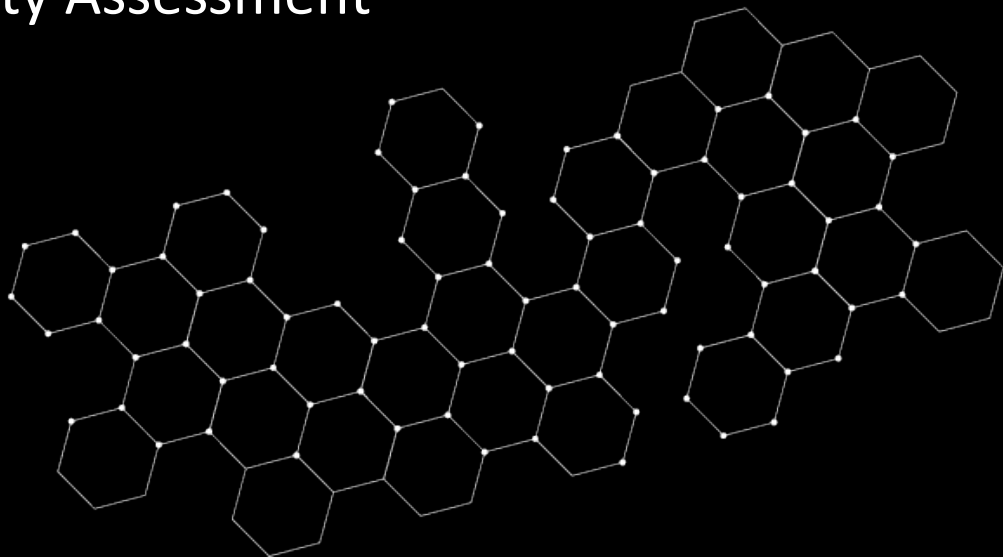




# Full report

## AuraSwap Security Assessment





THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

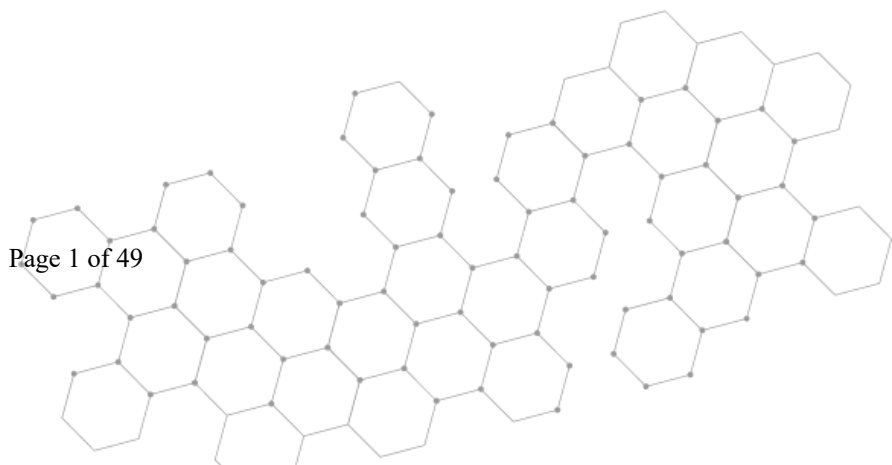
<b>Table of Contents</b>	<b>1</b>
<b>Report Information</b>	<b>2</b>
<b>Disclaimer</b>	<b>3</b>
<b>Executive Summary</b>	<b>4</b>
<b>Audit Result</b>	
<b>Project Introduction</b>	<b>5</b>
<b>Scope Information</b>	
<b>Audit Information</b>	
<b>Audit Version History</b>	
<b>Initial Audit Scope</b>	<b>6</b>
<b>Security Assessment Procedure</b>	<b>7</b>
<b>Risk Rating</b>	<b>8</b>
<b>Vulnerability Severity Summary</b>	<b>9</b>
<b>Vulnerability Findings</b>	<b>10-18</b>
<b>SWC &amp; SEC-01 To SEC-04</b>	
<b>SWC Findings</b>	<b>19-21</b>
<b>Visibility, Mutability, Modifier function testing</b>	<b>22-40</b>
<b>Inheritate Function Relation Graph</b>	<b>41-48</b>
<b>Inheritate Function Graph</b>	
<b>Contract Interaction Graph</b>	
<b>About SECURI</b>	<b>49</b>

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)





THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

### Report Information

About Report	AuraSwap Security Assessment
Version	v1.1
Client	AuraSwap
Language	Solidity
Confidentiality	Public
Platform	Polygon (Previously Matic Chain)
Contract Address	Router: <b>0x09Fd8B8ed6E30e583379Dc73b9261dF5E1A28b6F</b> Factory: <b>0x015DE3ec460869eb5ceAe4224Dc7112ac0a39303</b> AuraToken: <b>0x1b7805e2829fd7D194DCc3078a4199b13c77E467</b> SousChef: <b>0x266Eb9a845f677B1E24d59a4c0fDC24F625f7757</b> MasterChef: <b>0x44Bb1a3E56Cb12b7B1a8E925f09A170e3646346d</b> Timelock: <b>0x96257018553A4e988d884BE928B9bc7bC85B2649</b>
Audit Method	Whitebox

#### \*Audit Method

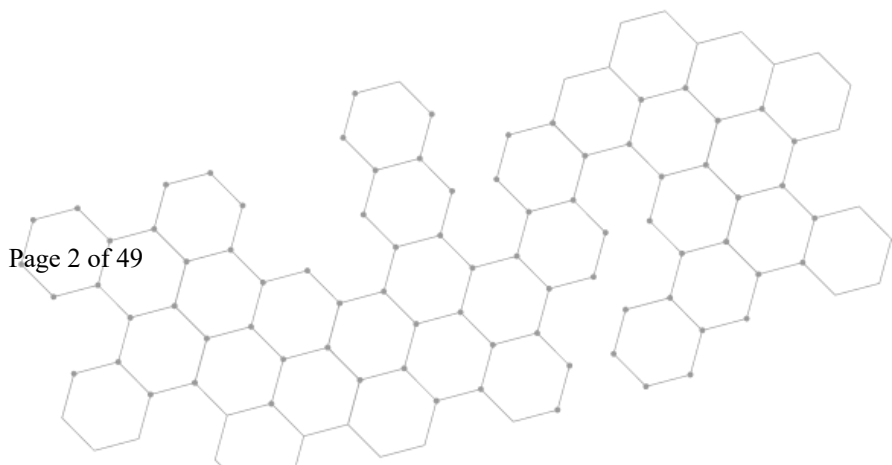
1. **Whitebox:** Securi Team receives all source code from the client to provide the assessment.
2. **Blackbox:** Securi Team receives only bytecode from the client to provide the assessment.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)





## FULL 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.**

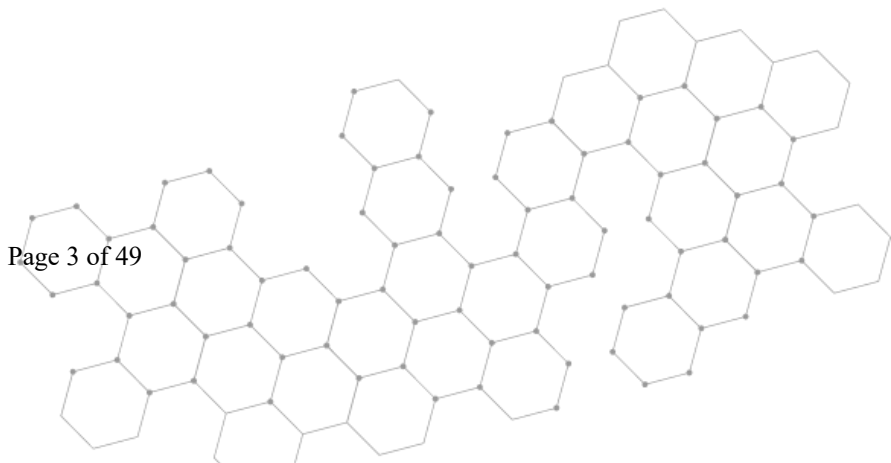
**SECURI disclaims any liability incurred. Whether it's Rugpull, Abandonment, Soft Rugpull**

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### Executive Summary

For this security assessment, Securi received a request from AuraSwap on Tuesday, August 16, 2022.

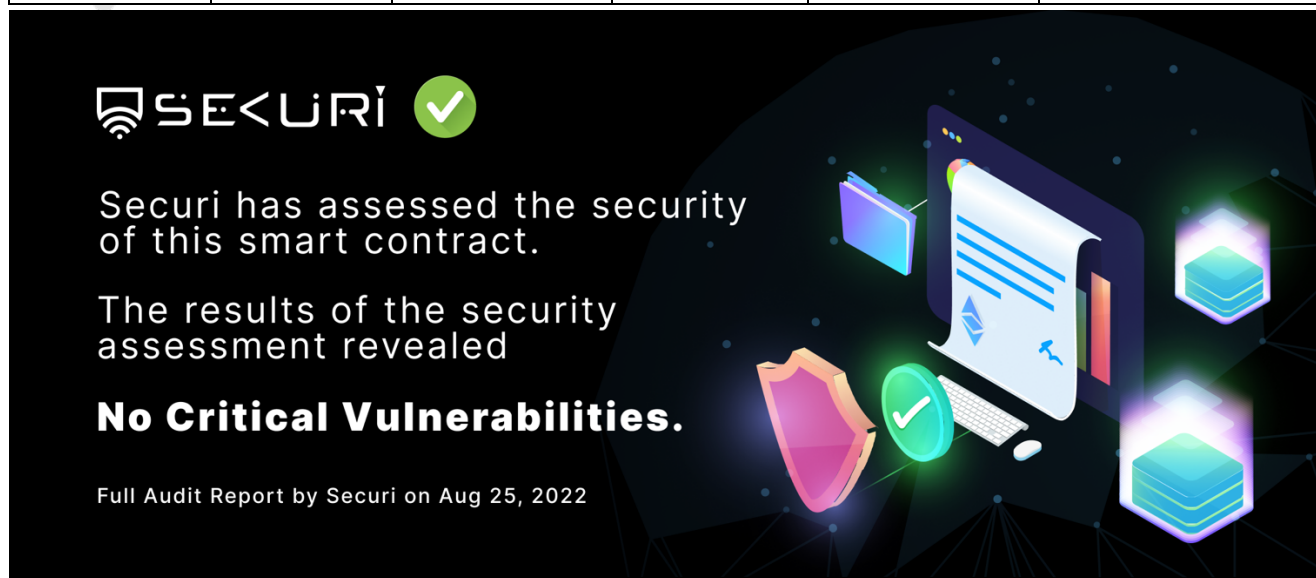
The Securi team has conducted a comprehensive security assessment of the vulnerabilities. This assessment is tested with an expert assessment. Using the following test requirements


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:

Critical	High	Medium	Low	Very Low	Informational
0	0	0	4	0	3



**SECURI** 

Securi has assessed the security of this smart contract.

The results of the security assessment revealed

**No Critical Vulnerabilities.**

Full Audit Report by Securi on Aug 25, 2022

The banner features a dark background with a network of glowing nodes and lines. On the right, there are several glowing blue and purple cubes, a shield icon, and a green checkmark icon. A computer monitor and keyboard are also visible in the background.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

### Project Introduction Scope Information:

Project Name	AuraSwap DEX
Website	<a href="https://www.auraswap.finance/home">https://www.auraswap.finance/home</a>
Chain	Polygon (Previously Matic Chain)
Language	Solidity

### Audit Information:

Request Date	Tuesday, August 16, 2022
Audit Date	Wednesday, August 24, 2022

### Audit Version History:

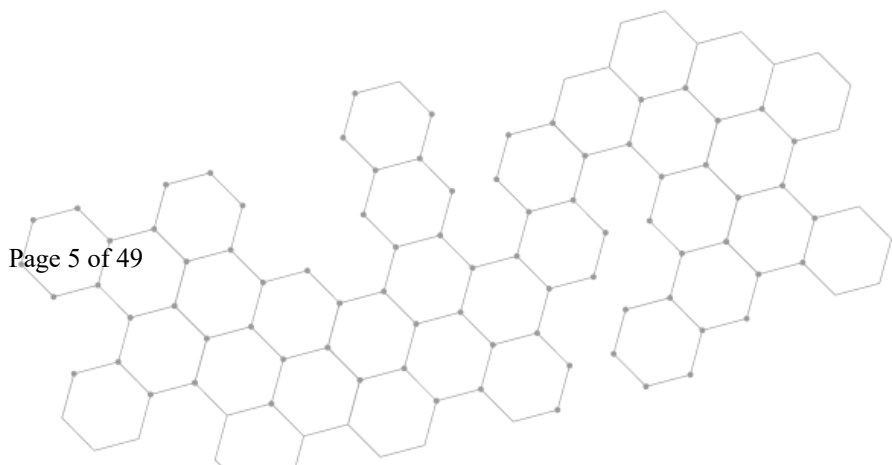
Version	Date	Description
1.0	Wednesday, August 24, 2022	Preliminary Report
1.1	Thursday, August 25, 2022	Full Report

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)





THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

### Initial Audit Scope: Contract:

Smart Contract	<p>Router: <b>0x09Fd8B8ed6E30e583379Dc73b9261dF5E1A28b6F</b></p> <p>Factory: <b>0x015DE3ec460869eb5ceAe4224Dc7112ac0a39303</b></p> <p>AuraToken: <b>0x1b7805e2829fd7D194DCc3078a4199b13c77E467</b></p> <p>SousChef: <b>0x266Eb9a845f677B1E24d59a4c0fDC24F625f7757</b></p> <p>MasterChef: <b>0x44Bb1a3E56Cb12b7B1a8E925f09A170e3646346d</b></p> <p>Timelock: <b>0x96257018553A4e988d884BE928B9bc7bC85B2649</b></p>
Compiler Version	<p>Router: <b>v0.6.12+commit.27d51765</b></p> <p>Factory: <b>v0.6.12+commit.27d51765</b></p> <p>AuraToken: <b>v0.6.12+commit.27d51765</b></p> <p>SousChef: <b>v0.6.12+commit.27d51765</b></p> <p>MasterChef: <b>v0.6.12+commit.27d51765</b></p> <p>Timelock: <b>v0.6.12+commit.27d51765</b></p>

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL 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



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### Risk Rating

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

- 1. Impact** The severity and potential impact of an attacker attack
- 2. 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	Low	Medium	High
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**

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

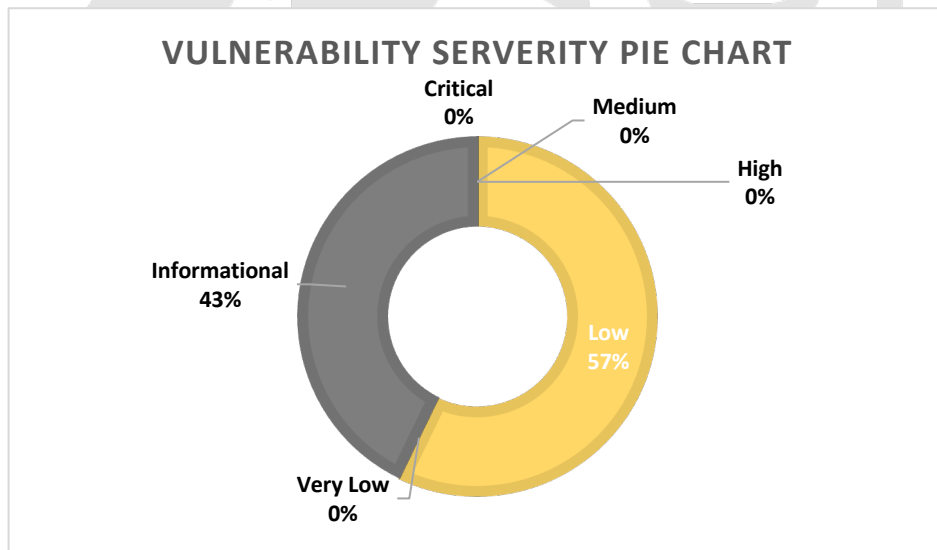
Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Vulnerability Severity Summary

Vulnerability Severity Level	Total
Critical	0
High	0
Medium	0
Low	4
Very Low	0
Informational (Non severity level)	3



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

## Vulnerability Findings

ID	Title	Severity	Status
SEC-01	Unused return values	LOW	Acknowledge
SEC-02	Imprecise arithmetic operations order	LOW	Acknowledge
SEC-03	Dangerous usage of `block.timestamp`	LOW	Acknowledge
SEC-04	Missing Zero Address Validation	LOW	Acknowledge
SEC-05	Assembly usage	Informational	Acknowledge
SEC-06	Conformity to Solidity naming conventions	Informational	Acknowledge
SWC-102	Outdated Compiler Version	Informational	Acknowledge

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)Website: <https://securi-lab.com>Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### SEC-01: Unused return values (unused-return)

Type	Severity	Location	Status
Unused return values (unused-return)	LOW	Line: 1379-1410	Acknowledge

#### Finding:

✗ MasterChef.add(uint256,IERC20,IRewarder,bool) (MasterChef.sol:1379-1410) ignores return value by \_lpToken.balanceOf(address(this)) (MasterChef.sol#1387)

#### Recommendation:

Ensure that all the return values of the function calls are used.

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return>

#### Alleviation:

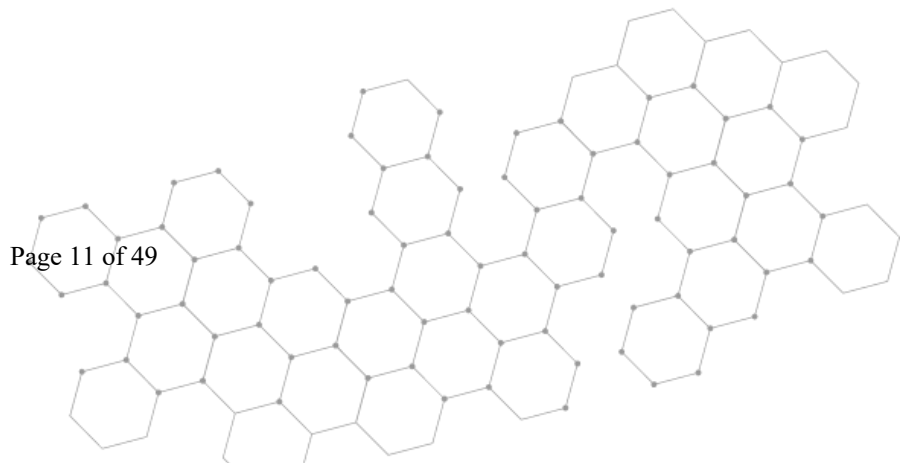
AuraSwap Team has Acknowledge this issues.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



**FULL REPORT****SEC-02: Imprecise arithmetic operations order**

Type	Severity	Location	Status
Imprecise arithmetic operations order (divide-before-multiply)	LOW	Line: 1448-1475, 1490-1506	Acknowledge

**Description:**

✗ MasterChef.pendingTokens(uint256,address) (MasterChef.sol:1448-1475) performs a multiplication on the result of a division:

- auraReward = timeElapsed.mul(auraPerSec).mul(pool.allocPoint).div(totalAllocPoint) (MasterChef.sol#1464)
- accAuraPerShare = accAuraPerShare.add(auraReward.mul(ACC\_AURA\_PRECISION).div(lpSupply)) (MasterChef.sol#1465)

✗ MasterChef.updatePool(uint256) (MasterChef.sol:1490-1506) performs a multiplication on the result of a division:

- auraReward = timeElapsed.mul(auraPerSec).mul(pool.allocPoint).div(totalAllocPoint) (MasterChef.sol#1497)
- pool.accAuraPerShare = pool.accAuraPerShare.add(auraReward.mul(ACC\_AURA\_PRECISION).div(lpSupply)) (MasterChef.sol#1500)

**Recommendation:**

Consider ordering multiplication before division.

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

**Alleviation:**

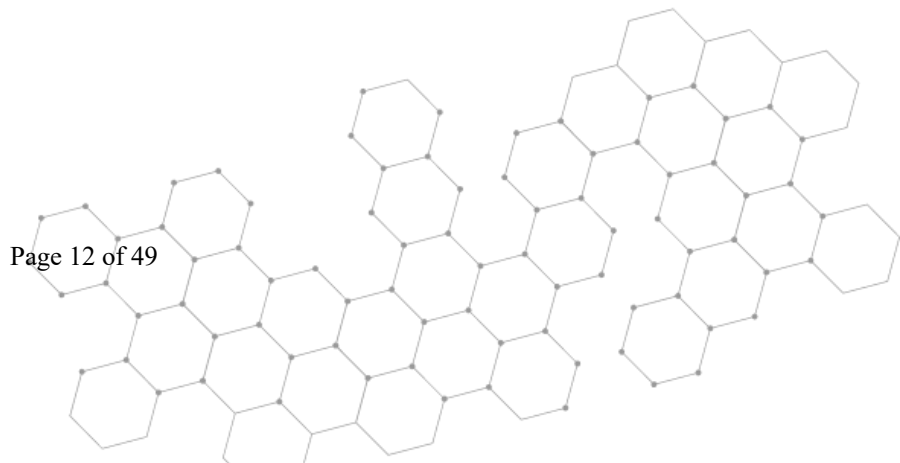
AuraSwap Team has Acknowledge this issues.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### SEC-03: Dangerous usage of `block.timestamp` (timestamp)

Type	Severity	Location	Status
Dangerous usage of `block.timestamp` (timestamp)	LOW	Line: Check on description	Acknowledge

#### Description:

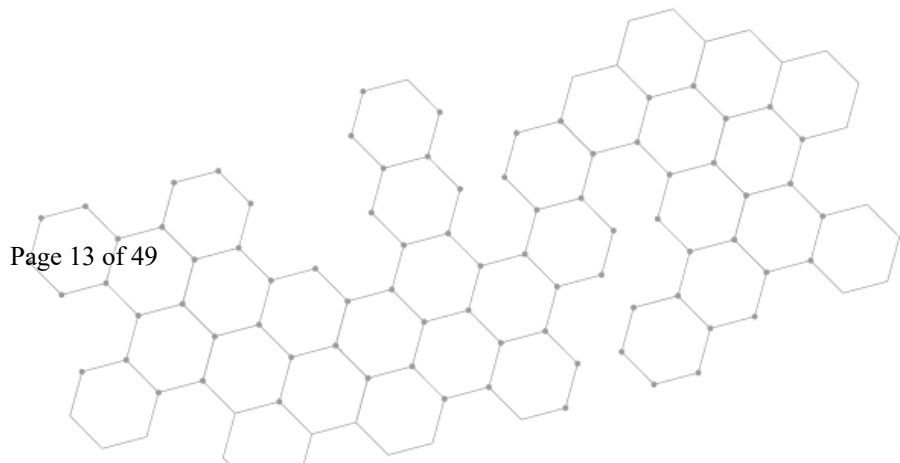
- ✗ AuraToken.delegateBySig(address,uint256,uint256,uint8,bytes32,bytes32) (MasterChef.sol:1093-1134) uses timestamp for comparisons
  - require(bool,string)(now <= expiry,AURA::delegateBySig: signature expired) (MasterChef.sol#1132)
- ✗ AuraToken.delegateBySig(address,uint256,uint256,uint8,bytes32,bytes32) (SousChef.sol:868-909) uses timestamp for comparisons
  - require(bool,string)(now <= expiry,AURA::delegateBySig: signature expired) (SousChef.sol#907)
- ✗ MasterChef.add(uint256,IERC20,IRewarder,bool) (MasterChef.sol:1379-1410) uses timestamp for comparisons
  - block.timestamp > startTimestamp (MasterChef.sol#1396)
- ✗ MasterChef.massUpdatePools() (MasterChef.sol:1478-1486) uses timestamp for comparisons
  - pid < length (MasterChef.sol#1480)
  - pool.allocPoint != 0 (MasterChef.sol#1482)
- ✗ MasterChef.pendingTokens(uint256,address) (MasterChef.sol:1448-1475) uses timestamp for comparisons
  - block.timestamp > pool.lastRewardTimestamp && lpSupply != 0 (MasterChef.sol#1462)
  - address(pool.rewarder) != address(0) (MasterChef.sol#1470)
- ✗ MasterChef.updatePool(uint256) (MasterChef.sol:1490-1506) uses timestamp for comparisons
  - block.timestamp > pool.lastRewardTimestamp (MasterChef.sol#1492)
  - lpSupply > 0 && totalAllocPoint > 0 (MasterChef.sol#1495)
- ✗ Timelock.executeTransaction(address,uint256,string,bytes,uint256) (Timelock.sol:266-291) uses timestamp for comparisons
  - require(bool,string)(getBlockTimestamp() >= eta,Timelock::executeTransaction: Transaction hasn't surpassed time lock.) (Timelock.sol#271)
  - require(bool,string)(getBlockTimestamp() <= eta.add(GRACE\_PERIOD),Timelock::executeTransaction: Transaction is stale.) (Timelock.sol#272)
- ✗ Timelock.queueTransaction(address,uint256,string,bytes,uint256) (Timelock.sol:246-255) uses timestamp for comparisons
  - require(bool,string)(eta >= getBlockTimestamp().add(delay),Timelock::queueTransaction: Estimated execution block must satisfy delay.) (Timelock.sol#248)
- ✗ UniswapV2ERC20.permit(address,address,uint256,uint256,uint8,bytes32,bytes32) (Factory.sol:122-134) uses timestamp for comparisons
  - require(bool,string)(deadline >= block.timestamp,UniswapV2: EXPIRED) (Factory.sol#123)

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)





THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

✗ UniswapV2Pair.\_update(uint256,uint256,uint112,uint112) (Factory.sol:285-298) uses timestamp for comparisons

- timeElapsed > 0 && \_reserve0 != 0 && \_reserve1 != 0 (Factory.sol#289)

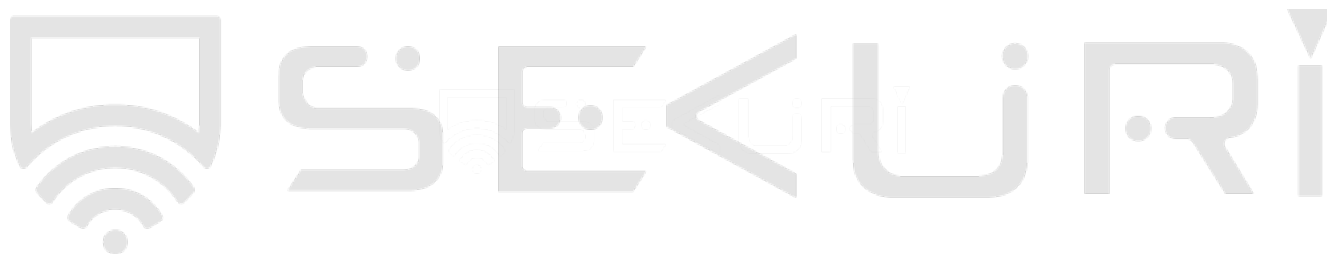
### Recommendation:

Avoid relying on `block.timestamp`.

Reference: <https://github.com/cryptic/slither/wiki/Detector-Documentation#block-timestamp>

### Alleviation:

AuraSwap Team has Acknowledge this issues.

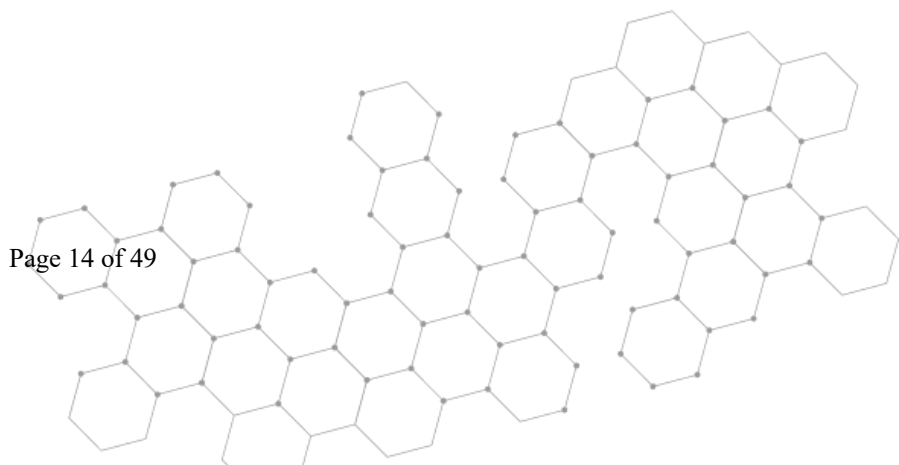


Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### SEC-04: Missing Zero Address Validation

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

#### Description:

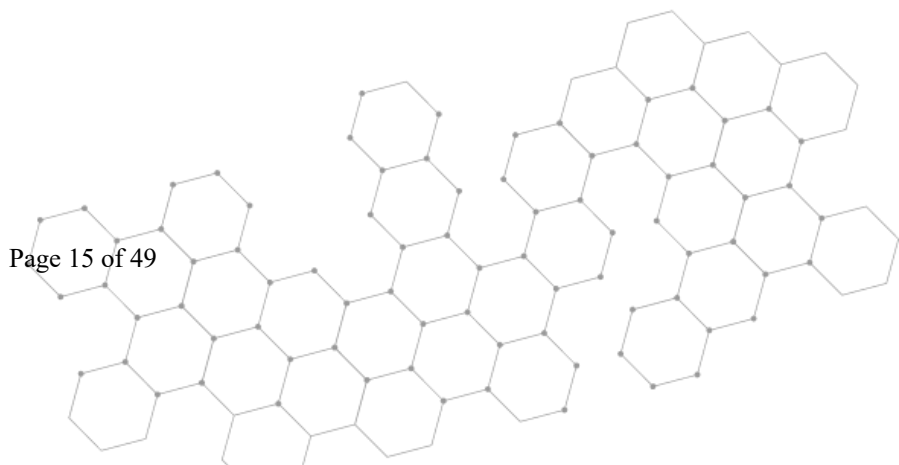
- ✗ MasterChef.constructor(AuraToken,SousChef,address,uint256,uint256).\_devAddr (MasterChef.sol:1355) lacks a zero-check on :
  - devAddr = \_devAddr (MasterChef.sol#1361)
- ✗ MasterChef.dev(address).\_devAddr (MasterChef.sol:1594) lacks a zero-check on :
  - devAddr = \_devAddr (MasterChef.sol#1596)
- ✗ Timelock.constructor(address,uint256).admin\_ (Timelock.sol:204) lacks a zero-check on :
  - admin = admin\_ (Timelock.sol#208)
- ✗ Timelock.executeTransaction(address,uint256,string,bytes,uint256).target (Timelock.sol:266) lacks a zero-check on :
  - (success,returnData) = target.call.value(value)(callData) (Timelock.sol#285)
- ✗ Timelock.setPendingAdmin(address).pendingAdmin\_ (Timelock.sol:233) lacks a zero-check on :
  - pendingAdmin = pendingAdmin\_ (Timelock.sol#241)
- ✗ UniswapV2Factory.constructor(address).\_feeToSetter (Factory.sol:429) lacks a zero-check on :
  - feeToSetter = \_feeToSetter (Factory.sol#430)
- ✗ UniswapV2Factory.setFeeTo(address).\_feeTo (Factory.sol:458) lacks a zero-check on :
  - feeTo = \_feeTo (Factory.sol#460)
- ✗ UniswapV2Factory.setFeeToSetter(address).\_feeToSetter (Factory.sol:463) lacks a zero-check on :
  - feeToSetter = \_feeToSetter (Factory.sol#465)
- ✗ UniswapV2Pair.initialize(address,address).\_token0 (Factory.sol:278) lacks a zero-check on :
  - token0 = \_token0 (Factory.sol#280)
- ✗ UniswapV2Pair.initialize(address,address).\_token1 (Factory.sol:278) lacks a zero-check on :
  - token1 = \_token1 (Factory.sol#281)
- ✗ UniswapV2Router02.constructor(address,address).\_WETH (Router.sol:405) lacks a zero-check on :
  - WETH = \_WETH (Router.sol#407)
- ✗ UniswapV2Router02.constructor(address,address).\_factory (Router.sol:405) lacks a zero-check on :
  - factory = \_factory (Router.sol#406)

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)







THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

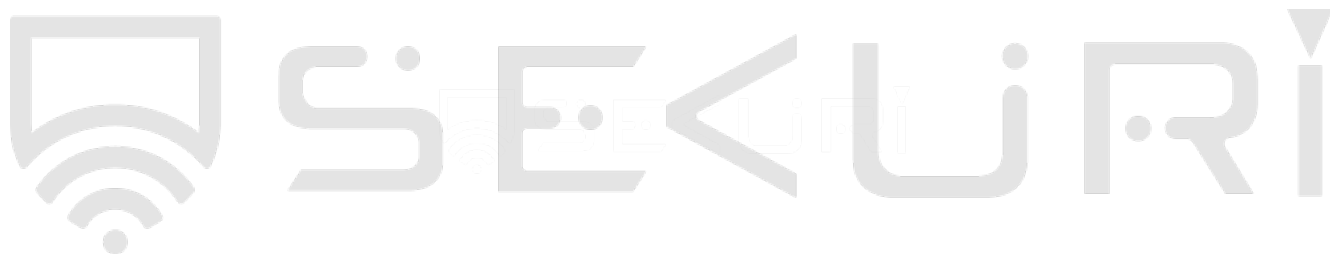
### Recommendation:

Check that the address is not zero.

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

### Alleviation:

AuraSwap Team has Acknowledge this issues.

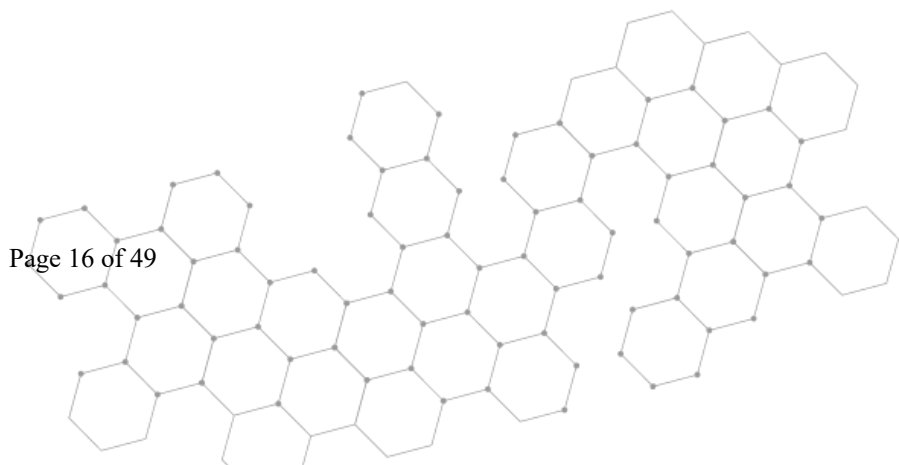


Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)





THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

### SEC-05: Assembly usage (assembly)

Type	Severity	Location	Status
Assembly usage (assembly)	Informational	Line: Check on description	Acknowledge

#### Description:

- ✗ AuraToken.getChainId() (MasterChef.sol:1252-1256) uses assembly
  - INLINE ASM (MasterChef.sol#1254)
- ✗ AuraToken.getChainId() (SousChef.sol:1027-1031) uses assembly
  - INLINE ASM (SousChef.sol#1029)

#### Recommendation:

Do not use `evm` assembly.

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage>

#### Alleviation:

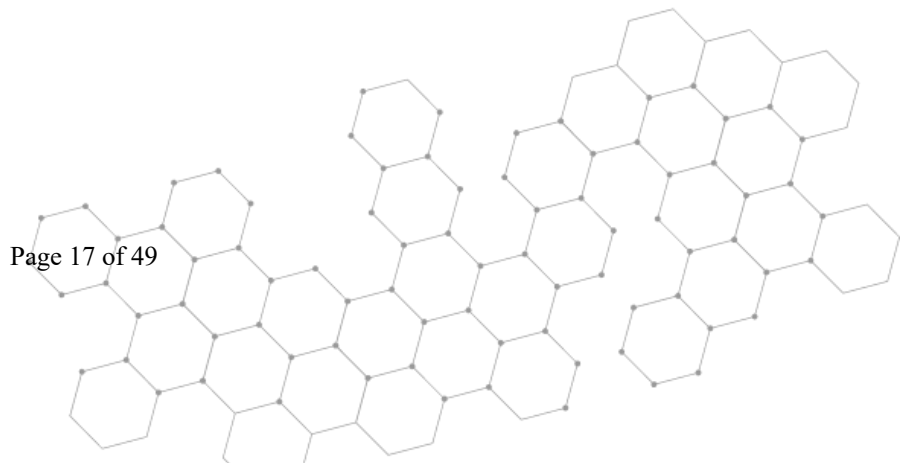
AuraSwap Team has Acknowledge this issues.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

**SEC-06: Conformity to Solidity naming conventions**

Type	Severity	Location	Status
Conformity to Solidity naming conventions (naming-convention)	Informational	Line: Check on description	<b>Acknowledge</b>

**Description:**

- ✗ Constant AuraToken.maxSupply (SousChef.sol:793) is not in UPPER\_CASE\_WITH\_UNDERSCORES
- ✗ Parameter AuraToken.mint(address,uint256).\_amount (SousChef.sol:796) is not in mixedCase
- ✗ Parameter SousChef.safeAuraTransfer(address,uint256).\_amount (SousChef.sol:1048) is not in mixedCase
- ✗ Variable AuraToken.\_delegates (SousChef.sol:810) is not in mixedCase
- ✗ Variable Timelock.admin\_initialized (Timelock.sol:199) is not in mixedCase

**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:**

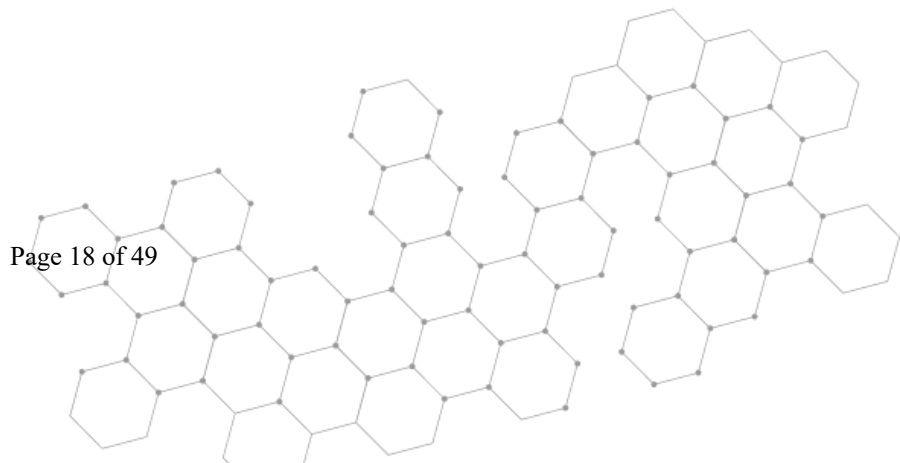
AuraSwap Team has Acknowledge this issues.

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



**FULL 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	Informational
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

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)Website: <https://securi-lab.com>Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

SWC-115	Authorization through tx.origin	Complete	No risk
SWC-116	Block values as a proxy for time	Complete	Informational
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

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

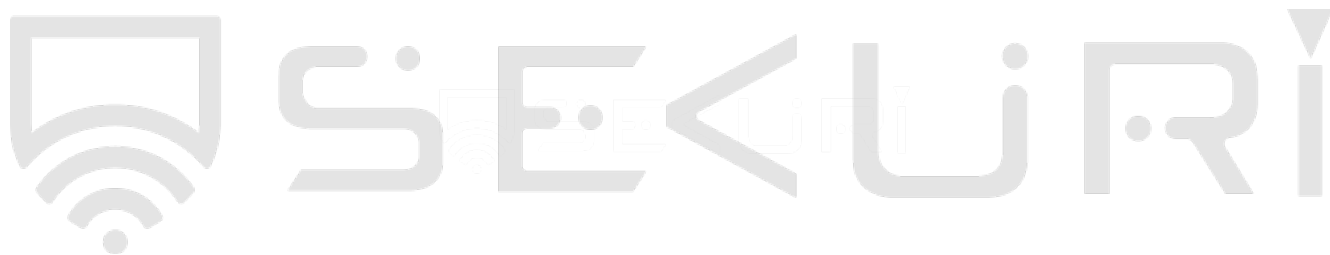
Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

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

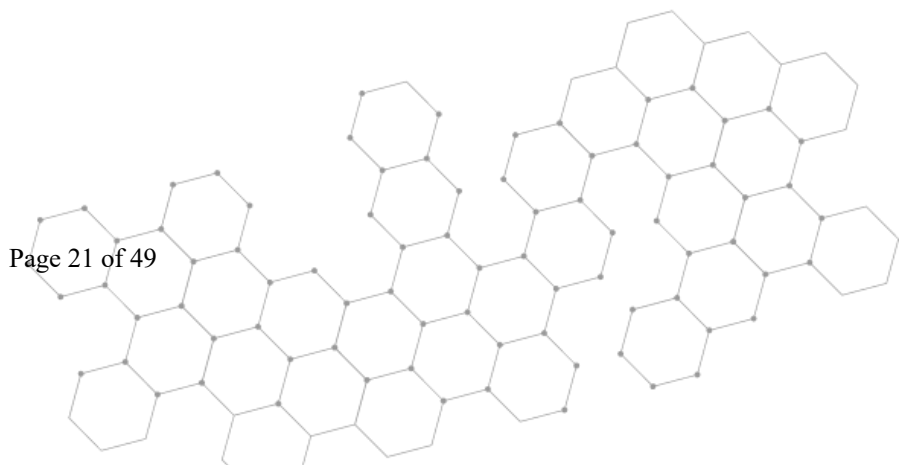


Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### Visibility, Mutability, Modifier function testing

Router: 0x09Fd8B8ed6E30e583379Dc73b9261dF5E1A28b6F

Contracts Description Table

Contract	Type	Bases		
-----: :-----: :-----: :-----: :-----:				
----:				
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	
<b>**Modifiers**</b>				
<b>**IUniswapV2Pair**</b>   Interface				
L	name   External	!	NO	!
L	symbol   External	!	NO	!
L	decimals   External	!	NO	!
L	totalSupply   External	!	NO	!
L	balanceOf   External	!	NO	!
L	allowance   External	!	NO	!
L	approve   External	!	●	NO
L	transfer   External	!	●	NO
L	transferFrom   External	!	●	NO
L	DOMAIN_SEPARATOR   External	!	NO	!
L	PERMIT_TYPEHASH   External	!	NO	!
L	nonces   External	!	NO	!
L	permit   External	!	●	NO
L	MINIMUM_LIQUIDITY   External	!	NO	!
L	factory   External	!	NO	!
L	token0   External	!	NO	!
L	token1   External	!	NO	!
L	getReserves   External	!	NO	!
L	price0CumulativeLast   External	!	NO	!
L	price1CumulativeLast   External	!	NO	!
L	kLast   External	!	NO	!
L	mint   External	!	●	NO
L	burn   External	!	●	NO
L	swap   External	!	●	NO
L	skim   External	!	●	NO

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

```
| L | sync | External ! | ● | NO ! |
| L | initialize | External ! | ● | NO ! |
|||||
| **SafeMathUniswap** | Library | |||
| L | add | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | mul | Internal 🔒 | | |
|||||
| **UniswapV2Library** | Library | |||
| L | sortTokens | Internal 🔒 | | |
| L | pairFor | Internal 🔒 | | |
| L | getReserves | Internal 🔒 | | |
| L | quote | Internal 🔒 | | |
| L | getAmountOut | Internal 🔒 | | |
| L | getAmountIn | Internal 🔒 | | |
| L | getAmountsOut | Internal 🔒 | | |
| L | getAmountsIn | Internal 🔒 | | |
|||||
| **TransferHelper** | Library | |||
| L | safeApprove | Internal 🔒 | ● | |
| L | safeTransfer | Internal 🔒 | ● | |
| L | safeTransferFrom | Internal 🔒 | ● | |
| L | safeTransferETH | Internal 🔒 | ● | |
|||||
| **IUniswapV2Router01** | Interface | |||
| L | factory | External ! | | NO ! |
| L | WETH | External ! | | NO ! |
| L | addLiquidity | External ! | ● | NO ! |
| L | addLiquidityETH | External ! | ⚠️ | NO ! |
| L | removeLiquidity | External ! | ● | NO ! |
| L | removeLiquidityETH | External ! | ● | NO ! |
| L | removeLiquidityWithPermit | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermit | External ! | ● | NO ! |
| L | swapExactTokensForTokens | External ! | ● | NO ! |
| L | swapTokensForExactTokens | External ! | ● | NO ! |
| L | swapExactETHForTokens | External ! | ⚠️ | NO ! |
| L | swapTokensForExactETH | External ! | ● | NO ! |
| L | swapExactTokensForETH | External ! | ● | NO ! |
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```
| L | swapETHForExactTokens | External ! | 🚫 |NO ! |
| L | quote | External ! | |NO ! |
| L | getAmountOut | External ! | |NO ! |
| L | getAmountIn | External ! | |NO ! |
| L | getAmountsOut | External ! | |NO ! |
| L | getAmountsIn | External ! | |NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | 🚫 |NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | 🚫
|NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | 🚫 |NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🚫 |NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | 🚫 |NO ! |
|||||
| **IUniswapV2Factory** | Interface | |||
| L | feeTo | External ! | |NO ! |
| L | feeToSetter | External ! | |NO ! |
| L | getPair | External ! | |NO ! |
| L | allPairs | External ! | |NO ! |
| L | allPairsLength | External ! | |NO ! |
| L | createPair | External ! | 🚫 |NO ! |
| L | setFeeTo | External ! | 🚫 |NO ! |
| L | setFeeToSetter | External ! | 🚫 |NO ! |
|||||
| **IERC20Uniswap** | Interface | |||
| L | name | External ! | |NO ! |
| L | symbol | External ! | |NO ! |
| L | decimals | External ! | |NO ! |
| L | totalSupply | External ! | |NO ! |
| L | balanceOf | External ! | |NO ! |
| L | allowance | External ! | |NO ! |
| L | approve | External ! | 🚫 |NO ! |
| L | transfer | External ! | 🚫 |NO ! |
| L | transferFrom | External ! | 🚫 |NO ! |
|||||
| **IWETH** | Interface | |||
| L | deposit | External ! | 🚫 |NO ! |
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

```

| L | transfer | External ! | ● | NO ! |
| L | withdraw | External ! | ● | NO ! |
|||||
| **UniswapV2Router02** | Implementation | IUniswapV2Router02 |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | <Receive Ether> | External ! | ● | NO ! |
| L | _addLiquidity | Internal 🔒 | ● | |
| L | addLiquidity | External ! | ● | ensure |
| L | addLiquidityETH | External ! | ● | ensure |
| L | removeLiquidity | Public ! | ● | ensure |
| L | removeLiquidityETH | Public ! | ● | ensure |
| L | removeLiquidityWithPermit | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermit | External ! | ● | NO ! |
| L | removeLiquidityETHSupportingFeeOnTransferTokens | Public ! | ● | ensure |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | _swap | Internal 🔒 | ● | |
| L | swapExactTokensForTokens | External ! | ● | ensure |
| L | swapTokensForExactTokens | External ! | ● | ensure |
| L | swapExactETHForTokens | External ! | ● | ensure |
| L | swapTokensForExactETH | External ! | ● | ensure |
| L | swapExactTokensForETH | External ! | ● | ensure |
| L | swapETHForExactTokens | External ! | ● | ensure |
| L | _swapSupportingFeeOnTransferTokens | Internal 🔒 | ● | |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | ensure |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | ● | ensure |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | ensure |
| L | quote | Public ! | | NO ! |
| L | getAmountOut | Public ! | | NO ! |
| L | getAmountIn | Public ! | | NO ! |
| L | getAmountsOut | Public ! | | NO ! |
| L | getAmountsIn | Public ! | | NO ! |

```

### Legend

Symbol	Meaning
!-----:	-----

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

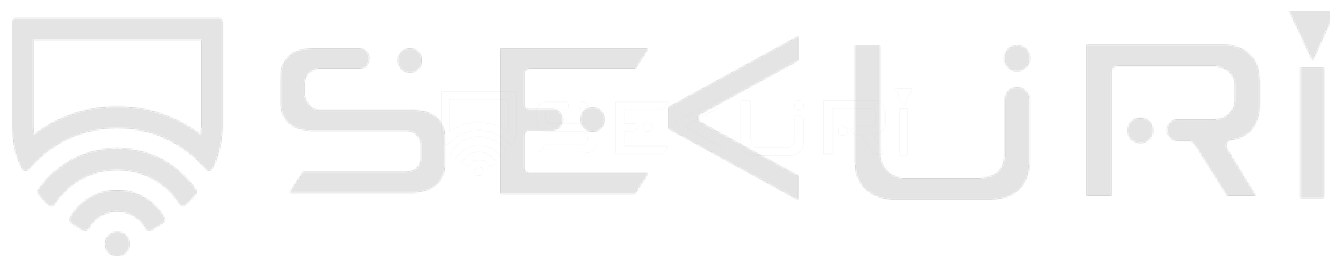




THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

		Function can modify state
		Function is payable

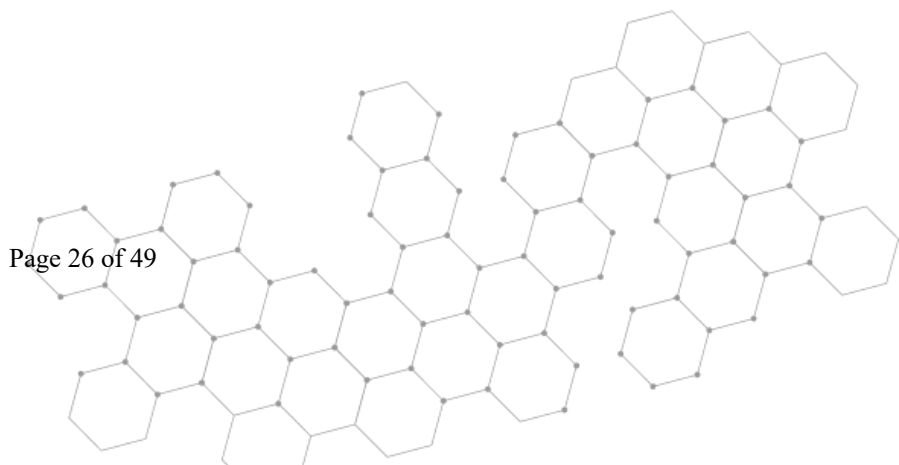


Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

Factory: 0x015DE3ec460869eb5ceAe4224Dc7112ac0a39303

### Contracts Description Table

Contract	Type	Bases		
-----: :-----: :-----: :-----: :-----				
----:				
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	
<b>**Modifiers**</b>				
L	<b>**IUniswapV2Factory**</b>	Interface		
L	feeTo	External !	NO !	
L	feeToSetter	External !	NO !	
L	getPair	External !	NO !	
L	allPairs	External !	NO !	
L	allPairsLength	External !	NO !	
L	createPair	External !	NO !	
L	setFeeTo	External !	NO !	
L	setFeeToSetter	External !	NO !	
L	<b>**SafeMathUniswap**</b>	Library		
L	add	Internal		
L	sub	Internal		
L	mul	Internal		
L	<b>**UniswapV2ERC20**</b>	Implementation		
L	<Constructor>	Public !	NO !	
L	_mint	Internal		
L	_burn	Internal		
L	_approve	Private		
L	_transfer	Private		
L	approve	External !	NO !	
L	transfer	External !	NO !	
L	transferFrom	External !	NO !	
L	permit	External !	NO !	
L	<b>**Math**</b>	Library		

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

```

| L | min | Internal 🔒 | | |
| L | sqrt | Internal 🔒 | | |
| | | | |
| **UQ112x112** | Library | | |
| L | encode | Internal 🔒 | | |
| L | uqdiv | Internal 🔒 | | |
| | | | |
| **IERC20Uniswap** | Interface | | |
| L | name | External ! | | NO ! |
| L | symbol | External ! | | NO ! |
| L | decimals | External ! | | NO ! |
| L | totalSupply | External ! | | NO ! |
| L | balanceOf | External ! | | NO ! |
| L | allowance | External ! | | NO ! |
| L | approve | External ! | 🔴 | NO ! |
| L | transfer | External ! | 🔴 | NO ! |
| L | transferFrom | External ! | 🔴 | NO ! |
| | | | |
| **IUniswapV2Callee** | Interface | | |
| L | uniswapV2Call | External ! | 🔴 | NO ! |
| | | | |
| **UniswapV2Pair** | Implementation | UniswapV2ERC20 | | |
| L | getReserves | Public ! | | NO ! |
| L | _safeTransfer | Private 🔒 | 🔴 | |
| L | <Constructor> | Public ! | 🔴 | NO ! |
| L | initialize | External ! | 🔴 | NO ! |
| L | _update | Private 🔒 | 🔴 | |
| L | _mintFee | Private 🔒 | 🔴 | |
| L | mint | External ! | 🔴 | lock |
| L | burn | External ! | 🔴 | lock |
| L | swap | External ! | 🔴 | lock |
| L | skim | External ! | 🔴 | lock |
| L | sync | External ! | 🔴 | lock |
| | | | |
| **UniswapV2Factory** | Implementation | IUniswapV2Factory | | |
| L | <Constructor> | Public ! | 🔴 | NO ! |
| L | allPairsLength | External ! | | NO ! |
| L | pairCodeHash | External ! | | NO ! |

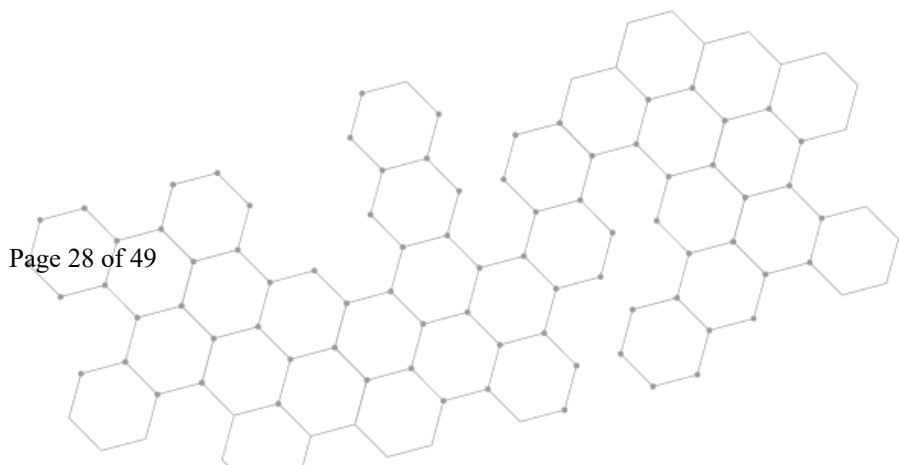
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

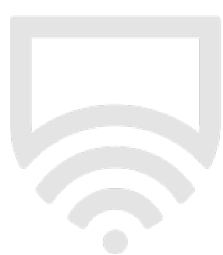


## FULL REPORT

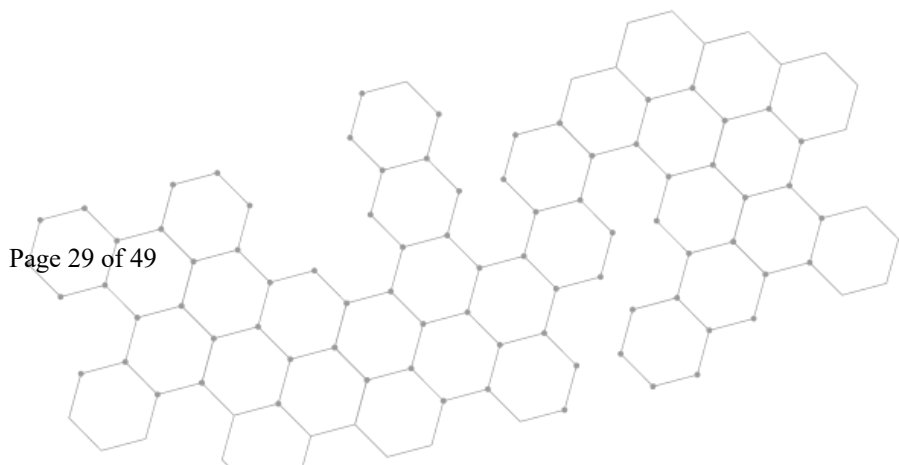
```
| L | createPair | External ! | ● | NO ! |  
| L | setFeeTo | External ! | ● | NO ! |  
| L | setFeeToSetter | External ! | ● | NO ! |
```

## Legend

Symbol	Meaning
●	Function can modify state
💵	Function is payable



SECURI

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)Website: <https://securi-lab.com>Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

AuraToken: 0x1b7805e2829fd7D194DCc3078a4199b13c77E467

### Contracts Description Table

Contract	Type	Bases		
:-----: :-----: :-----: :-----: :-----				
----:				
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	
<b>**Modifiers**</b>				
<b>**Context**</b>	Implementation			
L	_msgSender	Internal	🔒	
L	_msgData	Internal	🔒	
<b>**IERC20**</b>	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 !
<b>**SafeMath**</b>	Library			
L	add	Internal	🔒	
L	sub	Internal	🔒	
L	sub	Internal	🔒	
L	mul	Internal	🔒	
L	div	Internal	🔒	
L	div	Internal	🔒	
L	mod	Internal	🔒	
L	mod	Internal	🔒	
<b>**Address**</b>	Library			
L	isContract	Internal	🔒	
L	sendValue	Internal	🔒 🔴	
L	functionCall	Internal	🔒 🔴	
L	functionCall	Internal	🔒 🔴	

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```
| L | functionCallWithValue | Internal | 🔒 | 🔴 | |
| L | functionCallWithValue | Internal | 🔒 | 🔴 | |
| L | _functionCallWithValue | Private | 🔒 | 🔴 | |
| | | | |
| **ERC20** | Implementation | Context, IERC20 | | |
| L | <Constructor> | Public | ! | 🔴 | NO ! |
| L | name | Public | ! | 🔴 | NO ! |
| L | symbol | Public | ! | 🔴 | NO ! |
| L | decimals | Public | ! | 🔴 | NO ! |
| L | totalSupply | Public | ! | 🔴 | NO ! |
| L | balanceOf | Public | ! | 🔴 | NO ! |
| L | transfer | Public | ! | 🔴 | NO ! |
| L | allowance | Public | ! | 🔴 | NO ! |
| L | approve | Public | ! | 🔴 | NO ! |
| L | transferFrom | Public | ! | 🔴 | NO ! |
| L | increaseAllowance | Public | ! | 🔴 | NO ! |
| L | decreaseAllowance | Public | ! | 🔴 | NO ! |
| L | _transfer | Internal | 🔒 | 🔴 | |
| L | _mint | Internal | 🔒 | 🔴 | |
| L | _burn | Internal | 🔒 | 🔴 | |
| L | _approve | Internal | 🔒 | 🔴 | |
| L | _setupDecimals | Internal | 🔒 | 🔴 | |
| L | _beforeTokenTransfer | Internal | 🔒 | 🔴 | |
| | | | |
| **Ownable** | Implementation | Context | | |
| L | <Constructor> | Internal | 🔒 | 🔴 | |
| L | owner | Public | ! | 🔴 | NO ! |
| L | renounceOwnership | Public | ! | 🔴 | onlyOwner |
| L | transferOwnership | Public | ! | 🔴 | onlyOwner |
| | | | |
| **AuraToken** | Implementation | ERC20, Ownable | | |
| L | mint | Public | ! | 🔴 | onlyOwner |
| L | delegates | External | ! | 🔴 | NO ! |
| L | delegate | External | ! | 🔴 | NO ! |
| L | delegateBySig | External | ! | 🔴 | NO ! |
| L | getCurrentVotes | External | ! | 🔴 | NO ! |
| L | getPriorVotes | External | ! | 🔴 | NO ! |
| L | _delegate | Internal | 🔒 | 🔴 | |
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```
| L | _moveDelegates | Internal | 🔒 | 🔴 | |
| L | _writeCheckpoint | Internal | 🔒 | 🔴 | |
| L | safe32 | Internal | 🔒 | | |
| L | getChainId | Internal | 🔒 | | |
```

### Legend

Symbol	Meaning
🔴	Function can modify state
🔒	Function is payable



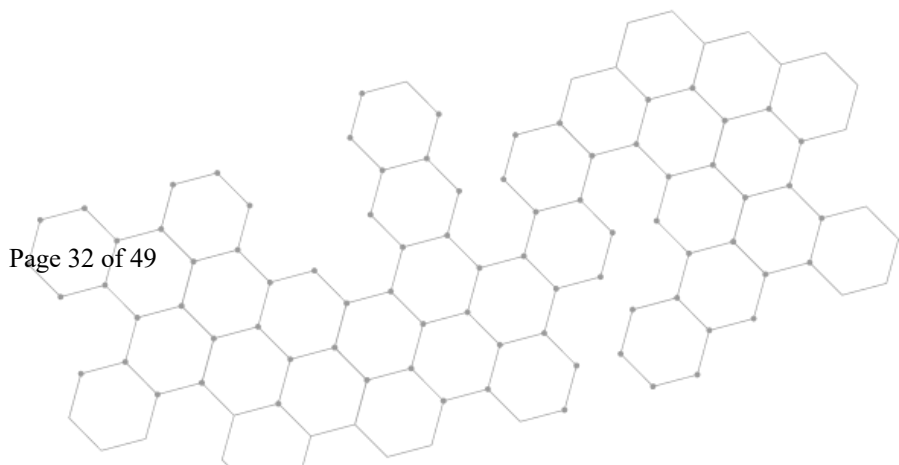
# SECURI

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

SousChef: 0x266Eb9a845f677B1E24d59a4c0fDC24F625f7757

### Contracts Description Table

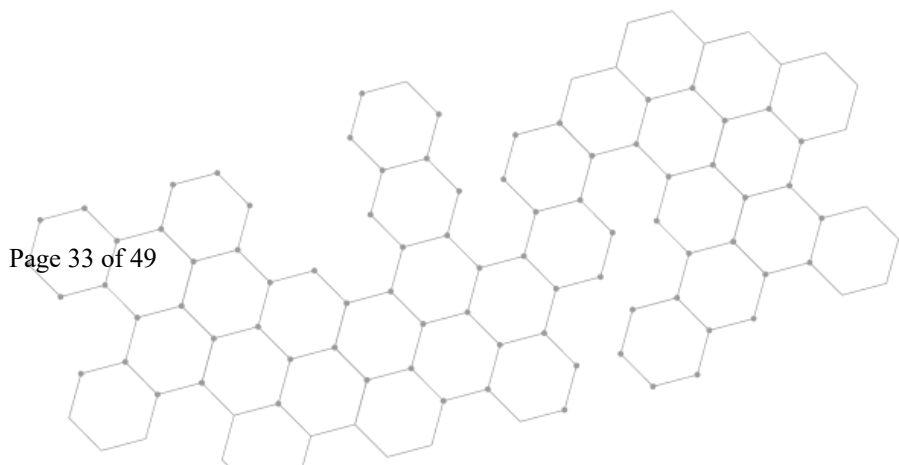
Contract	Type	Bases		
-----: :-----: :-----: :-----: :-----				
----:				
L	**Function Name**	**Visibility**	**Mutability**	
**Modifiers**				
**Context**	Implementation			
L	_msgSender	Internal	🔒	
L	_msgData	Internal	🔒	
**Ownable**	Implementation	Context		
L	<Constructor>	Internal	🔒	🔴
L	owner	Public	!	NO !
L	renounceOwnership	Public	!	🔴   onlyOwner
L	transferOwnership	Public	!	🔴   onlyOwner
**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 !
**SafeMath**	Library			
L	add	Internal	🔒	
L	sub	Internal	🔒	
L	sub	Internal	🔒	
L	mul	Internal	🔒	
L	div	Internal	🔒	
L	div	Internal	🔒	
L	mod	Internal	🔒	
L	mod	Internal	🔒	

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```

||||| | |
| **Address** | Library | |||
| L | isContract | Internal | 🔒 | | |
| L | sendValue | Internal | 🔒 | 🔴 | |
| L | functionCall | Internal | 🔒 | 🔴 | |
| L | functionCall | Internal | 🔒 | 🔴 | |
| L | functionCallWithValue | Internal | 🔒 | 🔴 | |
| L | functionCallWithValue | Internal | 🔒 | 🔴 | |
| L | _functionCallWithValue | Private | 🔒 | 🔴 | |
|||||
| **ERC20** | Implementation | Context, IERC20 | |||
| L | <Constructor> | Public | ! | 🔴 | NO ! |
| L | name | Public | ! | | NO ! |
| L | symbol | Public | ! | | NO ! |
| L | decimals | Public | ! | | NO ! |
| L | totalSupply | Public | ! | | NO ! |
| L | balanceOf | Public | ! | | NO ! |
| L | transfer | Public | ! | 🔴 | NO ! |
| L | allowance | Public | ! | | NO ! |
| L | approve | Public | ! | 🔴 | NO ! |
| L | transferFrom | Public | ! | 🔴 | NO ! |
| L | increaseAllowance | Public | ! | 🔴 | NO ! |
| L | decreaseAllowance | Public | ! | 🔴 | NO ! |
| L | _transfer | Internal | 🔒 | 🔴 | |
| L | _mint | Internal | 🔒 | 🔴 | |
| L | _burn | Internal | 🔒 | 🔴 | |
| L | _approve | Internal | 🔒 | 🔴 | |
| L | _setupDecimals | Internal | 🔒 | 🔴 | |
| L | _beforeTokenTransfer | Internal | 🔒 | 🔴 | |
|||||
| **AuraToken** | Implementation | ERC20, Ownable | |||
| L | mint | Public | ! | 🔴 | onlyOwner |
| L | delegates | External | ! | | NO ! |
| L | delegate | External | ! | 🔴 | NO ! |
| L | delegateBySig | External | ! | 🔴 | NO ! |
| L | getCurrentVotes | External | ! | | NO ! |
| L | getPriorVotes | External | ! | | NO ! |
| L | _delegate | Internal | 🔒 | 🔴 | |

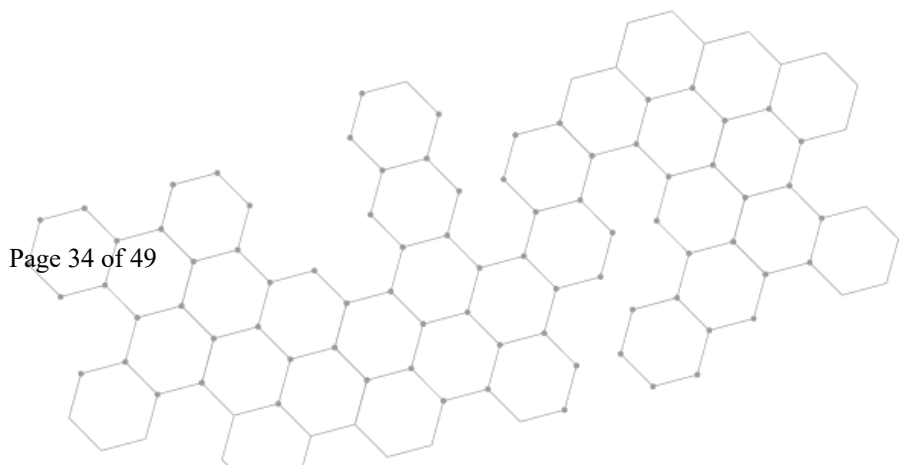
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```
| L | _moveDelegates | Internal | 🔒 | 🔴 | | |
| L | _writeCheckpoint | Internal | 🔒 | 🔴 | | |
| L | safe32 | Internal | 🔒 | | | |
| L | getChainId | Internal | 🔒 | | | |
| | | |
| **SousChef** | Implementation | Ownable | | |
| L | <Constructor> | Public | ! | 🔴 | NO! |
| L | safeAuraTransfer | Public | ! | 🔴 | onlyOwner |
```

### Legend

Symbol	Meaning
🔴	Function can modify state
🔒	Function is payable

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

MasterChef: 0x44Bb1a3E56Cb12b7B1a8E925f09A170e3646346d

### Contracts Description Table

Contract	Type	Bases		
-----: :-----: :-----: :-----: :-----				
----:				
L	**Function Name**	**Visibility**	**Mutability**	
**Modifiers**				
**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 !	
**SafeMath**	Library			
L	add	Internal		
L	sub	Internal		
L	sub	Internal		
L	mul	Internal		
L	div	Internal		
L	div	Internal		
L	mod	Internal		
L	mod	Internal		
**Address**	Library			
L	isContract	Internal		
L	sendValue	Internal		
L	functionCall	Internal		
L	functionCall	Internal		
L	functionCallWithValue	Internal		
L	functionCallWithValue	Internal		
L	_functionCallWithValue	Private		

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

```

**SafeERC20** | Library | |||
| L | safeTransfer | Internal | 🔒 | 🚫 | |
| L | safeTransferFrom | Internal | 🔒 | 🚫 | |
| L | safeApprove | Internal | 🔒 | 🚫 | |
| L | safeIncreaseAllowance | Internal | 🔒 | 🚫 | |
| L | safeDecreaseAllowance | Internal | 🔒 | 🚫 | |
| L | _callOptionalReturn | Private | 🔒 | 🚫 | |
| ||||
**Context** | Implementation | |||
| L | _msgSender | Internal | 🔒 | | |
| L | _msgData | Internal | 🔒 | | |
| ||||
**Ownable** | Implementation | Context | |||
| L | <Constructor> | Internal | 🔒 | 🚫 | |
| L | owner | Public | ! | | NO ! |
| L | renounceOwnership | Public | ! | 🚫 | onlyOwner |
| L | transferOwnership | Public | ! | 🚫 | onlyOwner |
| ||||
**ReentrancyGuard** | Implementation | |||
| L | <Constructor> | Internal | 🔒 | 🚫 | |
| ||||
**BoringERC20** | Library | |||
| L | returnDataToString | Internal | 🔒 | | |
| L | safeSymbol | Internal | 🔒 | | |
| L | safeName | Internal | 🔒 | | |
| L | safeDecimals | Internal | 🔒 | | |
| L | safeTransfer | Internal | 🔒 | 🚫 | |
| L | safeTransferFrom | Internal | 🔒 | 🚫 | |
| ||||
**ERC20** | Implementation | Context, IERC20 | |||
| L | <Constructor> | Public | ! | 🚫 | NO ! |
| L | name | Public | ! | | NO ! |
| L | symbol | Public | ! | | NO ! |
| L | decimals | Public | ! | | NO ! |
| L | totalSupply | Public | ! | | NO ! |
| L | balanceOf | Public | ! | | NO ! |
| L | transfer | Public | ! | 🚫 | NO ! |
| L | allowance | Public | ! | | NO ! |

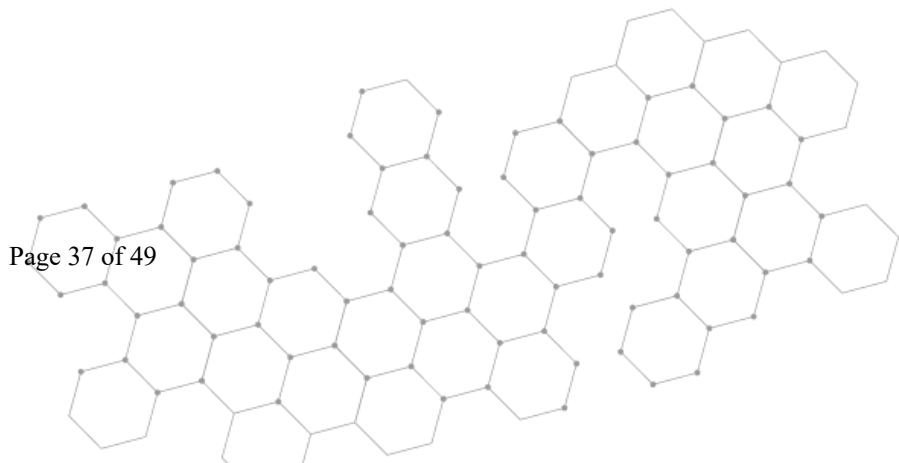
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

```
| L | approve | Public ! | ● | NO ! |
| L | transferFrom | Public ! | ● | NO ! |
| L | increaseAllowance | Public ! | ● | NO ! |
| L | decreaseAllowance | Public ! | ● | NO ! |
| L | _transfer | Internal 🔒 | ● | |
| L | _mint | Internal 🔒 | ● | |
| L | _burn | Internal 🔒 | ● | |
| L | _approve | Internal 🔒 | ● | |
| L | _setupDecimals | Internal 🔒 | ● | |
| L | _beforeTokenTransfer | Internal 🔒 | ● | |
|||||
| **AuraToken** | Implementation | ERC20, Ownable |||
| L | mint | Public ! | ● | onlyOwner |
| L | delegates | External ! | ● | NO ! |
| L | delegate | External ! | ● | NO ! |
| L | delegateBySig | External ! | ● | NO ! |
| L | getCurrentVotes | External ! | ● | NO ! |
| L | getPriorVotes | External ! | ● | NO ! |
| L | _delegate | Internal 🔒 | ● | |
| L | _moveDelegates | Internal 🔒 | ● | |
| L | _writeCheckpoint | Internal 🔒 | ● | |
| L | safe32 | Internal 🔒 | | |
| L | getChainId | Internal 🔒 | | |
|||||
| **SousChef** | Implementation | Ownable |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | safeAuraTransfer | Public ! | ● | onlyOwner |
|||||
| **IRewarder** | Interface | |||
| L | onAuraReward | External ! | ● | NO ! |
| L | pendingTokens | External ! | ● | NO ! |
| L | rewardToken | External ! | ● | NO ! |
|||||
| **MasterChef** | Implementation | Ownable, ReentrancyGuard |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | poolLength | External ! | ● | NO ! |
| L | add | External ! | ● | onlyOwner |
| L | set | External ! | ● | onlyOwner |
```

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

```

| L | pendingTokens | External ! | NO ! |
| L | massUpdatePools | Public ! | NO ! |
| L | updatePool | Public ! | NO ! |
| L | deposit | External ! | nonReentrant |
| L | withdraw | External ! | nonReentrant |
| L | emergencyWithdraw | External ! | nonReentrant |
| L | safeAuraTransfer | Internal | NO ! |
| L | dev | External ! | NO ! |
| L | updateEmissionRate | External ! | onlyOwner |

```

### Legend

Symbol	Meaning
●	Function can modify state
🔒	Function is payable

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

Timelock: 0x96257018553A4e988d884BE928B9bc7bC85B2649

### Contracts Description Table

Contract	Type	Bases		
:-----: :-----: :-----: :-----: :-----:				
----:				
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	
<b>**Modifiers**</b>				
L	<b>**SafeMath**</b>   Library			
L	add   Internal	🔒		
L	sub   Internal	🔒		
L	sub   Internal	🔒		
L	mul   Internal	🔒		
L	div   Internal	🔒		
L	div   Internal	🔒		
L	mod   Internal	🔒		
L	mod   Internal	🔒		
L	<b>**Timelock**</b>   Implementation			
L	<Constructor>   Public	!   🔴	NO !	
L	<Receive Ether>   External	!   💰	NO !	
L	setDelay   Public	!   🔴	NO !	
L	acceptAdmin   Public	!   🔴	NO !	
L	setPendingAdmin   Public	!   🔴	NO !	
L	queueTransaction   Public	!   🔴	NO !	
L	cancelTransaction   Public	!   🔴	NO !	
L	executeTransaction   Public	!   💰	NO !	
L	getBlockTimestamp   Internal	🔒		

### Legend

Symbol	Meaning
:-----: -----:	
🔴	Function can modify state
💰	Function is payable

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

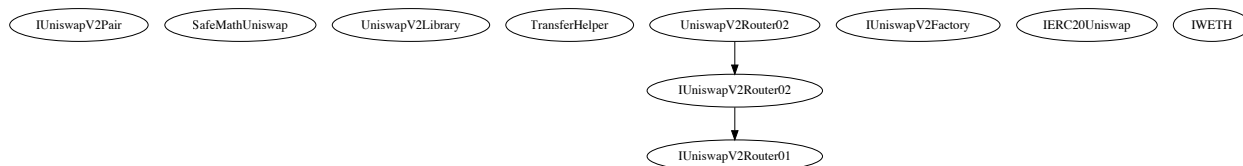
Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

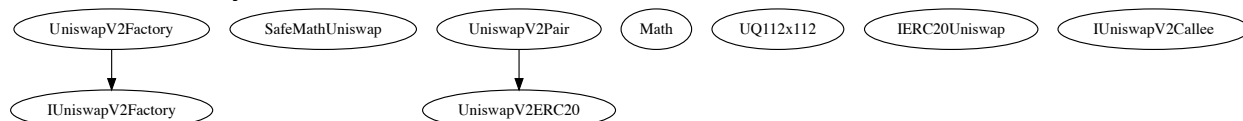
## FULL REPORT

### Inheritate Function Relation Graph

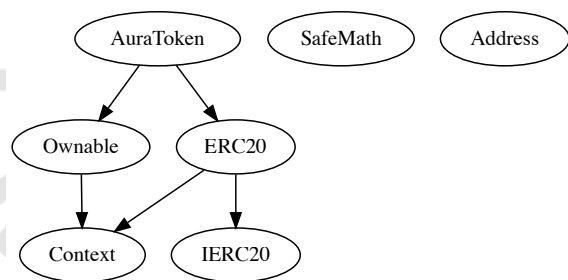
#### Inheritate Router:



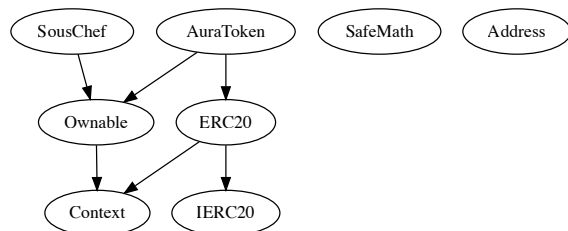
#### Inheritate Factory:



#### Inheritate AuraToken:



#### Inheritate SousChef:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

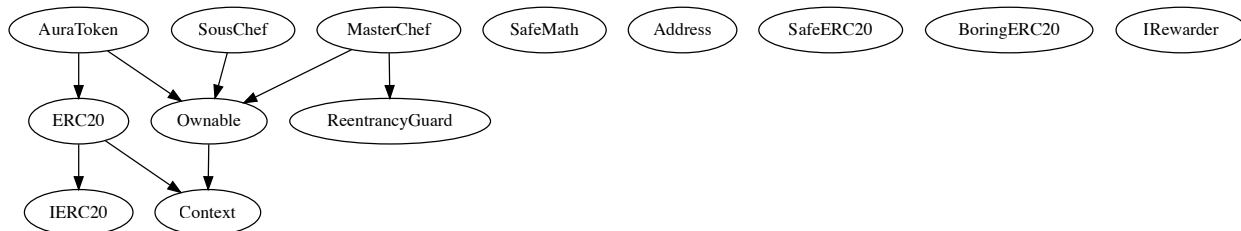
Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

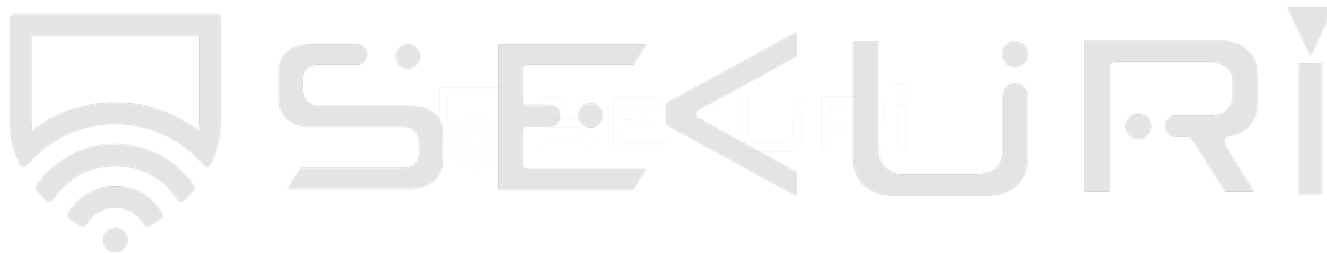
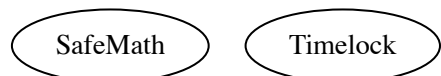
Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Inheritate MasterChef:



### Inheritate Timelock:

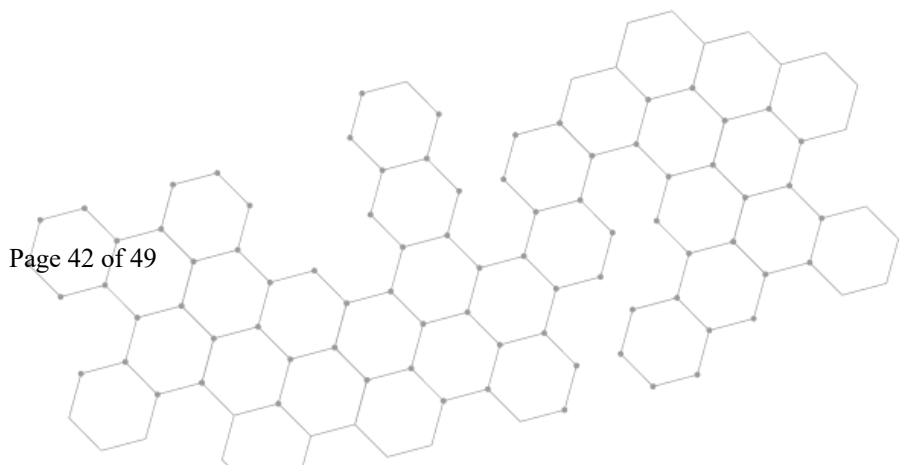


Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

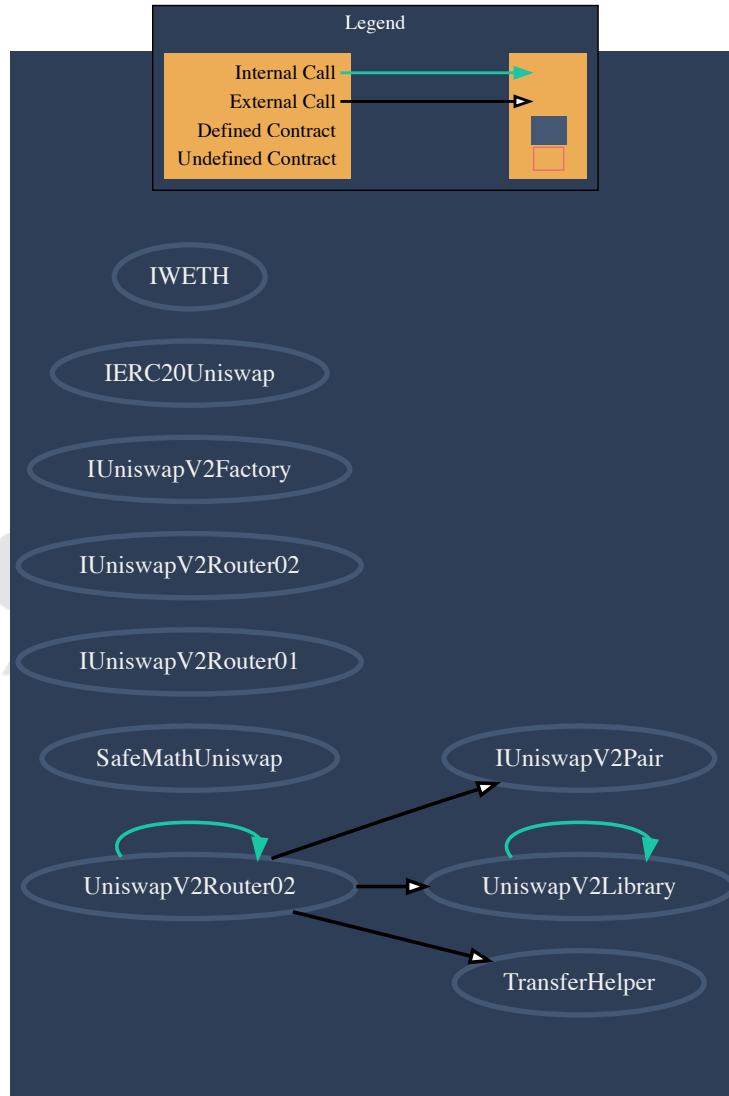
Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### Contract Interaction Graph

Inheritate Router:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

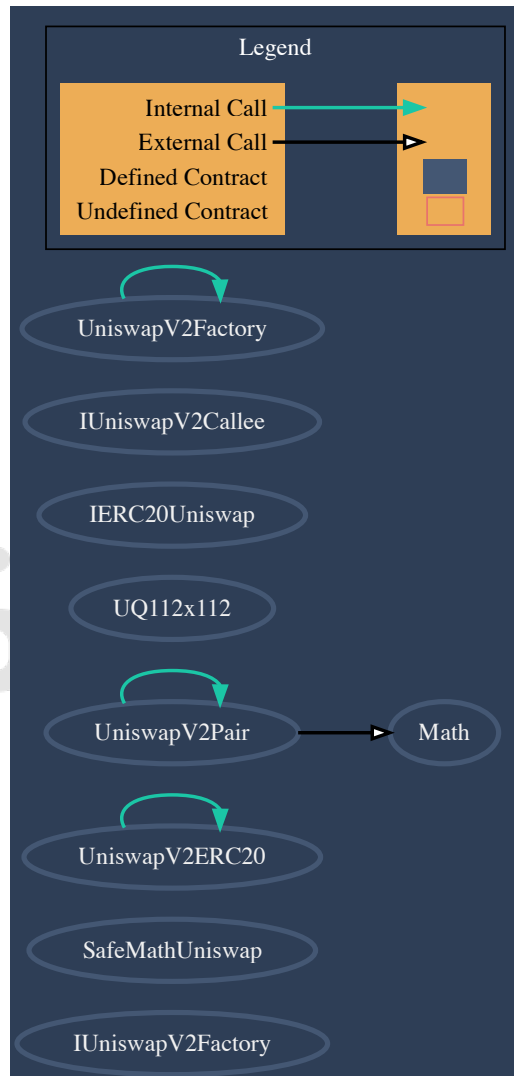
Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Inheritate Factory:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Inheritate AuraToken:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

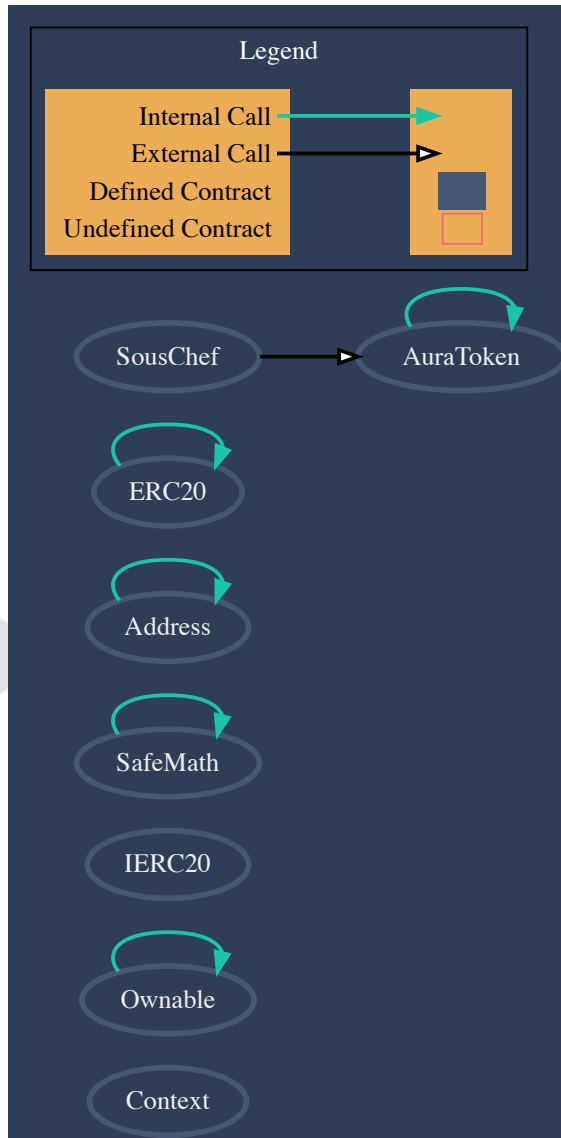
Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Inheritate SousChef:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

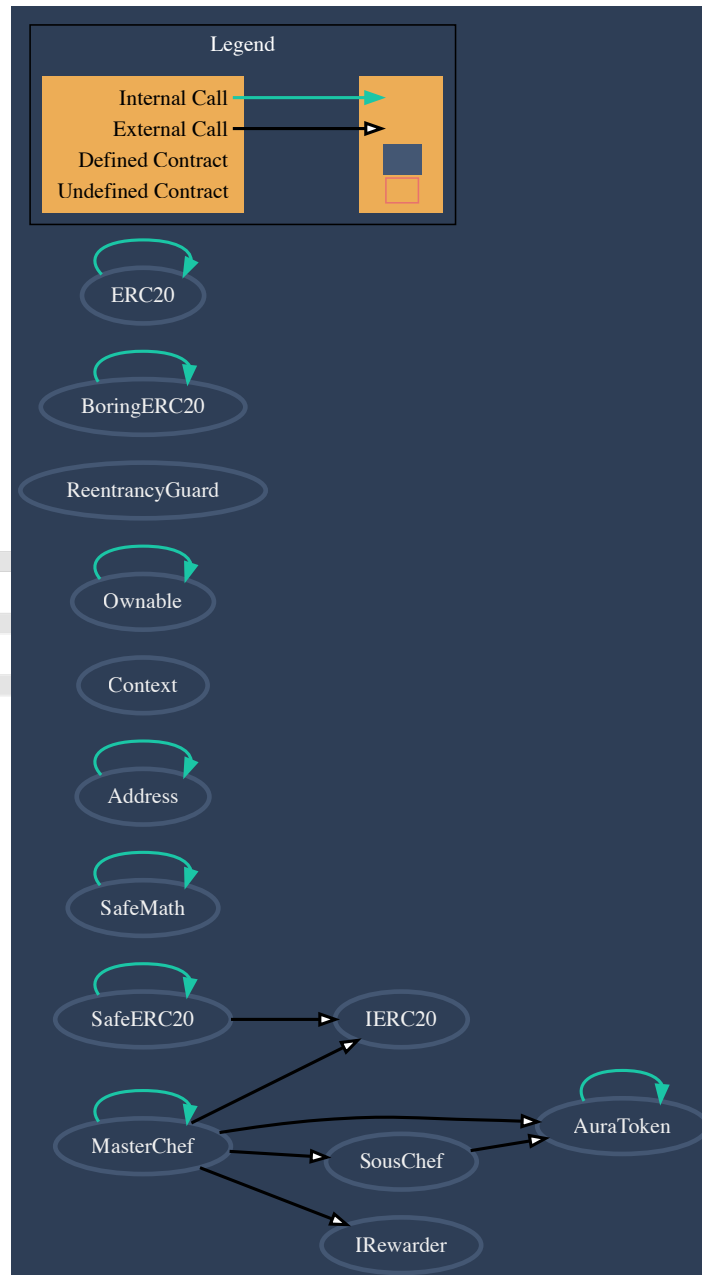
Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

## FULL REPORT

### Inheritate MasterChef:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

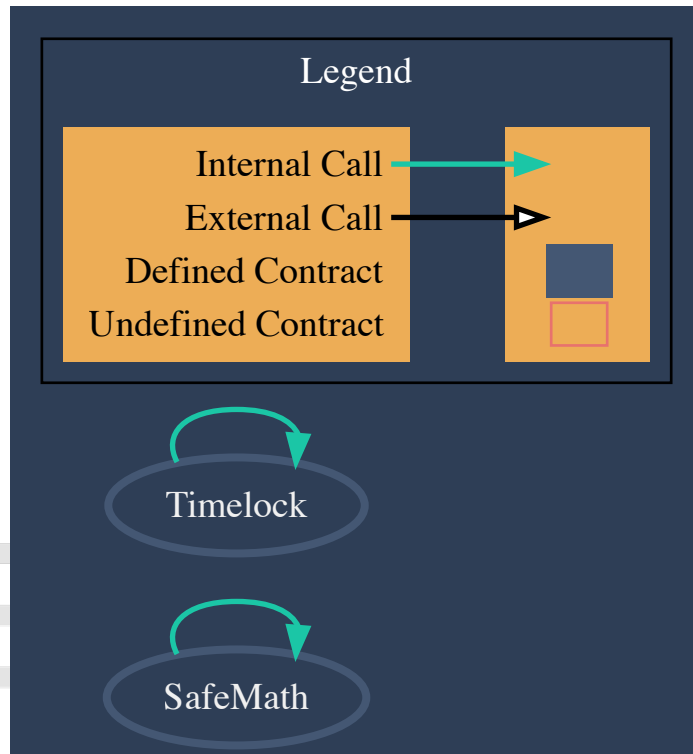
Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)



## FULL REPORT

### Inheritate Timelock:



Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

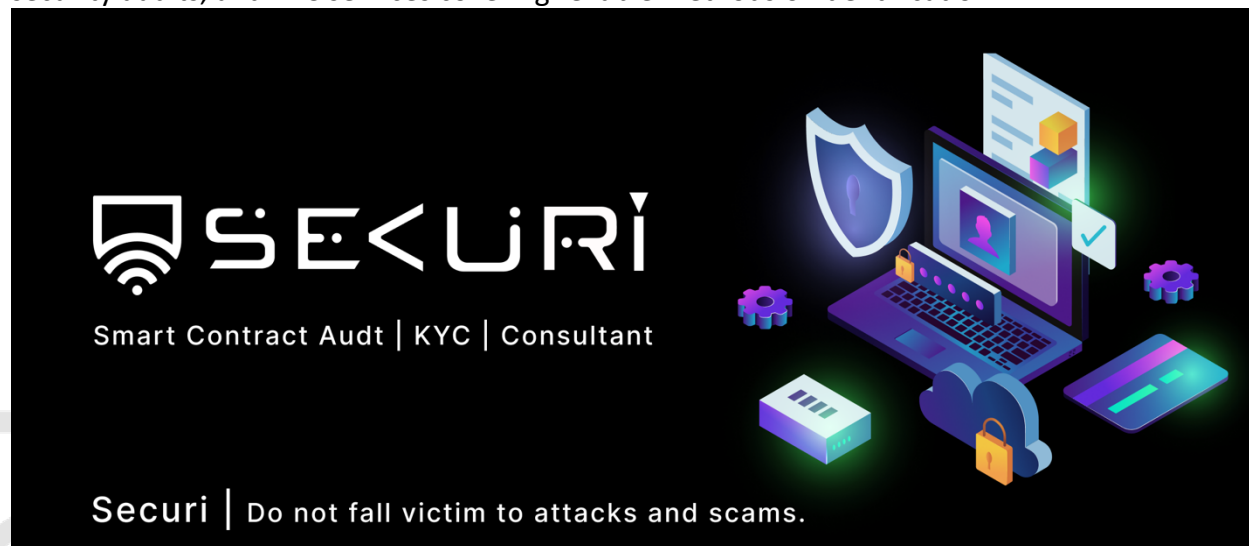


THURSDAY, AUGUST 25, 2022  
AuraSwap Security Assessment

## FULL REPORT

### About Securi

Securi is a group of cyber security experts providing cyber security consulting, smart contract security audits, and KYC services covering reliable methods of identification.



### Follow Us On:

Website	<a href="https://securi-lab.com/">https://securi-lab.com/</a>
Twitter	<a href="https://twitter.com/SECURI_LAB">https://twitter.com/SECURI_LAB</a>
Telegram	<a href="https://t.me/securi_lab">https://t.me/securi_lab</a>
Medium	<a href="https://medium.com/@securi">https://medium.com/@securi</a>

Contact us: [contact@securi-lab.com](mailto:contact@securi-lab.com)

Website: <https://securi-lab.com>

Telegram: [https://t.me/securi\\_lab](https://t.me/securi_lab)

Twitter: [https://twitter.com/SECURI\\_LAB](https://twitter.com/SECURI_LAB)

