Cybersecurity Audit | KYC | Consultant

Full Audit Report

DogenNft Security Assessment

SECURI LAB 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
SECURI REPORT TEMPLATE VERSION 1.3

FULL AUDIT REPORT

Report Information

About Report	**DogenNft Security Assessment**
Version	**v1.1**
Client	**dogens.io**
Language	**Solidity**
Confidentiality	**Public**
Platform	**Ethereum Chain [ERC-721]**
Contract Address	**0xdd2a0db3e25d0b375ea4457fb80fa4331be0f801**
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)

DocuSigned by:
3164949877D1431...
DS
11/26/2022

Contact US: contact@securi-lab.com
Website: https://securi-lab.com
Telegram: https://t.me/securi_lab
Twitter: https://twitter.com/SECURI_LAB
SECURI REPORT TEMPLATE VERSION 1.3

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 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 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. 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.

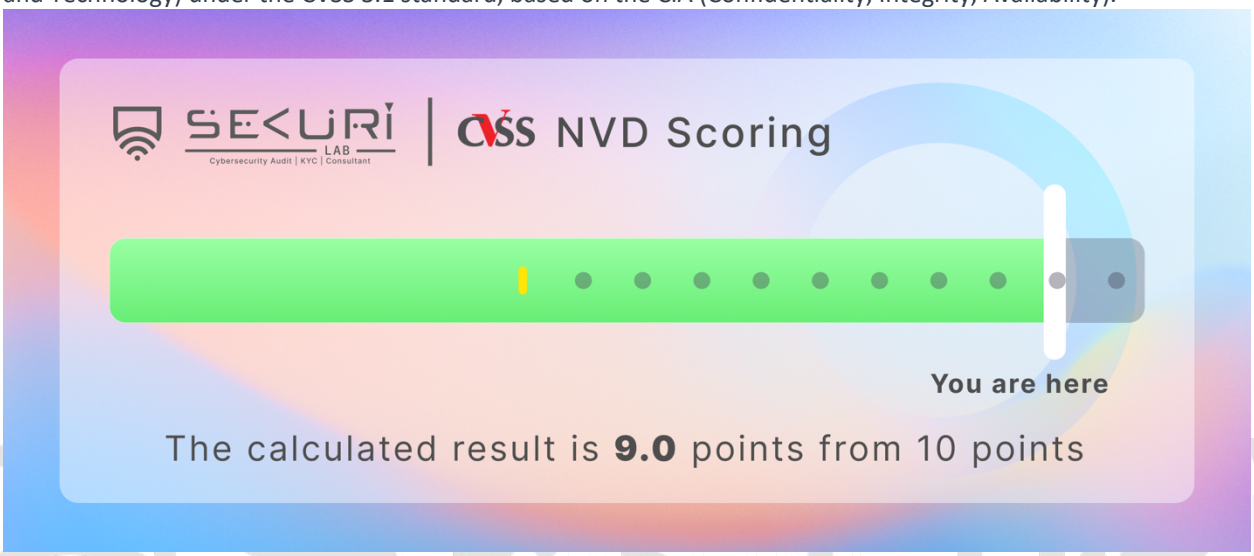
FULL AUDIT REPORT

Executive Summary

For this security assessment, SECURI LAB received a request from dogen.io on Monday, November 21, 2022.

NVD CVSS Scoring

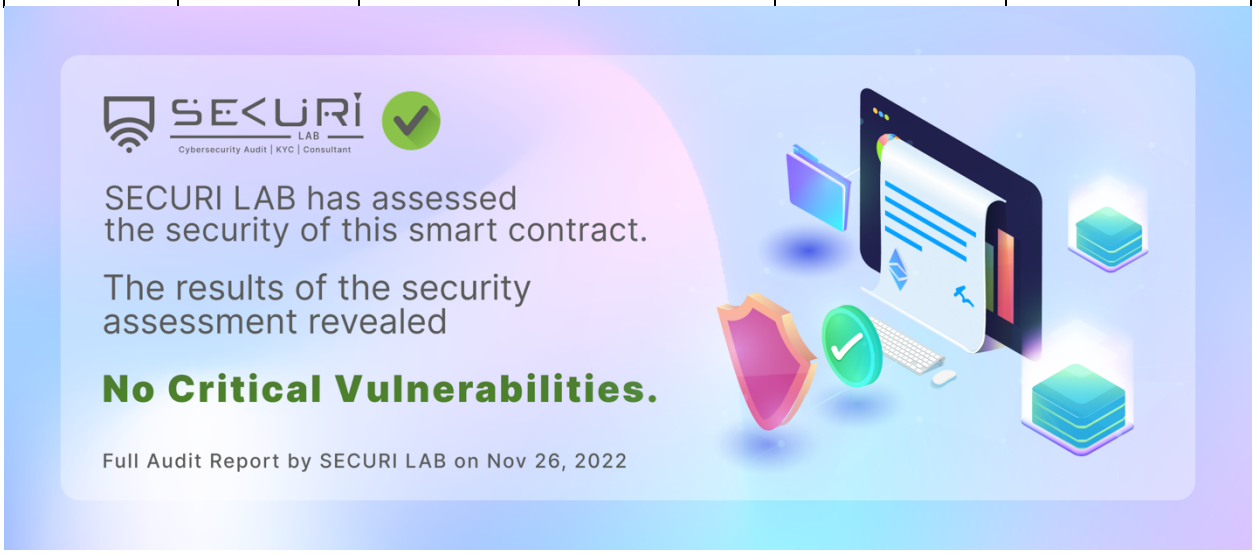
The score was calculated using the NVD (National Vulnerability Database) of NIST (National Institute of Standards and Technology) under the CVSS 3.1 standard, based on the CIA (Confidentiality, Integrity, Availability).



Audit Result

SECURI LAB evaluated the smart contract security of the project and found: [Total : 3 Issues]

Critical	High	Medium	Low	Very Low	Informational
0	0	0	2	0	1



FULL AUDIT REPORT

Project Introduction

Scope Information:

Project Name	Dogens NFT
Website	https://dogens.io/
Chain	Ethereum Chain [ERC-721]
Language	Solidity

Audit Information:

Request Date	Monday, November 21, 2022
Audit Date	Wednesday, November 23, 2022

Audit Version History:

Version	Date	Description
1.0	Wednesday, November 23, 2022	Preliminary Report
1.1	Saturday, November 26, 2022	Full Audit Report

FULL AUDIT REPORT

Initial Audit Scope: Contract: 0xdd2a0db3e25d0b375ea4457fb80fa4331be0f801

Smart Contract	0xdd2a0db3e25d0b375ea4457fb80fa4331be0f801
Contract Name	**DogensNft**
Compiler Version	**v0.8.7+commit.e28d00a7**

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

FULL AUDIT REPORT

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

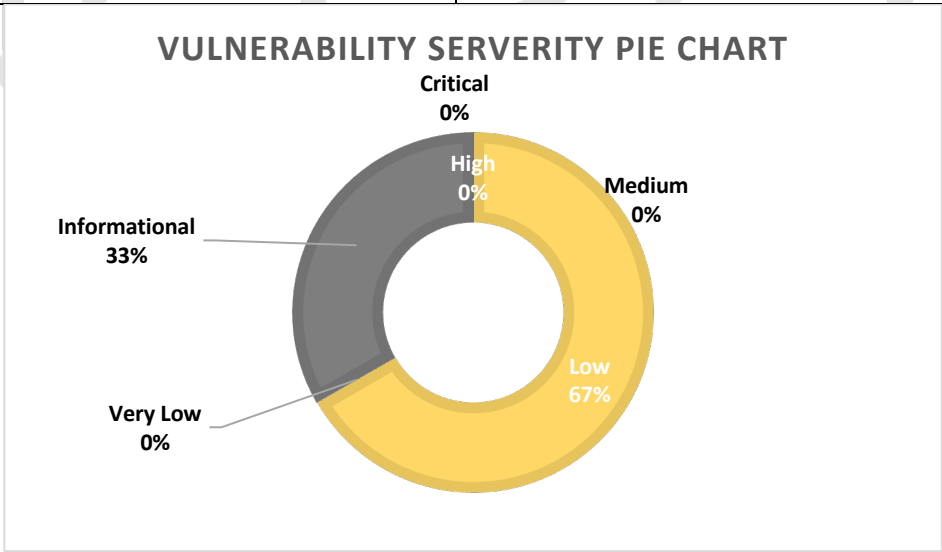
Confidence / Impact	Low	Medium	High
Low	**Very Low**	**Low**	**Medium**
Medium	**Low**	**Medium**	**High**
High	**Medium**	**High**	**Critical**

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	2
Very Low	0
Informational (Non severity level)	1



FULL AUDIT REPORT

Vulnerability Findings

ID	Title	Severity	Status
SEC-01	Missing Events Arithmetic (events-maths)	LOW	**Acknowledge**
SEC-02	Missing Zero Address Validation (missing-zero-check)	LOW	**Acknowledge**
SEC-03	If different pragma directives are used (pragma)	informational	**Acknowledge**

FULL AUDIT REPORT

SEC-01: Missing Events Arithmetic (events-maths)

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

Finding:

❌ DogensNft.setMintRate(uint256) (DogensNft.sol:1941-1943) should emit an event for:
- mintRate = _mintRate (DogensNft.sol#1942)

Recommendation:

Recommendation: Emit an event for critical parameter changes.

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

Alleviation:

DogenNft Team has **Acknowledge** this issue.

FULL AUDIT REPORT

SEC-02: Missing Zero Address Validation (missing-zero-check)

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

Finding:

❌ DogensNft.setRoyaltyAddress(address)._address (DogensNft.sol:1946) lacks a zero-check on :

- royaltyAddress = _address (DogensNft.sol#1947)

Recommendation:

Check that the address is not zero.

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

Alleviation:

DogenNft Team has **Acknowledge** this issue.

FULL AUDIT REPORT

SEC-03: If different pragma directives are used (pragma)

Type	Severity	Location	Status
If different pragma directives are used (pragma)	Informational	Line: check on finding	**Acknowledge**

Finding:

❌ Different versions of Solidity are used:
- Version used: ['^0.8.0', '^0.8.4']
- ^0.8.0 (DogensNft.sol:21)
- ^0.8.0 (DogensNft.sol#99)
- ^0.8.0 (DogensNft.sol#319)
- ^0.8.0 (DogensNft.sol#346)
- ^0.8.4 (DogensNft.sol#432)
- ^0.8.4 (DogensNft.sol#717)
- ^0.8.4 (DogensNft.sol#1806)

Recommendation:

Use one Solidity version.

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

Alleviation:

DogenNft Team has **Acknowledge** this issue.

FULL AUDIT REPORT

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

FULL AUDIT REPORT

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

FULL AUDIT REPORT

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

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Strings	Library			
└	toString	Internal 🔒		
└	toHexString	Internal 🔒		
└	toHexString	Internal 🔒		
└	toHexString	Internal 🔒		
ECDSA	Library			
└	_throwError	Private 🔐		
└	tryRecover	Internal 🔒		
└	recover	Internal 🔒		
└	tryRecover	Internal 🔒		
└	recover	Internal 🔒		
└	tryRecover	Internal 🔒		
└	recover	Internal 🔒		
└	toEthSignedMessageHash	Internal 🔒		
└	toEthSignedMessageHash	Internal 🔒		
└	toTypedDataHash	Internal 🔒		
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 🔒	🛑	

FULL AUDIT REPORT

IERC721A	Interface			
└	totalSupply	External ❗		NO❗
└	supportsInterface	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	ownerOf	External ❗		NO❗
└	safeTransferFrom	External ❗	💸	NO❗
└	safeTransferFrom	External ❗	💸	NO❗
└	transferFrom	External ❗	💸	NO❗
└	approve	External ❗	💸	NO❗
└	setApprovalForAll	External ❗	🛑	NO❗
└	getApproved	External ❗		NO❗
└	isApprovedForAll	External ❗		NO❗
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	tokenURI	External ❗		NO❗
ERC721A__IERC721Receiver	Interface			
└	onERC721Received	External ❗	🛑	NO❗
ERC721A	Implementation	IERC721A		
└	<Constructor>	Public ❗	🛑	NO❗
└	_startTokenId	Internal 🔒		
└	_nextTokenId	Internal 🔒		
└	totalSupply	Public ❗		NO❗
└	_totalMinted	Internal 🔒		
└	_totalBurned	Internal 🔒		
└	balanceOf	Public ❗		NO❗
└	_numberMinted	Internal 🔒		
└	_numberBurned	Internal 🔒		
└	_getAux	Internal 🔒		
└	_setAux	Internal 🔒	🛑	
└	supportsInterface	Public ❗		NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	tokenURI	Public ❗		NO❗
└	_baseURI	Internal 🔒		
└	ownerOf	Public ❗		NO❗
└	_ownershipOf	Internal 🔒		
└	_ownershipAt	Internal 🔒		
└	_initializeOwnershipAt	Internal 🔒	🛑	
└	_packedOwnershipOf	Private 🔐		

FULL AUDIT REPORT

```
| └ | _unpackedOwnership | Private 🔐 |  | |
| └ | _packOwnershipData | Private 🔐 |  | |
| └ | _nextInitializedFlag | Private 🔐 |  | |
| └ | approve | Public ❗ | 💵 |NO❗ |
| └ | getApproved | Public ❗ |  |NO❗ |
| └ | setApprovalForAll | Public ❗ | 🛑 |NO❗ |
| └ | isApprovedForAll | Public ❗ |  |NO❗ |
| └ | _exists | Internal 🔒 |  | |
| └ | _isSenderApprovedOrOwner | Private 🔐 |  | |
| └ | _getApprovedSlotAndAddress | Private 🔐 |  | |
| └ | transferFrom | Public ❗ | 💵 |NO❗ |
| └ | safeTransferFrom | Public ❗ | 💵 |NO❗ |
| └ | safeTransferFrom | Public ❗ | 💵 |NO❗ |
| └ | _beforeTokenTransfers | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfers | Internal 🔒 | 🛑 | |
| └ | _checkContractOnERC721Received | Private 🔐 | 🛑 | |
| └ | _mint | Internal 🔒 | 🛑 | |
| └ | _mintERC2309 | Internal 🔒 | 🛑 | |
| └ | _safeMint | Internal 🔒 | 🛑 | |
| └ | _safeMint | Internal 🔒 | 🛑 | |
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _setExtraDataAt | Internal 🔒 | 🛑 | |
| └ | _extraData | Internal 🔒 |  | |
| └ | _nextExtraData | Private 🔐 |  | |
| └ | _msgSenderERC721A | Internal 🔒 |  | |
| └ | _toString | Internal 🔒 |  | |
||||||
| **DogensNft** | Implementation | ERC721A, Ownable |||
| └ | <Constructor> | Public ❗ | 🛑 | ERC721A |
| └ | _startTokenId | Internal 🔒 |  | |
| └ | TotalBurned | Public ❗ |  |NO❗ |
| └ | next | Public ❗ |  |NO❗ |
| └ | toggleSale | Public ❗ | 🛑 | onlyOwner |
| └ | getSigner | Internal 🔒 |  | |
| └ | mint | External ❗ | 💵 |NO❗ |
| └ | mintbyref | External ❗ | 💵 |NO❗ |
| └ | vipmint | External ❗ | 🛑 | onlyOwner |
| └ | withdraw | External ❗ | 💵 | onlyOwner |
| └ | _baseURI | Internal 🔒 |  | |
| └ | setMintRate | Public ❗ | 🛑 | onlyOwner |
```

FULL AUDIT REPORT

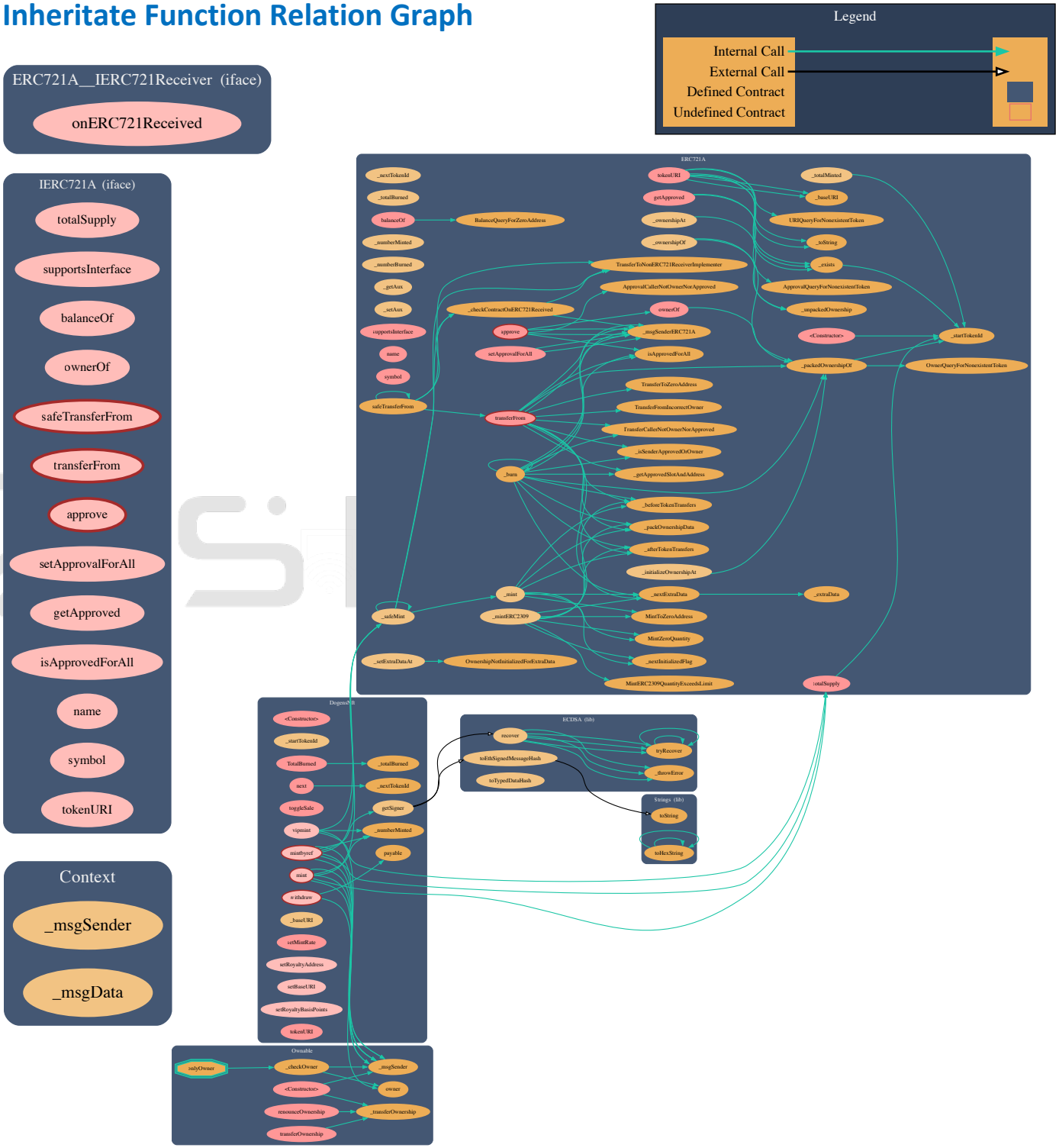
└	setRoyaltyAddress	External ❗	🛑	onlyOwner
└	setBaseURI	External ❗	🛑	onlyOwner
└	setRoyaltyBasisPoints	External ❗	🛑	onlyOwner
└	tokenURI	Public ❗		NO❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

FULL AUDIT REPORT

Inheritate Function Relation Graph



FULL AUDIT REPORT

About Securi

SECURI LAB is a group of cyber security experts Founded in 2018, we are security researchers with more than 3 years of expertise and we started out as a consultant to organizations on cybersecurity. We use highly reliable and industry-leading inspection tools.

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