Full Audit Report

Dogens NFT Staking + Vaults Security Assessment

SECURI LAB contact@securi-lab.com

FULL AUDIT REPORT

Table of Contents 1

Report Information 2-4

Disclaimer 5

Executive Summary 6

NVD CVSS Scoring

Audit Result

Project Introduction 7

Scope Information

Audit Information

Audit Version History

Initial Audit Scope 8

Security Assessment Procedure 9

Risk Rating 10

Vulnerability Severity Summary 11

Vulnerability Findings 12-17

SWC & SEC-01 to SEC-06

SWC FIndings 18-20

Visibility, Mutability, Modifier function testing 21-32

Component, Exposed Function

StateVariables, Capabilities, Contract Descripton Table

Inheritate Function Relation Graph 33-34

UML Diagram 35

About Securi 36

FULL AUDIT REPORT

Report Information

About Report	**Dogens NFT Staking + Vaults Security Assessment**
Version	**v1.5**
Client	**Dogens**
Language	**Solidity**
Confidentiality	**Public**
Contract File	

File Name	SHA-1 Hash
contracts/NFTV2.sol	964925140a53623c5727d4ea3246999de6934e61
contracts/IERC721A.sol	703e12ae3faac00128eace0454105d223f7233b3
contracts/IERC721AQueryable.sol	a3b963c4d8834e5992a0aa779f3b595de9a4853d
contracts/ERC721A.sol	ba727c16ac96cd55ebfdab4b9b411a0f0568278d
contracts/nftvault.sol	645a9418e7e4f0e463a36edf32db3e2461ca3642
contracts/ERC721AQueryable.sol	3907d3371961838326f51dda0d90e7869b53b2e3
contracts/IERC20.sol	5f937d9a8009770f12b8d4c395a2bd55578f67e5

Audit Method	**Whitebox**

FULL AUDIT REPORT

Source Units in Scope
Source Units Analyzed: **7**
Source Units in Scope: **7** (**100%**)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/NFTV2.sol	1	1	413	397	307	31	285	
	contracts/IERC721A.sol		1	282	136	57	190	41	
	contracts/IERC721AQueryable.sol		1	79	54	17	59	11	
	contracts/ERC721A.sol	1	1	1123	1048	397	549	444	Σ
	contracts/nftvault.sol	1		237	237	200	6	238	
	contracts/ERC721AQueryable.sol	1		178	168	95	67	101	Σ
	contracts/IERC20.sol		1	84	38	16	58	15	

FULL AUDIT REPORT

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	Totals	4	5	2396	2078	1089	960	1135	Σ

- **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, ...)

*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: 2023.01.18 18:54:43 +07'00'

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.

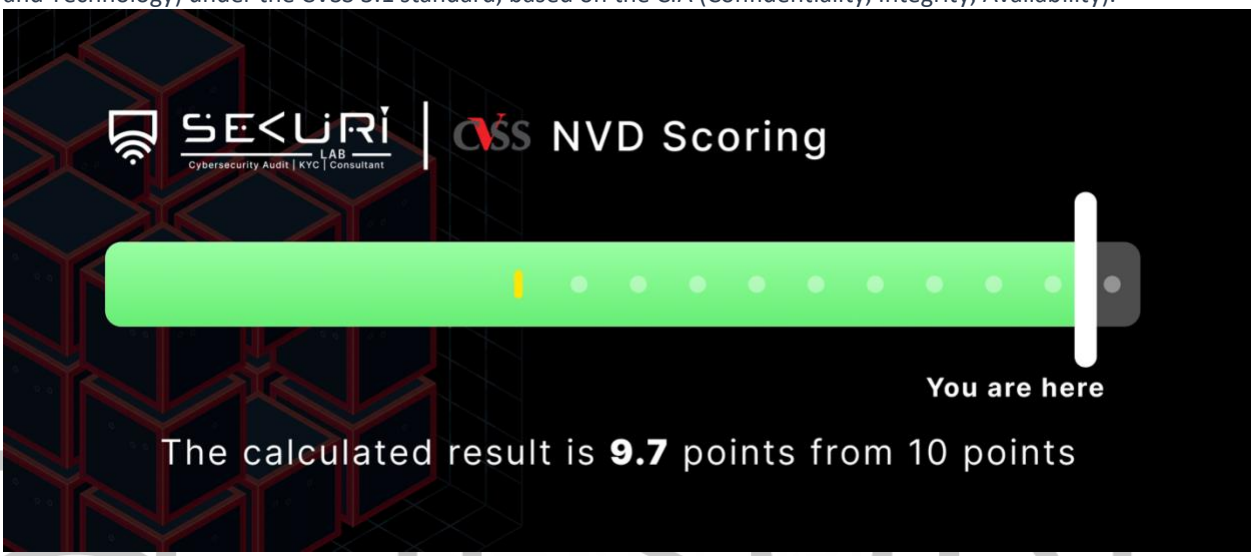
FULL AUDIT REPORT

Executive Summary

For this security assessment, SECURI LAB received a request from Dogens on Thursday, January 5, 2023.

NVD CVSS Scoring

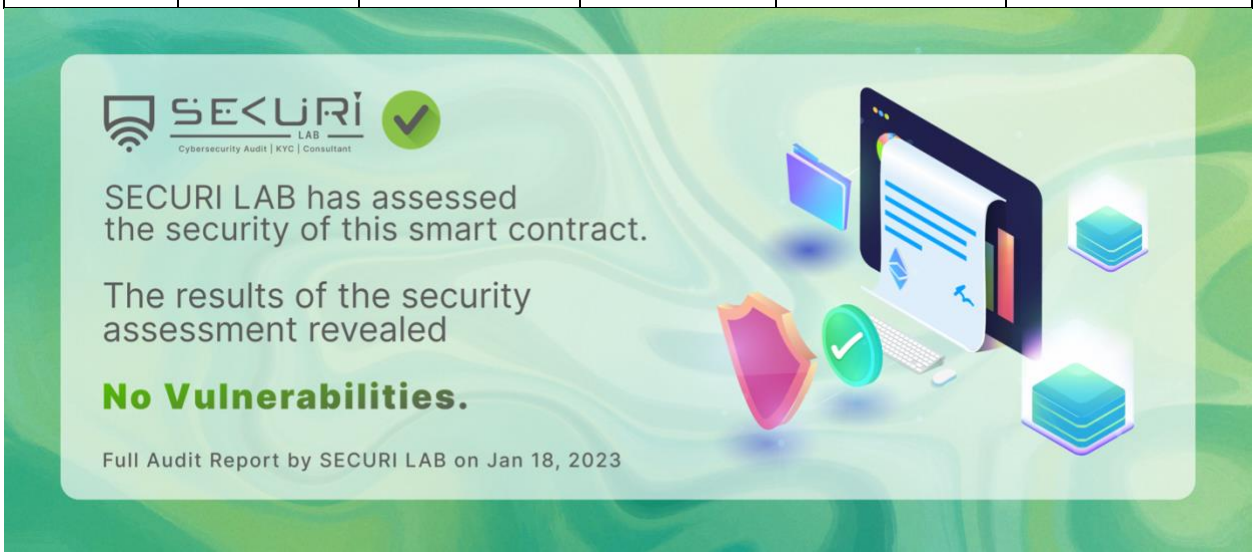
The score was calculated using the NVD (National Vulnerability Database) of NIST (National Institute of Standards and Technology) under the CVSS 3.1 standard, based on the CIA (Confidentiality, Integrity, Availability).



Audit Result

SECURI LAB evaluated the smart contract security of the project and found: **[Total : 5 Issues All issues has already resolved]**

Critical	High	Medium	Low	Very Low	Informational
0	1[Resolved]	0	2[Resolved]	0	2[Resolved]



FULL AUDIT REPORT

Project Introduction

Scope Information:

Project Name	**Dogens**
Website	**https://dogens.io/**
Chain	**Ethereum Chain**
Language	**Solidity**

Audit Information:

Request Date	**Thursday, January 5, 2023**
Audit Date	**Friday, January 13, 2023**
Re-assessment Date	**Wednesday, January 18, 2023**

Audit Version History:

Version	Date	Description
1.0	**Monday, October 24, 2022**	**Preliminary Report[Dogens NFT]** 0xdd2a0db3e25d0b375ea4457fb80fa4331be0f801
1.1	**Monday, October 24, 2022**	**Full Audit Report[Dogens NFT]** 0xdd2a0db3e25d0b375ea4457fb80fa4331be0f801
1.2	**Monday, December 19, 2022**	**Preliminary Report [Dogens]** 0x1b4dD5eA240732dDAc8d74FD1Cd9026Addc02e3c
1.3	**Tuesday, December 20, 2022**	**Full Audit Report [Dogens]** 0x1b4dD5eA240732dDAc8d74FD1Cd9026Addc02e3c
1.4	**Friday, January 13, 2023**	**Preliminary Report [Dogens NFT Staking + Vaults]**
1.5	**Wednesday, January 18, 2023**	**Full Audit Report with reassessment [Dogens NFT Staking + Vaults]**

FULL AUDIT REPORT

Initial Audit Scope:

Files

File Name	SHA-1 Hash
contracts/NFTV2.sol	964925140a53623c5727d4ea3246999de6934e61
contracts/IERC721A.sol	703e12ae3faac00128eace0454105d223f7233b3
contracts/IERC721AQueryable.sol	a3b963c4d8834e5992a0aa779f3b595de9a4853d
contracts/ERC721A.sol	ba727c16ac96cd55ebfdab4b9b411a0f0568278d
contracts/nftvault.sol	645a9418e7e4f0e463a36edf32db3e2461ca3642
contracts/ERC721AQueryable.sol	3907d3371961838326f51dda0d90e7869b53b2e3
contracts/IERC20.sol	5f937d9a8009770f12b8d4c395a2bd55578f67e5

Compiler Version **v0.8.4**

Re-assessment Audit Scope:

Smart Contract

NFTv2

https://etherscan.io/address/0x6c1cd8aa73722b64ed7e20ee357f0a42b09a9185#readContract

Vaults

https://etherscan.io/address/0x00c7b9dbd47742bc1c57690255624ba7b173cc16#code

Compiler Version **v0.8.4**

For previously Dogens audit report please check it on
https://securi-lab.com/our-case/dogen-nft/

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

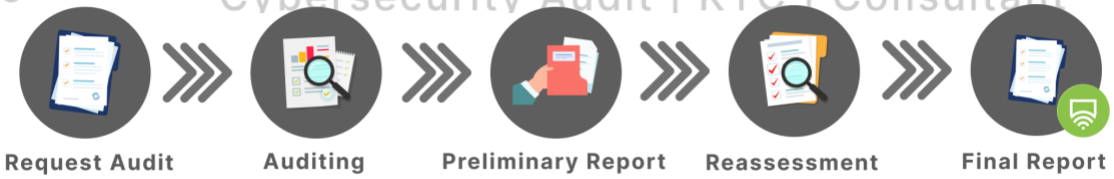
2.Auditing Securi performs security assessments of smart contracts obtained through automated analysis and expert manual audits.

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

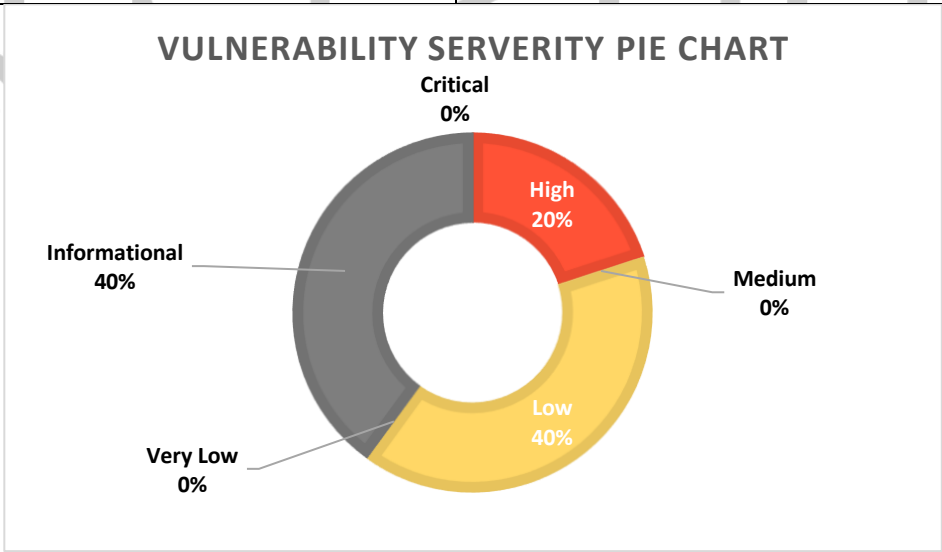
Confidence Impact	Low	Medium	High
Low	**Very Low**	**Low**	**Medium**
Medium	**Low**	**Medium**	**High**
High	**Medium**	**High**	**Critical**

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	1[Resolved]
Medium	0
Low	2[Resolved]
Very Low	0
Informational (Non severity level)	2[Resolved]



FULL AUDIT REPORT

Vulnerability Findings

ID	Title	Severity	Status
SEC-01	Uninitialized state variables (uninitialized-state)	High	**Resolved**
SEC-02	Missing Events Arithmetic (events-maths)	LOW	**Resolved**
SEC-03	Missing Zero Address Validation (missing-zero-check)	LOW	**Resolved**
SEC-04	Conformity to Solidity naming conventions (naming-convention)	Informational	**Resolved**
SEC-05	Costly operations in a loop (costly-loop)	Informational	**Resolved**

FULL AUDIT REPORT

SEC-01: Uninitialized state variables (uninitialized-state)

Type	Severity	Location	Status
Uninitialized state variables (uninitialized-state)	High	Check on finding	**Resolved**

Finding:

❌ NFT_v2.isEliminated (NFTV2.sol:41) is never initialized. It is used in:

- NFT_v2.handleClaim(uint256) (NFTV2.sol#276-301)
- NFT_v2.getUnclaimedAmount(uint256) (NFTV2.sol#303-322)

Recommendation:

Initialize all the variables. If a variable is meant to be initialized to zero, explicitly set it to zero to improve code readability.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-state-variables

Alleviation:

Dogens team has already resolved this issue

FULL AUDIT REPORT

SEC-02: Missing Events Arithmetic (events-maths)

Type	Severity	Location	Status
Missing Events Arithmetic (events-maths)	LOW	Check on finding	**Resolved**

Finding:

❌ NFT_v2.changeMaxMintPerWallet(uint256) (NFTV2.sol:200-202) should emit an event for:
- MAX_MINTS = _max_mint_amount (NFTV2.sol#201)

❌ NFT_v2.changeMaxSupply(uint256) (NFTV2.sol:205-208) should emit an event for:
- MAX_SUPPLY = _newSupply (NFTV2.sol#207)

❌ NFT_v2.claim(uint256,address) (NFTV2.sol:251-274) has external calls inside a loop: (userBalance,canClaim) = vault.userInfo(_msgSender()) (NFTV2.sol#255)

❌ NFT_v2.setMinErcHolding(uint256) (NFTV2.sol:386-390) should emit an event for:
- min_erc_holding = totalAmount (NFTV2.sol#389)

❌ NFT_v2.setMintRate(uint256) (NFTV2.sol:179-181) should emit an event for:
- mintRate = _mintRate (NFTV2.sol#180)

Recommendation:

Emit an event for critical parameter changes.

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

Alleviation:

Dogens team has already resolved this issue

FULL AUDIT REPORT

SEC-03: Missing Zero Address Validation (missing-zero-check)

Type	Severity	Location	Status
Missing Zero Address Validation (missing-zero-check)	LOW	Check on finding	**Resolved**

Finding:

❌ NFT_v2.constructor(address,address).treasure (NFTV2.sol:66) lacks a zero-check on :
- treasureAddress = treasure (NFTV2.sol#68)

❌ NFT_v2.setRoyaltyAddress(address)._address (NFTV2.sol:184) lacks a zero-check on :
- royaltyAddress = _address (NFTV2.sol#185)

❌ NFT_v2.setTreasureAddress(address)._newTreasure (NFTV2.sol:396) lacks a zero-check on :
- treasureAddress = _newTreasure (NFTV2.sol#397)

Recommendation:

Check that the address is not zero.

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

Alleviation:

Dogens team has already resolved this issue

FULL AUDIT REPORT

SEC-04: Missing Zero Address Validation (missing-zero-check)

Type	Severity	Location	Status
Conformity to Solidity naming conventions (naming-convention)	Informational	Check on finding	**Resolved**

Finding:

❌ Contract NFT_v2 (NFTV2.sol:14-413) is not in CapWords
❌ Function NFT_v2.TotalBurned() (NFTV2.sol:78-81) is not in mixedCase
❌ Low level call in NFT_v2._transferEth(address,uint256) (NFTV2.sol:407-410):
- (transferSuccess) = address(to).call{value: amount}() (NFTV2.sol#408)

❌ Low level call in NFT_v2.emergencyWithdraw() (NFTV2.sol:170-173):
- (success) = address(owner()).call{value: address(this).balance}() (NFTV2.sol#171)

❌ Low level call in NftVault.withdraw() (nftvault.sol:165-168):
- (success) = address(owner()).call{value: address(this).balance}() (nftvault.sol#166)

Recommendation:

Follow the Solidity [naming convention](https://solidity.readthedocs.io/en/v0.4.25/style-guide.html#naming-conventions).

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Alleviation:

Dogens team has already resolved this issue

SEC-05: Costly operations in a loop (costly-loop)

Type	Severity	Location	Status
Costly operations in a loop (costly-loop)	Informational	Check on finding	**Resolved**

Finding:

❌ NFT_v2.claim(uint256,address) (NFTV2.sol:251-274) has costly operations inside a loop:
- totalEthClaimed += totalEthReward (NFTV2.sol#266)

❌ NFT_v2.claim(uint256,address) (NFTV2.sol:251-274) has costly operations inside a loop:
- totalTokenClaimed += totalTokenReward (NFTV2.sol#270)

❌ NftVault.claimAll() (nftvault.sol:56-70) has costly operations inside a loop:
- delete receiver[token] (nftvault.sol#64)

❌ NftVault.claimExactToken(uint256) (nftvault.sol:72-86) has costly operations inside a loop:
- delete receiver[token] (nftvault.sol#82)

Recommendation:

Use a local variable to hold the loop computation result.

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop

Alleviation:

Dogens team has already resolved 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

FULL AUDIT REPORT

Visibility, Mutability, Modifier function testing

Components

Contracts	Libraries	Interfaces	Abstract
3	0	5	1

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
98	17

External	Internal	Private	Pure	View
65	95	8	8	58

StateVariables

Total	Public
58	32

Capabilities

Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
`^0.8.4` `^0.8.0`		`yes`	`yes` (12 asm blocks)	

FULL AUDIT REPORT

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

TryCatch	Σ Unchecked
yes	yes

Dependencies / External Imports

Dependency / Import Path	Count
@openzeppelin/contracts/access/Ownable.sol	2
@openzeppelin/contracts/security/ReentrancyGuard.sol	2
@openzeppelin/contracts/utils/Context.sol	1
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	1

FULL AUDIT REPORT

Contracts Description Table

Contract	Type	Bases		
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
IVault	Interface			
L	userInfo	External !		NO!
NFT_v2	Implementation	ERC721A, ERC721AQueryable, Ownable, ReentrancyGuard		
L		Public !		ERC721A
L	_startTokenId	Internal		
L	TotalBurned	Public !		NO!
L	next	Public !		NO!
L	toggleSale	Public !		onlyOwner
L	getSigner	Internal		
L	mint	External !		NO!
L	mintbyref	External !		NO!
L	giftmint	External !		onlyOwner
L	emergencyWithdraw	External !		onlyOwner
L	_baseURI	Internal		

FULL AUDIT REPORT

Contract	Type	Bases		
L	setMintRate	Public !	●	onlyOwner
L	setRoyaltyAddress	External !	●	onlyOwner
L	setBaseURI	External !	●	onlyOwner
L	setRoyaltyBasisPoints	External !	●	onlyOwner
L	changeMaxMintPerWallet	External !	●	onlyOwner
L	changeMaxSupply	External !	●	onlyOwner
L	tokenURI	Public !		NO!
L	claimRewards	Public !	●	nonReentrant
L	batchClaimRewards	Public !	●	NO!
L	claimAndDepositReward	Public !	●	nonReentrant
L	batchClaimAndDepositRewards	Public !	●	NO!
L	claim	Internal 🔒	●	
L	handleClaim	Internal 🔒	●	
L	getUnclaimedAmount	Public !		NO!
L	batchGetUnclaimedAmount	Public !		NO!
L	depositRewardToken	External !	●	onlyOwner

FULL AUDIT REPORT

Contract	Type	Bases		
L	depositRewardEth	External !		onlyOwner
L	cancelRound	External !		onlyOwner
L	toggleClaim	Public !		onlyOwner
L	setRewardToken	External !		onlyOwner
L	setVault	External !		onlyOwner
L	setMinErcHolding	External !		onlyOwner
L	flipExemptionStatus	External !		onlyOwner
L	setTreasureAddress	External !		onlyOwner
L	setMaxTokenId	External !		onlyOwner
L	_transferEth	Internal		
L		External !		NO!
IERC721A	Interface			
L	totalSupply	External !		NO!
L	supportsInterface	External !		NO!
L	balanceOf	External !		NO!
L	ownerOf	External !		NO!
L	safeTransferFrom	External !		NO!

FULL AUDIT REPORT

Contract	Type	Bases		
L	safeTransferFrom	External		NO
L	transferFrom	External		NO
L	approve	External		NO
L	setApprovalForAll	External		NO
L	getApproved	External		NO
L	isApprovedForAll	External		NO
L	name	External		NO
L	symbol	External		NO
L	tokenURI	External		NO
IERC721AQueryable	Interface	IERC721A		
L	explicitOwnershipOf	External		NO
L	explicitOwnershipsOf	External		NO
L	tokensOfOwnerIn	External		NO
L	tokensOfOwner	External		NO
ERC721A__IERC721Receiver	Interface			
L	onERC721Received	External		NO
ERC721A	Implementation	IERC721A		
L		Public		NO
L	_startTokenId	Internal		

FULL AUDIT REPORT

Contract	Type	Bases		
L	_nextTokenId	Internal 🔒		
L	totalSupply	Public ❗		NO❗
L	_totalMinted	Internal 🔒		
L	_totalBurned	Internal 🔒		
L	balanceOf	Public ❗		NO❗
L	_numberMinted	Internal 🔒		
L	_numberBurned	Internal 🔒		
L	_getAux	Internal 🔒		
L	_setAux	Internal 🔒	🛑	
L	supportsInterface	Public ❗		NO❗
L	name	Public ❗		NO❗
L	symbol	Public ❗		NO❗
L	tokenURI	Public ❗		NO❗
L	_baseURI	Internal 🔒		
L	ownerOf	Public ❗		NO❗
L	_ownershipOf	Internal 🔒		
L	_ownershipAt	Internal 🔒		
L	_initializeOwnershipAt	Internal 🔒	🛑	
L	_packedOwnershipOf	Private 🔐		
L	_unpackedOwnership	Private 🔐		
L	_packOwnershipData	Private 🔐		
L	_nextInitializedFlag	Private 🔐		

FULL AUDIT REPORT

Contract	Type	Bases		
L	approve	Public !		NO!
L	getApproved	Public !		NO!
L	setApprovalForAll	Public !		NO!
L	isApprovedForAll	Public !		NO!
L	_exists	Internal		
L	_isSenderApprovedOrOwner	Private		
L	_getApprovedSlotAndAddress	Private		
L	transferFrom	Public !		NO!
L	safeTransferFrom	Public !		NO!
L	safeTransferFrom	Public !		NO!
L	_beforeTokenTransfers	Internal		
L	_afterTokenTransfers	Internal		
L	_checkContractOnERC721Received	Private		
L	_mint	Internal		
L	_mintERC2309	Internal		
L	_safeMint	Internal		
L	_safeMint	Internal		
L	_approve	Internal		
L	_approve	Internal		
L	_burn	Internal		

FULL AUDIT REPORT

Contract	Type	Bases		
L	_burn	Internal 🔒	🛑	
L	_setExtraDataAt	Internal 🔒	🛑	
L	_extraData	Internal 🔒		
L	_nextExtraData	Private 🔐		
L	_msgSenderERC721A	Internal 🔒		
L	_toString	Internal 🔒		
NftVault	Implementation	Ownable, ReentrancyGuard		
L	airDrop	External ❗	🛑	onlyOwner
L	distributeTokens	External ❗	🛑	onlyOwner
L	claimAll	Public ❗	💵	nonReentrant
L	claimExactToken	Public ❗	💵	nonReentrant
L	getClaimAllFee	Public ❗		NO❗
L	lock	Public ❗	🛑	nonReentrant
L	unlock	Public ❗	🛑	nonReentrant
L	userInfo	External ❗		NO❗
L	setMinDayOfMonthCanUnlock	External ❗	🛑	onlyOwner

FULL AUDIT REPORT

Contract	Type	Bases		
L	setMaxDayOfMonthCanUnlock	External ❗	🛑	onlyOwner
L	reassignToken	Public ❗	🛑	onlyOwner
L		External ❗	💸	NO❗
L	getUnclaimedToken	External ❗		NO❗
L	withdraw	External ❗	💸	onlyOwner
L	emergencyWithdraw	External ❗	🛑	onlyOwner
L	changeClaimFee	External ❗	🛑	onlyOwner
L	clearUnclaimedTokens	External ❗	🛑	onlyOwner
L	setNfts	External ❗	🛑	onlyOwner
L	setRewardToken	External ❗	🛑	onlyOwner
L	setNewLockPeriod	External ❗	🛑	onlyOwner
L	setNewHoldingTime	External ❗	🛑	onlyOwner
L	testTime	External ❗		NO❗
L	_dayOfMonth	Internal 🔒		
L	_daysToDate	Internal 🔒		

FULL AUDIT REPORT

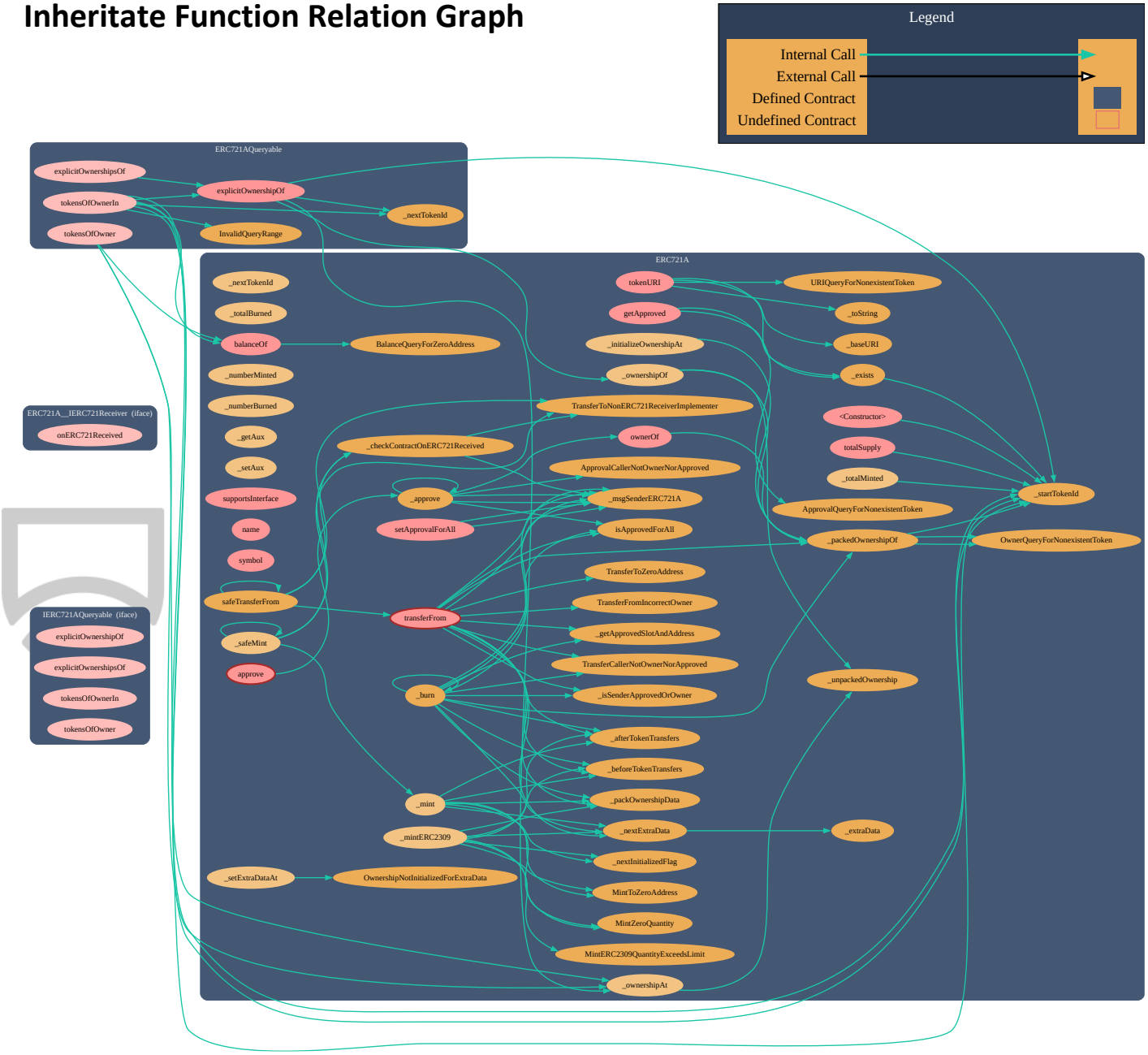
Contract	Type	Bases		
ERC721AQueryable	Implementation	ERC721A, IERC721AQueryable		
L	explicitOwnershipOf	Public !		NO!
L	explicitOwnershipsOf	External !		NO!
L	tokensOfOwnerIn	External !		NO!
L	tokensOfOwner	External !		NO!
IERC20	Interface			
L	totalSupply	External !		NO!
L	balanceOf	External !		NO!
L	transfer	External !	◉	NO!
L	allowance	External !		NO!
L	approve	External !	◉	NO!
L	transferFrom	External !	◉	NO!
L	decimals	External !		NO!

Legend

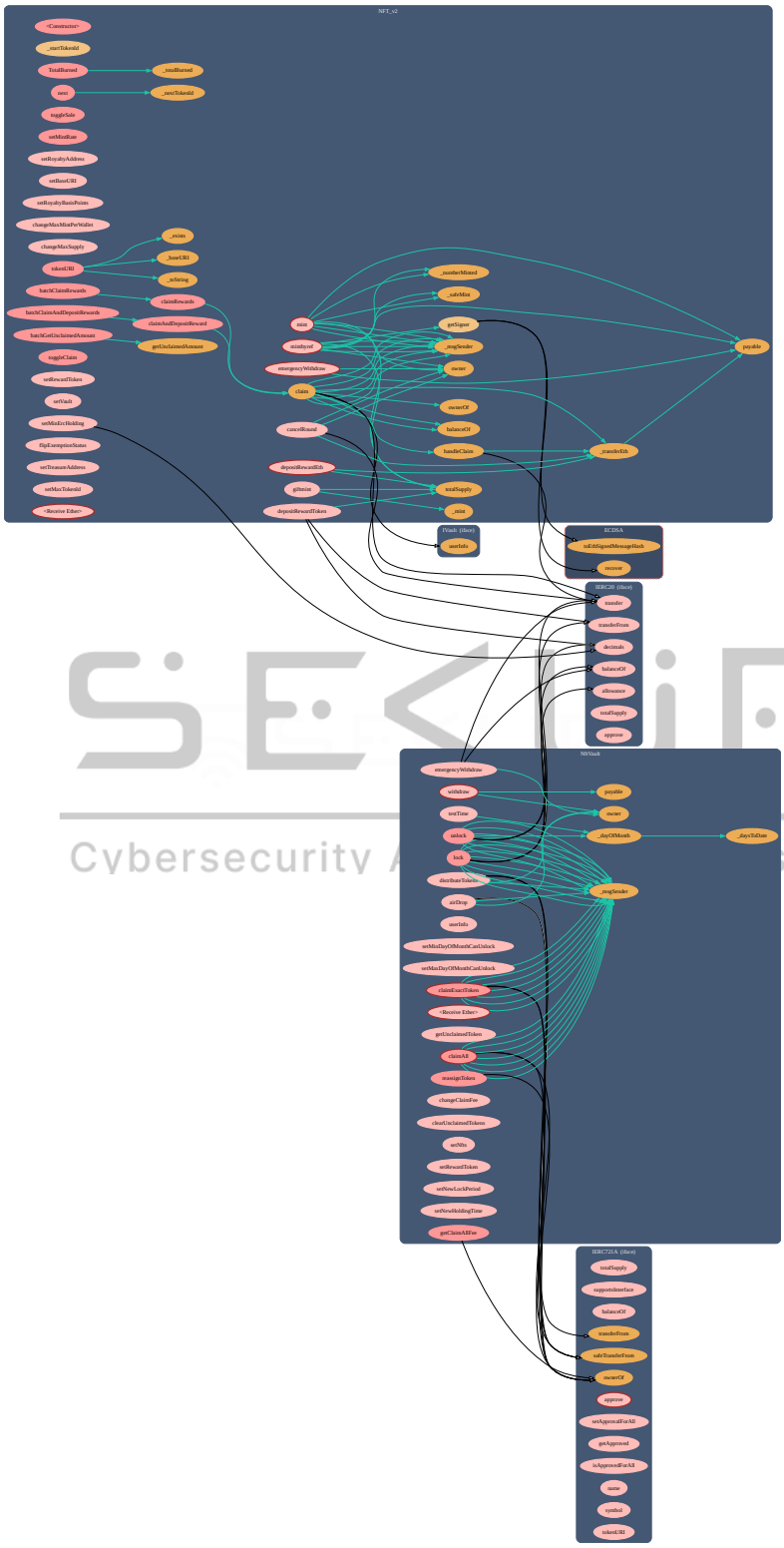
Symbol	Meaning
◉	Function can modify state
💵	Function is payable

FULL AUDIT REPORT

Inheritate Function Relation Graph

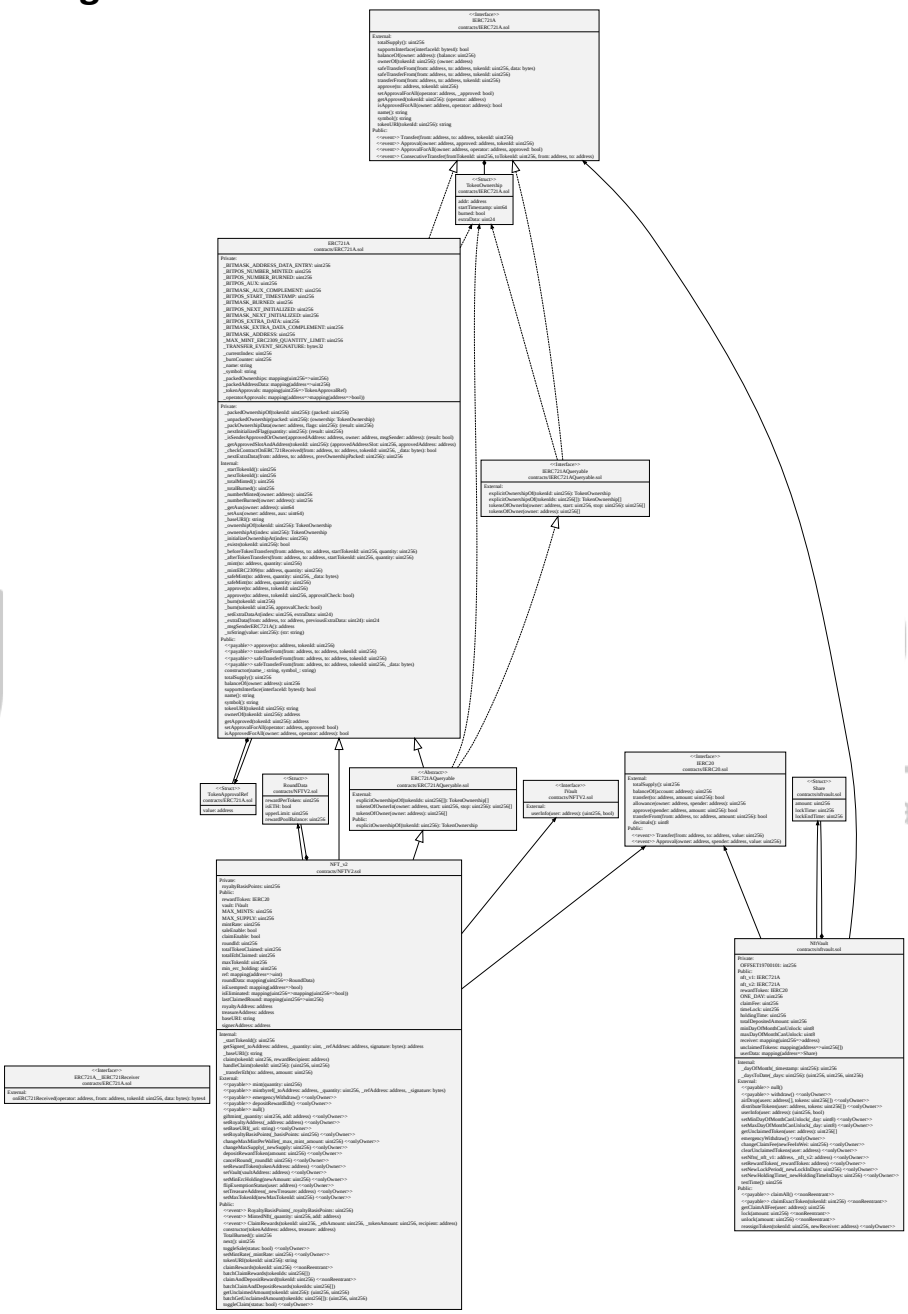


FULL AUDIT REPORT



FULL AUDIT REPORT

UML Class Diagram



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