
(THAILAND) contact@securi-lab.com

Table of Contents

Report Information

About Report	**ButcherCoin Security Assessment**
Version	**v1.1**
Client	**ButherCoin**
Language	**Solidity**
Confidentiality	**Public**
Contract Address	**0xC77b13B29c8900B28982Fc596535f89ffb34fa8D**
Audit Method	**Whitebox**
Security Assessment Author	**Auditor** **Mark K. [Security Researcher | Redteam]** **Kevin N. [Security Researcher | Web3 Dev]** **Yusheng T. [Security Researcher | Incident Response]** **Approve Document** **Ronny C. CTO & Head of Security Researcher** **Chinnakit J. CEO & Founder**

*Audit Method

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

Digital Sign (Only Full Audit Report)

Digitally signed by Chinnakit J.
DN: cn=Chinnakit J., o=SECURI LAB (Thailand), ou=CEO & Founder, email=contact@securi-lab.com, c=TH
Date: 2023.05.25 18:41:20 +07'00'

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 Lab** 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 LAB disclaims any liability incurred. Whether it's Rugpull, Abandonment, Soft Rugpull

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

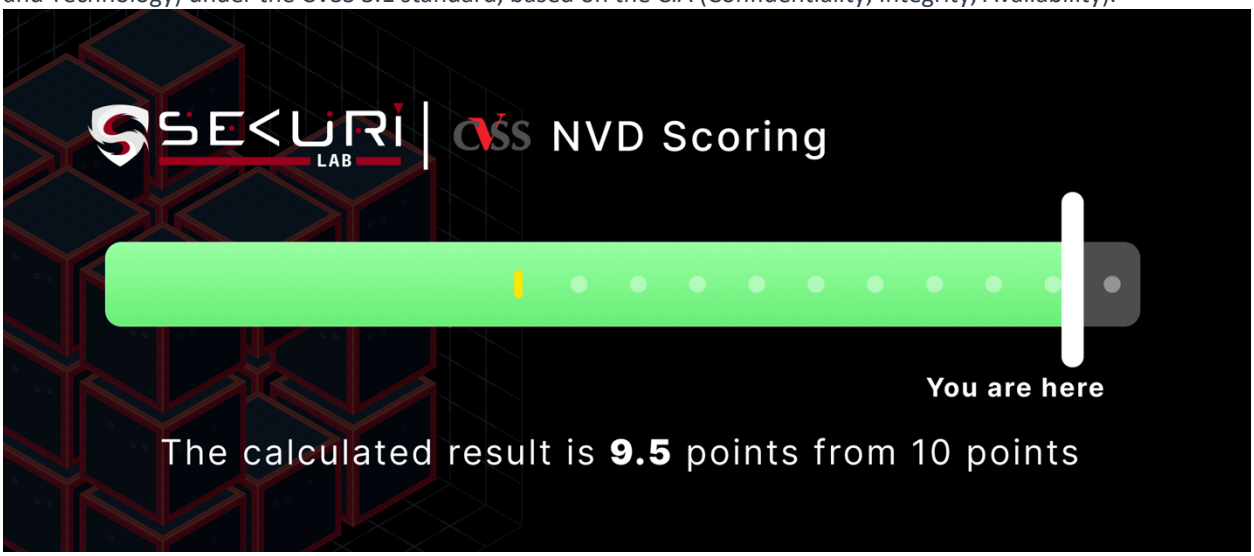
1. Smart Contract Testing with Expert Analysis By testing the most common and uncommon vulnerabilities.
2. Automated program testing It includes a sample vulnerability test and a sample of the potential vulnerabilities being used for the most frequent attacks.
3. Manual Testing with AST/WAS/ASE/SMT and reviewed code line by line
4. 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.
5. Function association test It will be displayed through the association graph.
6. This safety assessment is cross-checked prior to the delivery of the assessment results.

Executive Summary

For this security assessment, SECURI LAB received a request from ButcherCoin on Friday, May 19, 2023.

NVD CVSS Scoring

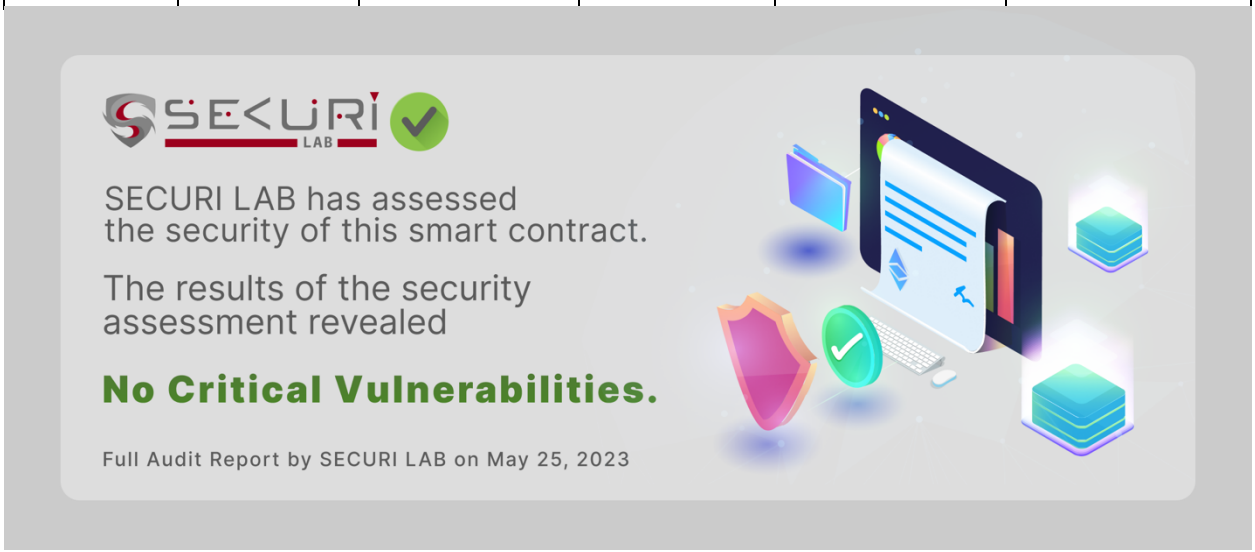
The score was calculated using the NVD (National Vulnerability Database) of NIST (National Institute of Standards and Technology) under the CVSS 3.1 standard, based on the CIA (Confidentiality, Integrity, Availability).



Audit Result

SECURI LAB evaluated the smart contract security of the project and found: [Total : 2]

Critical	High	Medium	Low	Very Low	Informational
0	0	0	0	0	2



FULL AUDIT REPORT

Project Introduction

Scope Information:

Project Name	**ButcherCoin**
Website	**https://butchercoin.xyz/**
Chain	**BNB Chain (Previously Binance Smart Chain)**
Language	**Solidity**

Audit Information:

Request Date	**Friday, May 19, 2023**
Audit Date	**Saturday, May 20, 2023**
Re-assessment Date	**-**

Audit Version History:

Version	Date	Description
1.0	**Sunday, May 21, 2023**	**Preliminary Report**
1.1	**Thursday, May 25, 2023**	**Full Audit Report**

FULL AUDIT REPORT

Initial Audit Scope:

Smart Contract File	0xC77b13B29c8900B28982Fc596535f89ffb34fa8D
Compiler Version	v0.8.18+commit.87f61d96

Source Units Analyzed: `1`
Source Units in Scope: `1` (**100%**)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
📝 🔍 🎨	contracts/BUTCHER.sol	4	2	627	520	197	339	138	🔆Σ
📝 🔍 🎨	**Totals**	**4**	**2**	**627**	**520**	**197**	**339**	**138**	🔆Σ

Legend: [▔]

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Description Report Files Description Table

File NameSHA-1 Hash	File NameSHA-1 Hash
contracts/BUTCHER.sol	contracts/BUTCHER.sol

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

Confidence / Impact [Likelihood]	Low	Medium	High
Low	**Very Low**	**Low**	**Medium**
Medium	**Low**	**Medium**	**High**
High	**Medium**	**High**	**Critical**

Vulnerability Severity Summary

Severity is a risk assessment It is calculated from the Impact and Confidence values using the following calculation methods,

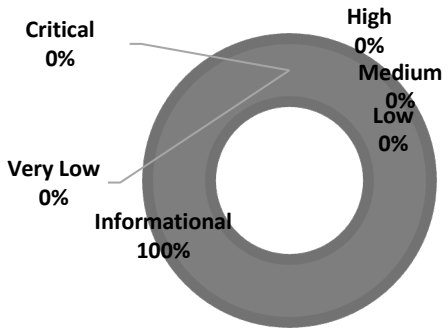
$Risk\ rating\ =\ impact\ *\ confidence$

It is categorized into

5 categories based on the **lowest severity**:

Very Low , Low , Medium , **High** , Critical .

For **Informational** & will **Non-class/Optimization/Best-practices will** not be counted as **severity**



Vulnerability Severity Level	Total
Critical	0
High	0
Medium	0
Low	0
Very Low	0
Informational	2
Non-class/Optimization/Best-practices	3

Category information:

Centralization

Centralization Risk is The risk incurred by a sole proprietor, such as the Owner being able to change something without permission

Economics Risk

Economics Risk is Risks that may affect the economic mechanism system, such as the ability to increase Mint token

Logical Issue

Logical Issue is that can cause errors to core processing, such as any prior operations that cause background processes to crash.

Authorization

Authorization is Possible pitfalls from weak coding allows unrelated people to take any action to modify the values.

Mathematical

Mathematical Any erroneous arithmetic operations affect the operation of the system or lead to erroneous values.

Naming Conventions

Naming Conventions naming variables that may affect code understanding or naming inconsistencies

Security Risk

Security Risk of loss or damage if it's no mitigate

Coding Style

Coding Style is Tips coding for efficiency performance

Best Practices

Best Practices is suggestions for improvement

Optimization

Optimization is performance improvement

Gas Optimization

Gas Optimization is increase performance to avoid expensive gas

Dead Code

Dead Code having unused code This may result in wasted resources and gas fees.

FULL AUDIT REPORT

Vulnerability Findings

ID	Vulnerability Detail	Severity	Category	Status
SEC-01	Conformance to numeric notation best practices (too-many-digits)	Informational	Best Practices	**Acknowledge**
SEC-02	If different pragma directives are used (pragma)	Informational	Best Practices	**Acknowledge**
GAS-01	Use assembly to check for `address(0)`	-	Gas Optimization	**Acknowledge**
GAS-02	Use Custom Errors	-	Gas Optimization	**Acknowledge**
GAS-02	Long revert strings	-	Gas Optimization	**Acknowledge**

SEC-01: Conformance to numeric notation best practices (too-many-digits)

Vulnerability Detail	Severity	Location	Category	Status
Conformance to numeric notation best practices (too-many-digits)	Informational	Check on finding	Best Practices	**Acknowledge**

Finding:

```
❌ BUTCHER.constructor() (BUTCHER.sol:624-626) uses literals with too many digits:
    • _mint(msg.sender,69000000000 * 10 ** decimals()) (BUTCHER.sol#625)
```

Recommendation:

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

Exploit Scenario:

-

Alleviation:

ButcherCoin Team has Acknowledge this issue.

SEC-02: If different pragma directives are used (pragma)

Vulnerability Detail	Severity	Location	Category	Status
If different pragma directives are used (pragma)	Informational	Check on finding	Best Practices	**Acknowledge**

Finding:

```
❌ Different versions of Solidity are used:
    • Version used: ['^0.8.0', '^0.8.9']
    • ^0.8.0 (BUTCHER.sol:3)
    • ^0.8.0 (BUTCHER.sol#30)
    • ^0.8.0 (BUTCHER.sol#115)
    • ^0.8.0 (BUTCHER.sol#200)
    • ^0.8.0 (BUTCHER.sol#230)
    • ^0.8.9 (BUTCHER.sol#619)
```

Recommendation:

Recommendation: Use one Solidity version.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used

Exploit Scenario:

-

Alleviation:

ButcherCoin Team has Acknowledge this issue.

GAS-01: Use assembly to check for `address(0)`

Vulnerability Detail	Severity	Location	Category	Status
Use assembly to check for `address(0)`	-	Check on finding	Gas Optimization	**Acknowledge**

Finding:

```
File: BUTCHER.sol

95:         require(newOwner != address(0), "Ownable: new owner is the zero address");

456:         require(from != address(0), "ERC20: transfer from the zero address");

457:         require(to != address(0), "ERC20: transfer to the zero address");

485:         require(account != address(0), "ERC20: mint to the zero address");

511:         require(account != address(0), "ERC20: burn from the zero address");

546:         require(owner != address(0), "ERC20: approve from the zero address");

547:         require(spender != address(0), "ERC20: approve to the zero address");
```

Recommendation:

-

Alleviation:

ButcherCoin Team has Acknowledge this issue.

GAS-02: Use Custom Errors

Vulnerability Detail	Severity	Location	Category	Status
Use Custom Errors	-	Check on finding	Gas Optimization	**Acknowledge**

Finding:

```
165:     require(c >= a, "SafeMath: addition overflow");

217:     require(c / a == b, "SafeMath: multiplication overflow");

326:     require(_owner == _msgSender(), "Ownable: caller is not the owner");

354:     require(newOwner != address(0), "Ownable: new owner is the zero address");

543:     require(from != address(0), "ERC20: transfer from the zero address");

544:     require(amount > 0, "Transfer amount must be greater than zero");

546:       require(amount <= _maxTxAmount, "Transfer amount exceeds the
maxTxAmount.");

595:     require(account != address(0), "ERC20: burn from the zero address");

616:     require(owner != address(0), "ERC20: approve from the zero address");

617:     require(spender != address(0), "ERC20: approve to the zero address");
```

Recommendation:

[Source](https://blog.soliditylang.org/2021/04/21/custom-errors/)
Instead of using error strings, to reduce deployment and runtime cost, you should use Custom Errors. This would save both deployment and runtime cost.

Alleviation:

ButcherCoin Team has Acknowledge this issue.

GAS-02: Long revert strings

Vulnerability Detail	Severity	Location	Category	Status
Long revert strings	-	Check on finding	Gas Optimization	**Acknowledge**

Finding:

```
File: BUTCHER.sol

95:         require(newOwner != address(0), "Ownable: new owner is the zero address");

429:         require(currentAllowance >= subtractedValue, "ERC20: decreased allowance
below zero");

456:         require(from != address(0), "ERC20: transfer from the zero address");

457:         require(to != address(0), "ERC20: transfer to the zero address");

462:         require(fromBalance >= amount, "ERC20: transfer amount exceeds balance");

511:         require(account != address(0), "ERC20: burn from the zero address");

516:         require(accountBalance >= amount, "ERC20: burn amount exceeds balance");

546:         require(owner != address(0), "ERC20: approve from the zero address");

547:         require(spender != address(0), "ERC20: approve to the zero address");
```

Recommendation:

-

Alleviation:

ButcherCoin 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
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

Visibility, Mutability, Modifier function testing

Components

Contracts	Libraries	Interfaces	Abstract
2	0	2	2

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

Public	Payable
23	0

External	Internal	Private	Pure	View
9	32	0	0	16

StateVariables

Total	Public
6	0

Capabilities

Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
^0.8.0 ^0.8.9				

Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	ECRecover	New/Create/Create2

TryCatch	Σ Unchecked
	yes

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└		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		

FULL AUDIT REPORT

Contract	Type	Bases		
└	name	External !		NO !
└	symbol	External !		NO !
└	decimals	External !		NO !
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└		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 🔒	🛑	

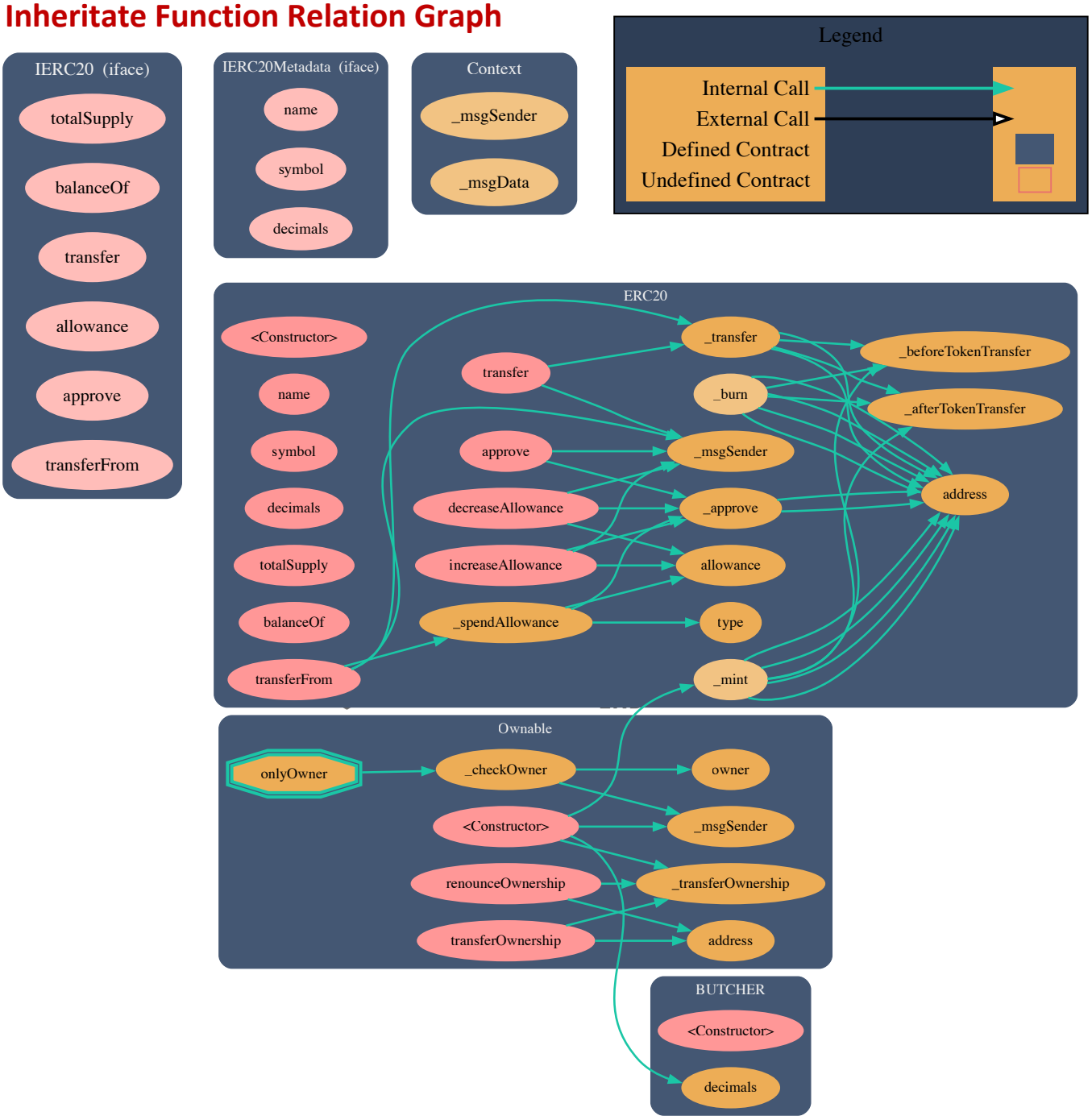
FULL AUDIT REPORT

Contract	Type	Bases		
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
BUTCHER	Implementation	ERC20, Ownable		
└		Public !	🛑	ERC20

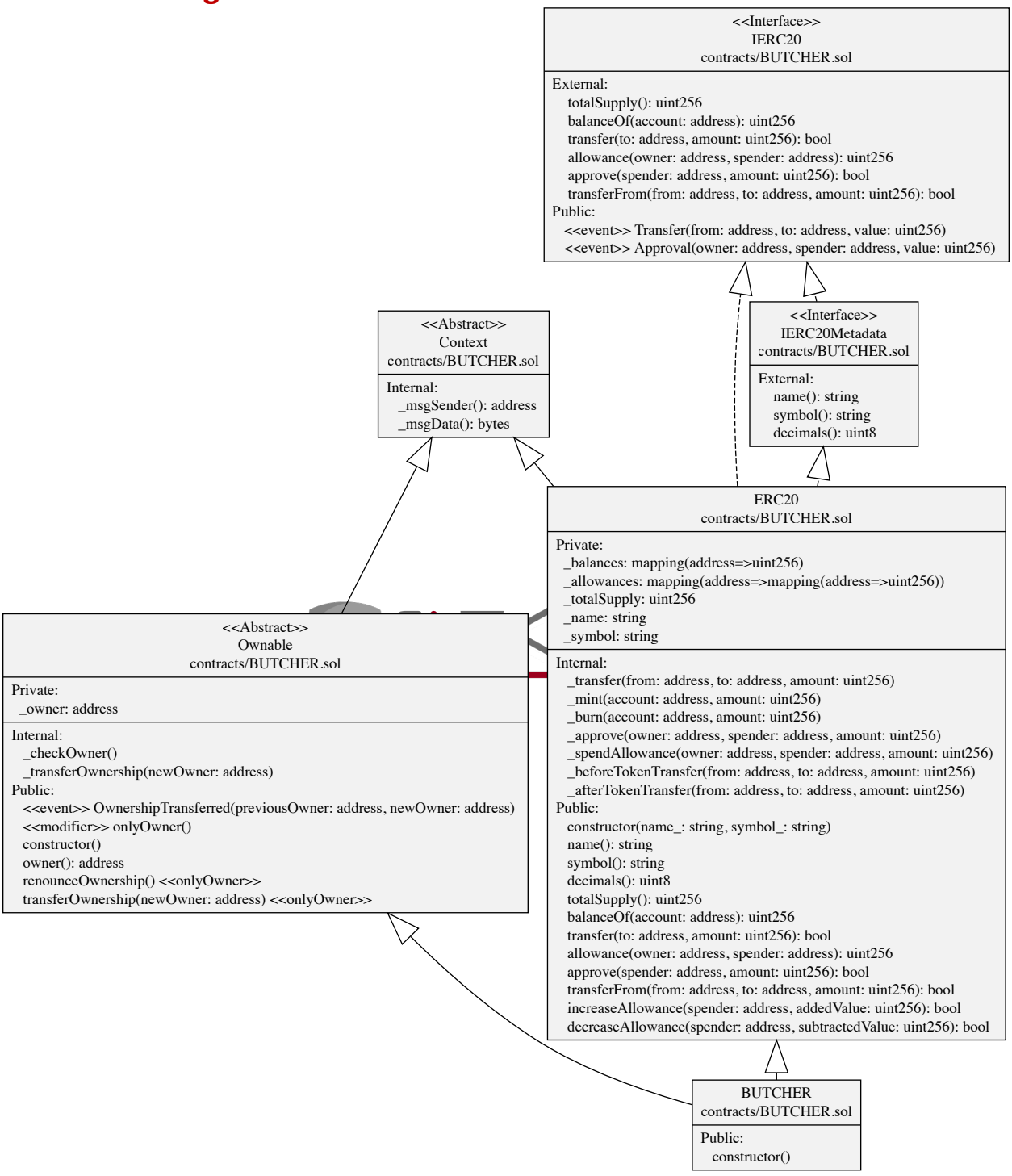
Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Inheritate Function Relation Graph



UML Class Diagram



About SECURI LAB

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