



Security Assessment

Owlswap Finance

Vital Block Verified on August 7th, 2023

 @Vital-Block

 @VB_Audit

 info@vitalblock.org

 www.vitalblock.org



PREPARED FOR:
Owlit Finance



INTRODUCTION

Auditing Firm	 VITAL BLOCK SECURITY
Client Firm	 OWLSWAP FINANCE
Methodology	Automated Analysis, Manual Code Review
Language	Move
Contract Code	events.move comparator.move control.move maths.move pool.move router.move tools.move
Blockchain	Sui Network
Centralization	Active ownership
Website	https://owlit.io
Discord	https://discord.com/invite/5FCFNPTpwG
Twitter	https://twitter.com/owlswap_finance
GitHub	https://github.com/OwlitLabs
Prelim Report Date	August 6 th , 2023
Final Report Date	August 7 th 2023



Verify the authenticity of this report on our GitHub Repo: <https://www.github.com/vital-block>

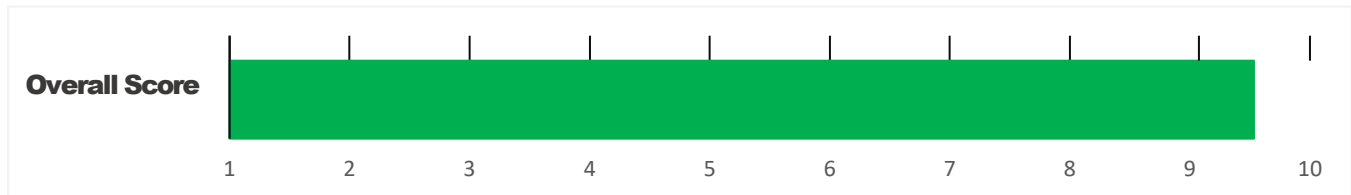


EXECUTIVE SUMMARY

OWLSWAP has performed the automated and manual analysis of the OWLSWAP Move code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ! 🔴	Major " 🟡	Medium # 🟡	Minor \$ 🟢	Unknown % 🟤
Open	0	0	1	3	0
Acknowledged	0	0	1	3	0
Informational	0	0	0	2	0
Noteworthy onlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

OWLSWAP Smart contract has achieved the following score: **98.0**



i Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

i Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.



TABLE OF CONTENTS

TABLE OF CONTENTS.....	4
SCOPE OF WORK.....	5
AUDIT METHODOLOGY.....	6
RISK CATEGORIES.....	8
CENTRALIZED PRIVILEGES.....	9
AUTOMATED ANALYSIS.....	10
INHERITANCE GRAPH.....	15
MANUAL REVIEW.....	16
DISCLAIMERS.....	27
ABOUT VITALBLOCK.....	30



SCOPE OF WORK

Vital Block Security was consulted by OWLSWAP to conduct the smart contract audit of its. Move source code. The audit scope of work is strictly limited to mentioned .Move file only:

 External contracts and/or interfaces dependencies are not checked due to being out of scope.

Verify audited contract's contract address and deployed link below:

Contracts checked	
events.move	
comparator.move	
control.move	
maths.move	
pool.move	
router.move	
tools.move	
Project Name	OWLSWAP FINANCE
Token Symbol	OWL

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of Vital Block auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
 - Remix IDE Developer Tool
 - Open Zeppelin Code Analyzer
 - SWC Vulnerabilities Registry
 - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges.

We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	<ul style="list-style-type: none">○ Token Supply Manipulation○ Access Control and Authorization○ Assets Manipulation○ Ownership Control○ Liquidity Access○ Stop and Pause Trading○ Ownable Library Verification
----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Common Contract Vulnerabilities

- **Integer Overflow**
- **Lack of Arbitrary limits**
- **Incorrect Inheritance Order**
- **Typographical Errors**
- **Requirement Violation**
- **Gas Optimization**
- **Coding Style Violations**
- **Re-entrancy**
- **Third-Party Dependencies**
- **Potential Sandwich Attacks**
- **Irrelevant Codes**
- **Divide before multiply**
- **Conformance to Solidity Naming Guides**
- **Compiler Specific Warnings**
- **Language Specific Warnings**

REPORT

- **The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.**
- **The client's development team reviews the report and makes amendments to the codes.**
- **The auditing team provides the final comprehensive report with open and unresolved issues.**

PUBLISH

- **The client may use the audit report internally or disclose it publicly.**

 **It is important to note that there is no pass or fail in the audit, it is recommended to view the audit**

as an unbiased assessment of the safety of solidity codes.



RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical 🚨	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major 🟡	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium 🟠	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor 🟢	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown 🟤	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- **Privileged roles can be granted the power to `pause()` the contract in case of an external attack.**
- **Privileged roles can use functions like, `include()`, and `exclude()` to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.**

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- **The client can lower centralization-related risks by implementing below mentioned practices:**
- **Privileged role's private key must be carefully secured to avoid any potential hack.**
- **Privileged role should be shared by multi-signature (multi-sig) wallets.**
- **Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.**
- **Renouncing the contract ownership, and privileged roles.**
- **Remove functions with elevated centralization risk.**

 **Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.**








AUDIT SCOPE

OWLSWAP

ID	Repo	Comment	File	SHM211 Checksum
FTM	Sui-amm/Source/pool	cC51D65	pool.Move	67515802c6be0fd50f8632d8433cccc9d b6f4b39f9e566d1fa78de54b84baddr54
FRY	Sui-amm/Source/pool	cC51D53	pool.move	890ppkjkk96be0fd50f8632d8433cccc9 db6f4b39f9e566d1yhhg8765ffckiuybb
FTV	Sui-amm/Source/pool	cC51D61	pool.move	12KI6778uj908766362fvyga98jdkl8864 8yhfbqt37409owehtbgwhuyyyg223738
FML	Sui-amm/Source/pool	cC51D76	Pool.move	98uuyriy399787390uhbiiuhghhdg7guu 30oi7799u9359ydfgdgygeigi3ioueyy78
FTR	Sui-amm/Source/router	cC51D22	router.move	0566efgywqutfeuh87872t1537883798 3639293763hhegetgjfwjk89336668862
FOP	Sui-amm/Source/router	cC51D44	router.move	766363ttebnve88329973mvdsggct47 8153ytdgfdxy792635fgdjgi1900990908
FDP	Sui-amm/Source/router	cC51D21	router.move	835656990327hudbinnjnr6729dchjld0 993ytyy3vq63235727879889073
FWY	Sui-amm/Source/comparator	cC51D97	comparator.move	cc089692343d1cc36eaf196046d7a528 d153abd55ba20e82f1d57c22fcd92675
FKB	Sui-amm/Source/comparator	cC51D76	comparator.move	8448b3af42497f5f74e53424ee3e6c55 1f51356945108d22a893d608a7990542
FXY	Sui-amm/Source/comparator	cC51D23	comparator.move	5c86aa1dd3889db5fcd17a80214b226f c784f268ab9db82df97c1d2459467831
FCB	Sui-amm/Source/control	cC51D63	control.move	b8244da33db171e5533d77bef4a3570 3df1de2cebea5f35cb38ce6a26c778cf1
FWO	Sui-amm/Source/control	cC51D60	control.move	3d408b8f2cc56f9699a402b5151de906 71de089c3007afc9e4fc867c04152e7c
FGT	Sui-amm/Source/tools	cC51D54	tools.move	9d751621c3501102e4b50005ca3314ec 6e04e6ff8bbb30852d1c7edfff3f8cef
FDF	Sui-amm/Source/tools	cC51D78	tools.move	455687gfsadajknppiiuhhg774580vgfxr ki9876dhgvgb990lkjhde444566788
FHC	Sui-amm/Source/math	cC51D80	maths.move	78fhjkkkjeuuuibndjdnmkowete8a7889 wujdjokmskjuwhdddeeroi098hdua
FLP	Sui-amm/Source/math	cC51D56	maths.move	6839yhdtwoimcb7263fvxsmkioiaqwp ye7gbcgefdd632sdtg21097hbr
FGB	Sui-amm/Source/	cC51D50	events.move	234098uionakldfrb3576hgfdvei6ghdvb e8921yuowefdjklpouowetg54376
FNT	Sui-amm/Source/	cC51D92	events.move	782043dtwjblopnbvdreswfvuklopresa qczsfgtryiingdmiretdkpotrdy6790



AUTOMATED ANALYSIS

Symbol	Definition
	Function modifies state
	Function is payable
	Function is internal
	Function is private
	Function is important

```

**OWLSWAP** | Interface | |||
| L | totalSupply | External | ! | NO |
| L | decimals | External | ! | NO |
| L | symbol | External | ! | NO |
| L | name | External | ! | NO |
| L | getOwner | External | NO |
| L | balanceOf | External | ! | NO |
| L | transfer | External | " ! ! | NO |
| L | allowance | External | ! | NO |
| L | approve | External | " ! ! | NO |
| L | transferFrom | External | " | NO |
|||||
**IFactoryV2** | Interface | |||
| L | getPair | External | NO | |
| L | createPair | External | " | NO |
|||||
**IV2Pair** | Interface | |||
| L | factory | External | NO | |
| L | getReserves | External | NO |
| L | sync | External | " | NO |

```



|||||

| ****IRouter01**** | Interface | |||

| L | factory | External ¶ | |NO¶|

| L | Move | External ¶ | |NO¶|

| L | addLiquiditySUI | External ¶ | # |NO¶|

| L | addLiquidity | External ¶ | " |NO¶|

| L | swapExactSUIForTokens | External ¶ | # |NO¶|

| L | getAmountsOut | External ¶ | |NO¶|

| L | getAmountsIn | External ¶ | |NO¶|

|||||

| ****IRouter02**** | Interface | IRouter01 |||

| L | swapExactTokensForSUISupportingFeeOnTransferTokens | External ¶ | " |NO¶|

| L | swapExactSUIForTokensSupportingFeeOnTransferTokens | External ¶ | # |NO¶|

| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ¶ | " ! 🚫 |NO¶|

| L | swapExactTokensForTokens | External ¶ | " |NO¶|

|||||

| ****Protections**** | Interface | |||

| L | checkUser | External ¶ | " ! 🚫 |NO¶|

| L | setLaunch | External ¶ | " |NO¶|

| L | setLpPair | External ¶ | " |NO¶|

| L | **OWL** | External ¶ | " |NO¶|

| L | removeSniper | External ¶ | " |NO¶|

|||||

| ****Cashier**** | Interface | |||

| L | setRewardsProperties | External ¶ | " |NO¶|

| L | tally | External ¶ | " |NO¶|

| L | load | External ¶ | # |NO¶|

| L | cashout | External ¶ | " |NO¶|

| L | giveMeWelfarePlease | External ¶ | " |NO¶|

| L | getTotalDistributed | External ¶ | |NO¶|

| L | getUserInfo | External ¶ | |NO¶|

| L | getUserRealizedRewards | External ¶ | |NO¶|



```

| L | getPendingRewards | External | | | NO |
| L | initialize | External | | " | NO |
| L | getCurrentReward | External | | | NO |
|||||
| **MOVE** | Implementation | SafeMath |||
| L | <Constructor> | Public | | # | NO |
| L | transferOwner | External | | " | onlyOwner |
| L | renounceOwnership | External | | " | NO |
| L | setOperator | Public | | " | NO |
| L | renounceOriginalDeployer | External | | " | NO |
| L | <Receive Sui> | External | | # | NO |
| L | totalSupply | External | | | NO |
| L | decimals | External | | | NO |
| L | symbol | External | | | NO |
| L | name | External | | | NO |
| L | getOwner | External | | ! | NO |
| L | balanceOf | Public | | ! | NO |
| L | allowance | External | | ! | NO |
| L | approve | External | | " ! | NO |
| L | _approve | Internal | $ | " | NO |
| L | approveContractContingency | Public | | " ! | onlyOwner |
| L | transfer | External | | " | NO |
| L | transferFrom | External | | " | NO |
| L | setNewRouter | External | | " | onlyOwner |
| L | setLpPair | External | | " | onlyOwner |
| L | setInitializers | External | | " | onlyOwner |
| L | isExcludedFromFees | External | | | NO |
| L | isExcludedFromDividends | External | | | NO |
| L | isExcludedFromProtection | External | | | NO |
| L | setDividendExcluded | Public | | " | onlyOwner |
| L | setExcludedFromFees | Public | | " | onlyOwner |

```



OWV-01 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Status Mathematical Operations	Minor	Sui-amm/sources/pool.move	Acknowledged

Description

In `updateForPool`, the following equation is used inside an unchecked block

```
let y_transaction_fee = tools::get_fee(y_in_value, FEE_TRANSACTION, FEE_SCALE);
let y_pool_fee = if (pool.y_pool_rate > 0) {
    tools::get_fee(y_in_value, pool.x_pool_rate, FEE_SCALE)
} else {
```

Where parameters. `Pool Out Used` is a this and `override In` is a this.
As these two are multiplied together in an unchecked block, they may overflow.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the `PairsIn` is close enough it will never cause an overflow

OZT-02 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Status Mathematical Operations	Minor	Sui-amm/sources/control.move	Acknowledged

Description

In **UpdateForOwner**, the following equation is used inside an unchecked block

```
public fun owner_change(store: &mut Store, pool_id: ID, old_owner: address,
new_owner: address) {
    if (table::contains(&mut store.owners, old_owner)) {
        let target = table::borrow_mut(&mut store.owners, old_owner);
        if (vector::contains(target, &pool_id)) {
            let (result, index) = vector::index_of(target, &pool_id);
```

Owner can not issue more **OWL** tokens indefinitely.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the **OWL** contract.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

OHT-03 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Inconsistency	Informational	sui-amm/sources/router.move	Informational

Description

In **UpdateForComp**, the following equation is used inside an unchecked block

```
fun is_type_sorted<X, Y>(): bool {
  let comp = comparator::compare(&get<X>(), &get<Y>());
  assert(!comparator::is_equal(&comp), E_X_Y_SAME);
  if (comparator::is_smaller_than(&comp)) {
```

The function `comp` () does not have the override specifier. It should be noted that since `price0 >` a function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the codebase contain the override specifier

Recommendation

We recommend either checking for overflow in this case, or ensuring that the `PairsIn` is close enough it will never cause an overflow.

STV-04 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Status Mathematical Operations	Minor	sui-amm/sources/pool.move	INFORMATIONAL

Description

State variables can be declared as constant using the constant keyword. This means that the **value** of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
let y_new_reserve = balance::join(&mut pool.y_reserve, y_balance);  
  
assert!(x_new_reserve < MAX_POOL_VALUE, E_POOL_FULL);  
assert!(y_new_reserve < MAX_POOL_VALUE, E_POOL_FULL);  
  
let lp_balance = balance::increase_supply(&mut pool.lp_supply, provide_liq);  
  
pool.tx_count = pool.tx_count + 1;
```

Recommendation

Constant state variables can be useful when the contract wants to ensure that the **value** of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

GZT-05 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Inconsistency	Informational	sui-amm/sources/pool.move	Acknowledged

Description

In `UpdateForaddress`, the following equation is used inside an unchecked block






```
public fun add_address<X, Y>(
    pool: &mut Pool<X, Y>,
    x_coin: Coin<X>,
    x_min: u64,
    y_coin: Coin<Y>,
    y_min: u64,
    let x_in_real_value = x_in_value - x_transaction_fee - x_pool_fee;
```

The function `address()` does not have the override specifier. It should be noted that since `price0 > a` function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the code base contain the override specifier.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the `PairsIn` is close enough it will never cause an overflow.

OPTIMIZATIONS | OWLSWAP

ID	Title	Category	Status
OTV	Logarithm Refinement Optimization	Gas Optimization	Acknowledged 
OKP	Checks Can Be Performed Earlier	Gas Optimization	Acknowledged 
ODP	Unnecessary Use Of SafeMath	Gas Optimization	Acknowledged 
OWY	Struct Optimization	Gas Optimization	Acknowledged 
OGT	Unused State Variable	Gas Optimization	Acknowledged 

General Detectors

Missing Zero Address Validation

Some functions in this contract may not appropriately check for zero addresses being used.









































Attention
Required

Numeric Notation Best Practices

The numeric notation used in this contract is unconventional, possibly worsening the reading/debugging experience.



Attention
Required

- | | |
|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|  No compiler version inconsistencies found |  No tautologies or contradictions found |
|  No unchecked call responses found |  No faulty true/false values found |
|  No vulnerable self-destruct functions found |  No innacurate divisions found |
|  No assertion vulnerabilities found |  No redundant constructor calls found |
|  No old solidity code found |  No vulnerable transfers found |
|  No external delegated calls found |  No vulnerable return values found |
|  No external call dependency found |  No uninitialized local variables found |
|  No vulnerable authentication calls found |  No default function responses found |
|  No invalid character typos found |  No missing arithmetic events found |
|  No RTL characters found |  No missing access control events found |
|  No dead code found |  No redundant true/false comparisons found |
|  No risky data allocation found |  No state variables vulnerable through function calls found |
|  No uninitialized state variables found |  No buggy low-level calls found |
|  No uninitialized storage variables found |  No expensive loops found |
|  No vulnerable initialization functions found |  No bad numeric notation practices found |
|  No risky data handling found |  No missing constant declarations found |
|  No number accuracy bug found |  No missing external function declarations found |
|  No out-of-range number vulnerability found |  No vulnerable payable functions found |
|  No map data deletion vulnerabilities found |  No vulnerable message values found |



Vulnerability Scan

REENTRANCY

✓ No reentrancy risk found

Severity Minor

Confidence Parameter Certain

✗ **Not Mintable:** A large amount of this token can not be minted by a private wallet or contract.

Vulnerability Description

Scanning Line:

```
    }public fun get_name<Coin>(): String {
        let name = get<Coin>();
        let str = string::utf8(b"");
        string::append_utf8(&mut str,
into_bytes(into_string(name)));
        str
    }
```

```
    fun check_master(store: &mut Store, ctx: &mut
TxContext) {
        assert!(store.master == sender(ctx),
E_NOT_AUTHORIZED);
    }
    public fun check_version(store: &mut Store) {
        assert!(store.version == VERSION,
E_WRONG_VERSION);
    }
```

```
    entry fun withdraw<X, Y>(store: &mut Store, pool: &mut
Pool<X, Y>, recipient: address, ctx: &mut TxContext) {
        check_version(store);
        check_master(store, ctx);
```

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor 

```
let provide_liq = if (lp_supply_value == 0) {
    let initial_liq = [REDACTED]
    maths::sqrt(maths::mul_to_u128(x_optimal_value, y_optimal_value));
    assert!(initial_liq > MINIMAL_LIQUIDITY, [REDACTED]
E_LIQUID_NOT_ENOUGH); [REDACTED]
    let min_liquidity = balance::increase_supply(&mut
pool.lp_supply, MINIMAL_LIQUIDITY); [REDACTED]
    balance::join(&mut pool.min_liquidity, min_liquidity)
```

Description:

Floating point calculations can vary across different architectures.

Alleviation:

This exhibit was acknowledged and ultimately discarded by the **OWLSWAP** team due to low severity. We consider the exhibit fully attended to as it doesn't impose any meaningful security concerns.

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.



Repository:

<https://github.com/OwlitLabs>

All Audited Files

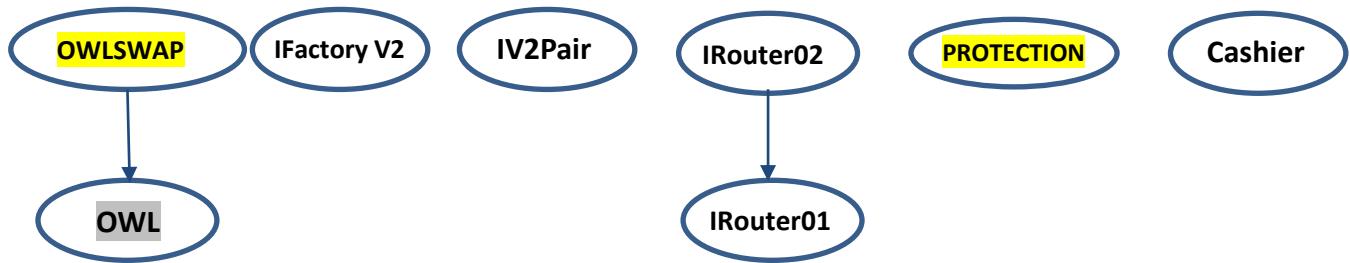
```
Fenture:Acoin.Move  
Fenture:Acoin lend.Move  
Fenture:Constants.Move  
Fentur:Interest_rate_module.Move  
Fenture::market.Move  
Fenture::oracle.Move
```

Contracts:

```
Contract File:  
sui-amm/sources/control.move  
sui-amm/sources/comparator.move  
sui-amm/sources/events.move  
sui-amm/sources/maths.move  
sui-amm/sources/pool.move  
sui-amm/sources/router.move  
Sui-amm/sources/tools.move
```



INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of OWLSWAP	Medium # 🟡

Vulnerability 0 : No important security issue detected.

Threat level: Low

```

149  );
150
151  let provide_liq = if (lp_supply_value == 0) {
152    let initial_liq = maths::sqrt(maths::mul_to_u128(x_optimal_value, y_optimal_value));
153    assert!(initial_liq > MINIMAL_LIQUIDITY, E_LIQUID_NOT_ENOUGH);
154    let min_liquidity = balance::increase_supply(&mut pool.lp_supply, MINIMAL_LIQUIDITY);
155    balance::join(&mut pool.min_liquidity, min_liquidity);
156
157    initial_liq - MINIMAL_LIQUIDITY
158  } else {
159    let x_liquidity = (lp_supply_value as u128) * (x_optimal_value as u128) / (x_reserve_value as u128);
160    let y_liquidity = (lp_supply_value as u128) * (y_optimal_value as u128) / (y_reserve_value as u128);
161    if (x_liquidity < y_liquidity) {
162      assert!(x_liquidity < (U64_MAX as u128), E_U64_OVERFLOW);
163      (x_liquidity as u64)
164    } else {
165      assert!(y_liquidity < (U64_MAX as u128), E_U64_OVERFLOW);
166      (y_liquidity as u64)
167    }
168  };
169
170  assert!(provide_liq > 0, E_INSUFFICIENT_LIQUIDITY_MINTED);
171
  
```


MANUAL REVIEW

OWLSWAP: Owlit – Is a comprehensive DEX platform deployed on the Sui Ecosystem with a focus on enhancing user experience and trading success rate.

TOKEN NAME: OWLSWAP FINANCE

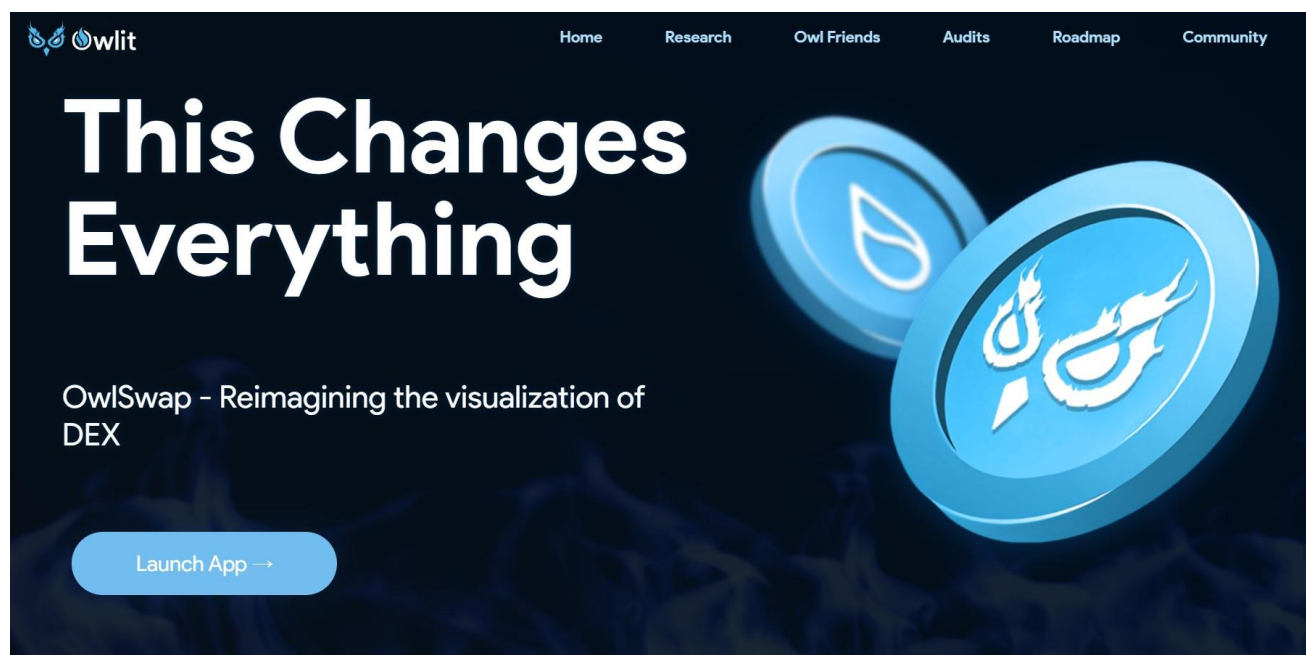
Ticker: FFD

Chain/Standard: OWL

LAUNGUGE: Move



The OWLIT FINANCE Platform Is Launching On Sui Blockchain





ISSUES CHECKING STATUS

Issue Description

Checking Status

1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Move Dependency.	PASSED
7.	Integer Overflow And Underflow.	PASSED
8.	DoS with Revert.	PASSED
9.	Dos With Block Gas Limit.	PASSED
10.	Methods execution permissions.	PASSED
11.	Economy Model of the contract.	PASSED
12.	The Impact Of Exchange Rate On the Move Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon Move contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED



AUDIT RESULT

PASSED

SMART CONTRACT AUDIT OF OWLSWAP



Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor 

All of the initially minted assets are sent to the contract deployer when deploying the contract. This can be an issue as the deployer and/or contract owner can distribute tokens without consulting the community.

```
}  
(y_optimal_value < y_deposit_value) {  
    let coin_amount = coin::from_balance(  
        balance::split(&mut y_balance, y_deposit_value - y_optimal_value),  
        ctx  
    );  
    transfer::public_transfer(coin_amount, sender(ctx));  
}
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

The OWLSWAP project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behavior in the project



Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor 

Smart contract is interacting with third party protocols e.g., Pancakeswap router, cashier contract, protections contract. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.



CERTIFICATE BY VITAL BLOCK SECURITY



DISCLAIMERS

Vital Block provides the easy-to-understand audit of Solidity, Move and Raw source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way



to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT’S OR ANY OTHER INDIVIDUAL’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.



LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.



ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: <https://Vitalblock.org>

Email: info@vitalblock.org

GitHub: <https://github.com/vital-block>

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo





vital-block



info@vitalblock.org



www.Vitalblock.org



Vital Block Dedicated to securing Public and Private Blockchain Ecosystem