CONTRACT WOLF

Blockchain Security - Smart Contract Audits

Security Assessment

April 4, 2023

Disclaimer

ContractWolf.io audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

ContractWolf does not provide any warranty on its released reports.

ContractWolf should not be used as a decision to invest into an audited project and is not affiliated nor partners to its audited contract projects.

ContractWolf provides transparent report to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

ContractWolf presence is to analyze, audit and assess the client's smart contract's code.

Each company or projects should be liable to its security flaws and functionalities.

Scope of Work

Sky Whales team agreed and provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract.

The goal of this engagement was to identify if there is a possibility of security flaws in the implementation of the contract or system.

ContractWolf will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository which has been provided by **Sky Whales**.

Description

Sky Whales is a community focused DEX empowering users with DeFi solutions that build towards innovation & sustainability to help facilitate the expansion of Arbitrum ecosystem.

Risk Level Classification

Risk Level represents the classification or the probability that a certain function or threat that can exploit vulnerability and have an impact within the system or contract.
Risk Level is computed based on CVSS Version 3.0

Level	Value	Vulnerability
Critical	9 - 10	An Exposure that can affect the contract functions in several events that can risk and disrupt the contract
High	7 - 8.9	An Exposure that can affect the outcome when using the contract that can serve as an opening in manipulating the contract in an unwanted manner
Medium	4 - 6.9	An opening that could affect the outcome in executing the contract in a specific situation
Low	0.1 - 3.9	An opening but doesn't have an impact on the functionality of the contract
Informational	0	An opening that consists of information's but will not risk or affect the contract

Auditing Approach

Every line of code along with its functionalities will undergo manual review to check its security issues, quality, and contract scope of inheritance. The manual review will be done by our team that will document any issues that there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    - Review of the specifications, sources, and instructions provided to ContractWolf to make sure we understand the size, scope, and functionality of the smart contract.
    - Manual review of code, our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities and security flaws.
2. Testing and automated analysis that includes:
    - Testing the smart contract functions with common test cases and scenarios, to ensure that it returns the expected results.
3. Best practices review, the team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security, and control within the smart contract.
4. Recommendations to help the project take steps to secure the smart contract.

Used Code from other Frameworks/Smart Contracts (Direct Imports)

Imported Packages

SkyWhalesFactory

- ISkyWhalesFactory
- SkyWhalesPair

SkyWhalesRouter02

- libraries/SkyWhalesLibrary
- libraries/SafeMath
- libraries/TransferHelper
- interfaces/ISkyWhalesRouter02
- interfaces/ISkyWhalesFactory
- interfaces/IERC20
- interfaces/IWETH

MasterWhaler

- libraries/SafeMath
- interfaces/IBEP20
- SafeBEP20
- Ownable

Sky

- BEP20

Description

Optimization enabled: No

Decimal: 18

Symbol: SKY

Max / Total Supply: 5,000,000

Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	4	4	5	0

Exposed Functions

Version	Public	Private	External	Internal
1.0	7	1	34	15

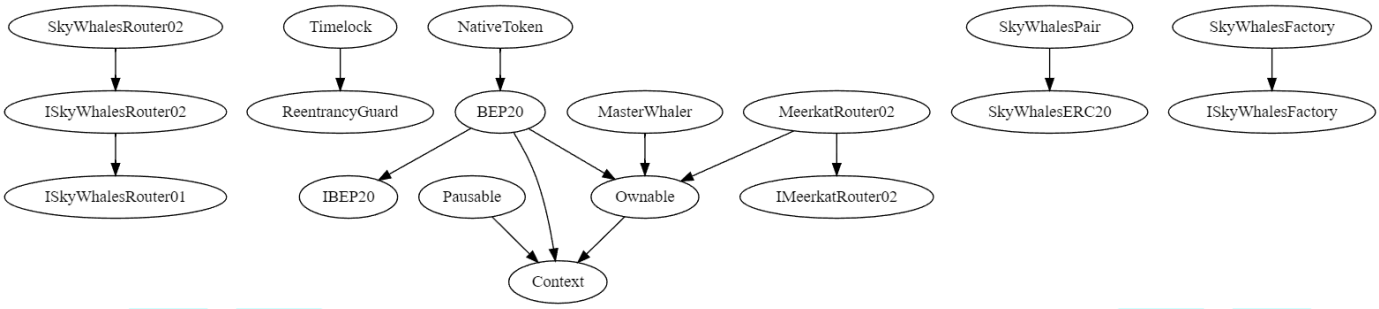
State Variables

Version	Total	Public
1.0	22	1

Capabilities

Version	Solidity Versions Observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	v0.8.0		Yes	No	No

Inheritance Graph



Correct implementation of Token Standard

Tested	Verified
✓	✓

Overall Checkup (Smart Contract Security)

Tested	Verified
✓	✓

Function	Description	Exist	Tested	Verified
TotalSupply	Information about the total coin or token supply	✓	✓	✓
BalanceOf	Details on the account balance from a specified address	✓	✓	✓
Transfer	An action that transfers a specified amount of coin or token to a specified address	✓	✓	✓
TransferFrom	An action that transfers a specified amount of coin or token from a specified address	✓	✓	✓

Approve	Provides permission to withdraw specified number of coin or token from a specified address	✓	✓	✓

Verify Claims

Statement	Exist	Tested	Owner
Renounce Ownership	✓	✓	✓
Mint	✓	✓	✓
Burn	-	-	-
Block	-	-	-
Pause	-	-	-

Legend

Attribute	Symbol
Verified / Can	✓
Verified / Cannot	✗
Unverified / Not checked	⚑
Not Available	-

Write Functions of Contract

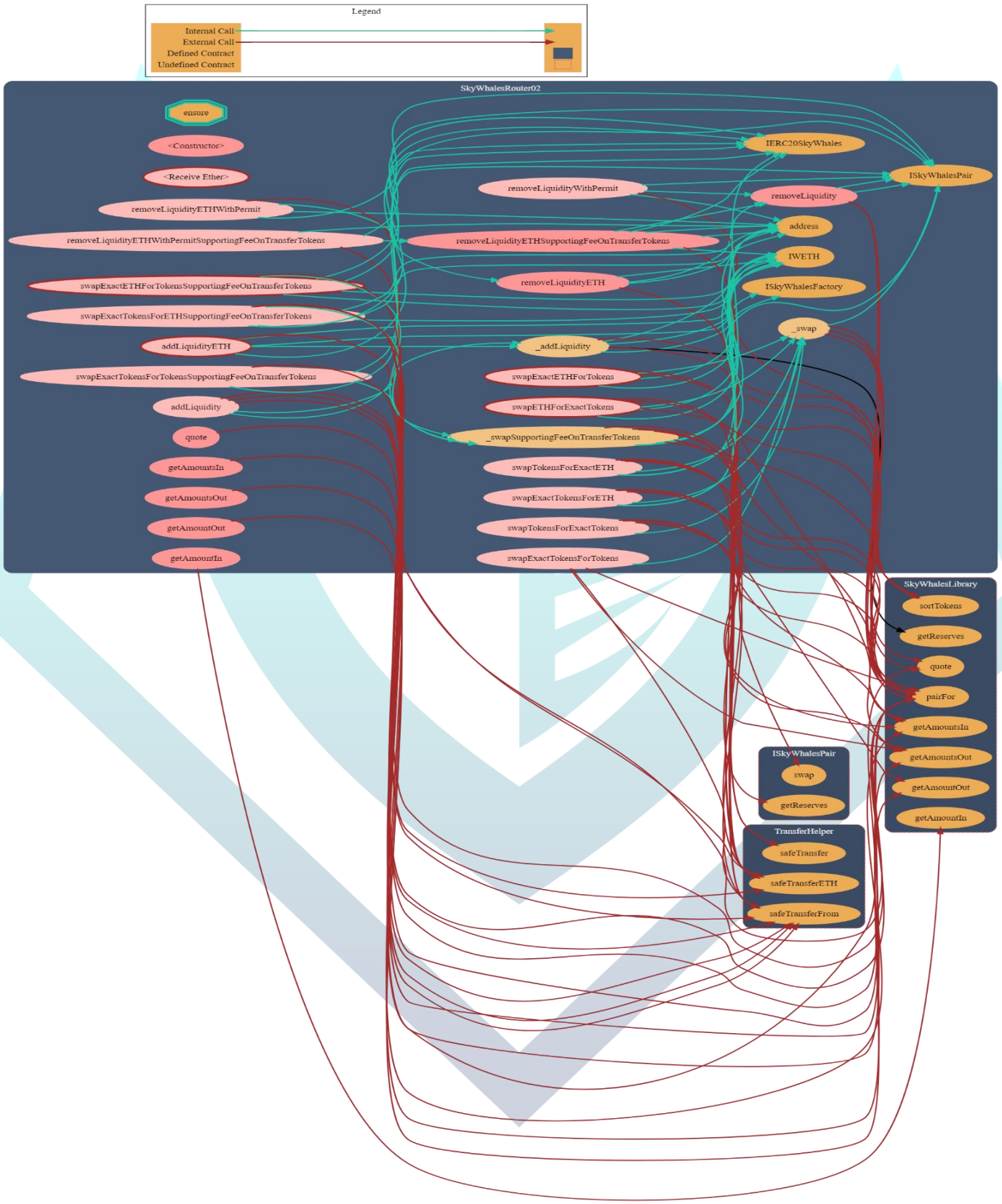
SkyWhalesRouter

1. addLiquidity (0xe8e33700)
2. addLiquidityETH (0xf305d719)
3. removeLiquidity (0xbaa2abde)
4. removeLiquidityETH (0x02751cec)
5. removeLiquidityETHSupportingFeeOnTransferTokens (0xaf2979eb)
6. removeLiquidityETHWithPermit (0xded9382a)
7. removeLiquidityETHWithPermitSupportingFeeOnTransferTokens (0x5b0d5984)
8. removeLiquidityWithPermit (0x2195995c)
9. swapETHForExactTokens (0xfb3bdb41)
10. swapExactETHForTokens (0x7ff36ab5)
11. swapExactETHForTokensSupportingFeeOnTransferTokens (0xb6f9de95)
12. swapExactTokensForETH (0x18cbafe5)
13. swapExactTokensForETHSupportingFeeOnTransferTokens (0x791ac947)
14. swapExactTokensForTokens (0x38ed1739)
15. swapExactTokensForTokensSupportingFeeOnTransferTokens (0x5c11d795)
16. swapTokensForExactETH (0x4a25d94a)
17. swapTokensForExactTokens (0x8803dbee)

Sky

1. approve (0x095ea7b3)
2. decreaseAllowance (0xa457c2d7)
3. increaseAllowance (0x39509351)
4. mint (0xa0712d68)
5. mintFor (0xda1919b3)
6. renounceOwnership (0x715018a6)
7. safeSkyTransfer (0x5c1875c3)
8. transfer (0xa9059cbb)
9. transferFrom (0x23b872dd)
10. transferOwnership (0xf2fde38b)

Call Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
SkyWhalesRouter02
ensure
<Constructor>
<Receive Ether>
removeLiquidityETHWithPermit
removeLiquidityETHWithPermitSupportingFeeOnTransferTokens
swapExactETHForTokensSupportingFeeOnTransferTokens
swapExactTokensForETHSupportingFeeOnTransferTokens
addLiquidityETH
swapExactTokensForTokensSupportingFeeOnTransferTokens
addLiquidity
quote
getAmountsIn
getAmountsOut
getAmountOut
getAmountIn
removeLiquidityWithPermit
removeLiquidityETHSupportingFeeOnTransferTokens
removeLiquidityETH
_addLiquidity
swapExactETHForTokens
swapETHForExactTokens
_swapSupportingFeeOnTransferTokens
swapTokensForExactETH
swapExactTokensForETH
swapTokensForExactTokens
swapExactTokensForTokens
IERC20SkyWhales
ISkyWhalesPair
removeLiquidity
address
IWETH
ISkyWhalesFactory
_swap
SkyWhalesLibrary
sortTokens
getReserves
quote
pairFor
getAmountsIn
getAmountsOut
getAmountOut
getAmountIn
ISkyWhalesPair
swap
getReserves
TransferHelper
safeTransfer
safeTransferETH
safeTransferFrom

SWC Attacks

ID	Title	Status
SWC-136	Unencrypted Private Data On-Chain	PASSED
SWC-135	Code With No Effects	PASSED
SWC-134	Message call with hardcoded gas amount	PASSED
SWC-133	Hash Collisions with Multiple Variable Length Arguments	PASSED
SWC-132	Unexpected Ether balance	PASSED
SWC-131	Presence of unused variables	PASSED
SWC-130	Right-To Left Override control character (U+202E)	PASSED
SWC-129	Typographical Error	PASSED
SWC-128	DoS With Block Gas Limit	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	PASSED
SWC-126	Insufficient Gas Griefing	PASSED
SWC-125	Incorrect Inheritance Order	PASSED
SWC-124	Write to Arbitrary Storage Location	PASSED
SWC-123	Requirement Violation	PASSED
SWC-122	Lack of Proper Signature Verification	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	PASSED
SWC-119	Shadowing State Variables	PASSED
SWC-118	Incorrect Constructor Name	PASSED
SWC-117	Signature Malleability	PASSED
SWC-116	Block values as a proxy for time	PASSED
SWC-115	Authorization through tx.origin	PASSED
SWC-114	Transaction Order Dependence	PASSED
SWC-113	DoS with Failed Call	PASSED
SWC-112	Delegate call to Untrusted Callee	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED

SWC-110	Assert Violation	**LOW ISSUE**
SWC-109	Uninitialized Storage Pointer	**PASSED**
SWC-108	State Variable Default Visibility	**PASSED**
SWC-107	Reentrancy	**PASSED**
SWC-106	Unprotected SELFDESTRUCT Instruction	**PASSED**
SWC-105	Unprotected Ether Withdrawal	**PASSED**
SWC-104	Unchecked Call Return Value	**PASSED**
SWC-103	Floating Pragma	**PASSED**
SWC-102	Outdated Compiler Version	**PASSED**
SWC-101	Integer Overflow and Underflow	**PASSED**
SWC-100	Function Default Visibility	**PASSED**

Audit Result

AUDIT PASSED

Low Issues

An Assertion violation was triggered(SWC-110)	SkyWhalesRouter02 L: 30

Findings

Assert Violation

```
        WETH = _WETH;
    }

    receive() external payable {
        assert(msg.sender == WETH); // only accept ETH via fallback from the WETH contract
```

Description:

Assert Violation (SWC-110)

Suggestion:

Consider whether the condition checked in the *assert()* is actually invariant. If not, replace *assert()* statement with a *require()* statement.

Additional Findings

Sky Token Contract

```
    /// @notice Creates `_amount` token to token address. Must only be called by the owner (MasterWhale).
    function mint(uint256 _amount) public override onlyOwner returns (bool) {    infinite gas
        return mintFor(address(this), _amount);
    }

    function mintFor(address _address, uint256 _amount) public onlyOwner returns (bool) {    infinite gas
        _mint(_address, _amount);
        require(totalSupply() <= maxSupply, "reach max supply");
        return true;
    }

    // Safe sky transfer function, just in case if rounding error causes pool to not have enough Sky.
    function safeSkyTransfer(address _to, uint256 _amount) public onlyOwner {    infinite gas
        uint256 skyBal = balanceOf(address(this));
        if (_amount > skyBal) {
            _transfer(address(this), _to, skyBal);
        } else {
            _transfer(address(this), _to, _amount);
        }
    }
```

Owner can mint tokens to its own address as well as to a specific address.

Audit Comments

- Owner can Mint tokens after initial deployment
- Owner can transfer and renounce contract ownership
- Owner can change SKY token generation/mint per second via function "*changeEmissions*"
- Owner cannot pause the trading
- Owner cannot block users
- Token Contract does not have fees/taxes
- Max transaction amount cannot be changed

CONTRACTWOLF

Blockchain Security - Smart Contract Audits