



# Smart Contract Audit

FOR  
SPYRO

DATED : 19 Feb, 2024



# AUDIT SUMMARY

---

**Project name – SPYRO**

**Date:** 19 Feb, 2024

**Scope of Audit-** Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

**Audit Status:** **Passed**

## Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	1	3
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

---

# USED TOOLS

---

## Tools:

### 1- Manual Review:

A line by line code review has been performed by audit ace team.

**2- BSC Test Network:** All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

### 3- Slither :

The code has undergone static analysis using Slither.

### Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/address/0x6e2826dc9e6b493c6470625e470c47d337b31e09#code>

---



# Token Information

---

**Token Name :** SPYRO

**Token Symbol:** SPYRO

**Decimals:** 18

**Token Supply:** 10000000000

**Network:** Binance smart chain

**Token Type:** BEP-20

**Token Address:**

0x2028b0E38B466bE7F9151C3129b6A2d6cbDB2890

**Checksum:**

A2032c616934aeb47e6039f76b20d331

**Owner:**

0x963CCE342409b588A76678b0aC4e1159b6A88498  
(at time of writing the audit)

**Deployer:**

0x963CCE342409b588A76678b0aC4e1159b6A88498

---



# TOKEN OVERVIEW

---

## **Fees:**

**Sell Tax: 3%**

**Marketing Tax: 3%**

---

**Fees Privilege: Owner**

---

**Ownership: Owned**

---

**Minting: None**

---

**Max Tx Amount/ Max Wallet Amount: No**

---

**Blacklist: No**

---



# AUDIT METHODOLOGY

---

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
  - Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
  - Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
  - Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
  - Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
  - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-



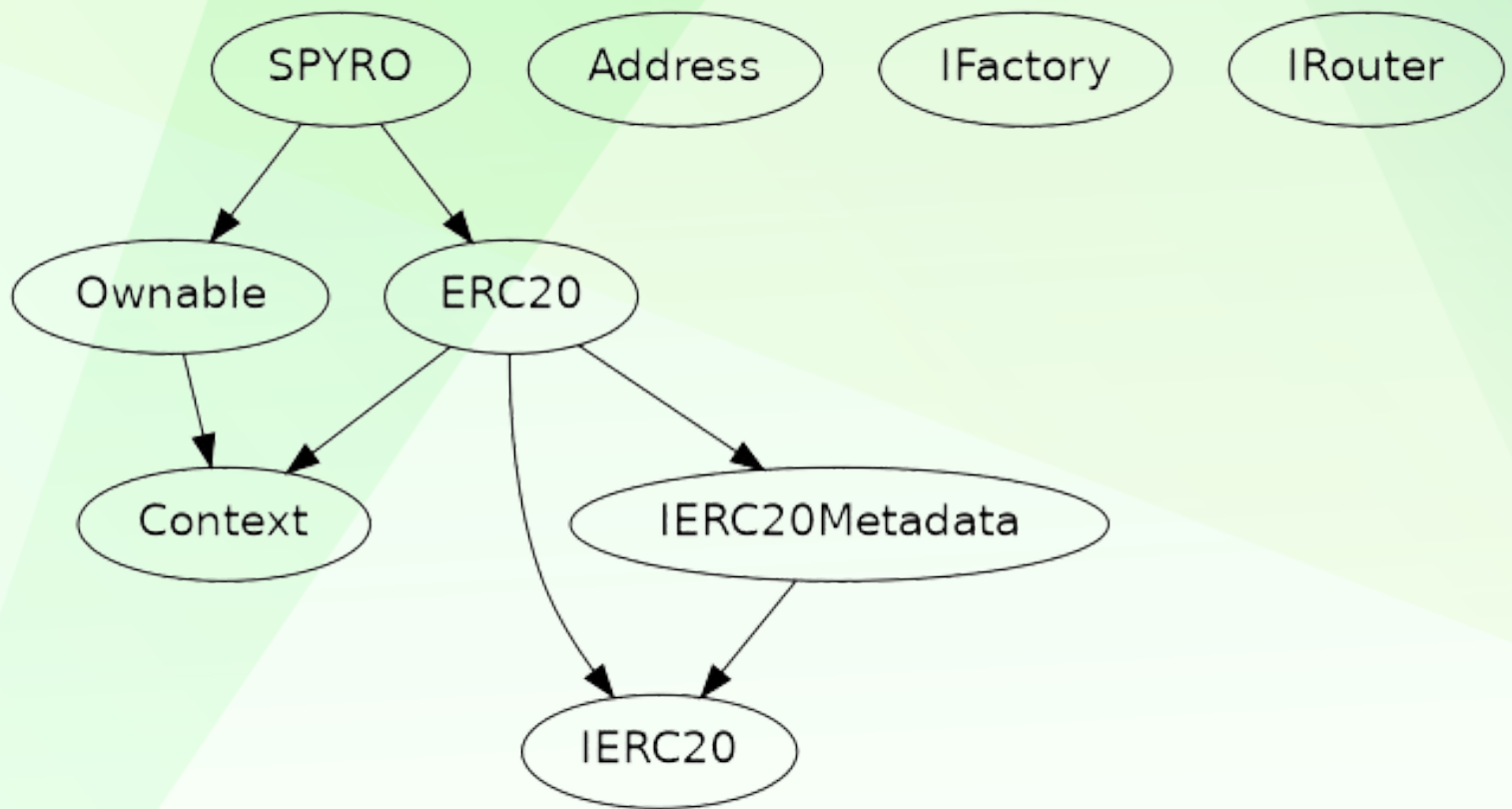
# VULNERABILITY CHECKLIST

---

- |                                    |                               |
|------------------------------------|-------------------------------|
| ✓ Return values of low-level calls | ✓ <b>Gasless Send</b>         |
| ✓ Private modifier                 | ✓ Using block.timestamp       |
| ✓ Multiple Sends                   | ✓ Re-entrancy                 |
| ✓ Using Suicide                    | ✓ Tautology or contradiction  |
| ✓ Gas Limitand Loops               | ✓ Timestamp Dependence        |
| ✓ Address hardcoded                | ✓ Revert/require functions    |
| ✓ Exception Disorder               | ✓ Use of tx.origin            |
| ✓ Using inline assembly            | ✓ Integer overflow/underflow  |
| ✓ Divide before multiply           | ✓ Dangerous strict equalities |
| ✓ Missing Zero Address Validation  | ✓ Using SHA3                  |
| ✓ Compiler version not fixed       | ✓ Using throw                 |
-

# INHERITANCE TREE

---







# STATIC ANALYSIS

A static analysis of the code was performed using Slither.  
No issues were found.

```
INFO:Detectors:
SPYRO.Liquify(uint256,SPYRO.Taxes) (SPYRO.sol#614-653) performs a multiplication on the result of a division:
- unitBalance = deltaBalance / (denominator - swapTaxes.liquidity) (SPYRO.sol#635)
- ethToAddLiquidityWith = unitBalance * swapTaxes.liquidity (SPYRO.sol#636)
SPYRO.Liquify(uint256,SPYRO.Taxes) (SPYRO.sol#614-653) performs a multiplication on the result of a division:
- unitBalance = deltaBalance / (denominator - swapTaxes.liquidity) (SPYRO.sol#635)
- marketingbAmt = unitBalance * 2 * swapTaxes.marketingb (SPYRO.sol#643)
SPYRO.Liquify(uint256,SPYRO.Taxes) (SPYRO.sol#614-653) performs a multiplication on the result of a division:
- unitBalance = deltaBalance / (denominator - swapTaxes.liquidity) (SPYRO.sol#635)
- devbAmt = unitBalance * 2 * swapTaxes.devb (SPYRO.sol#648)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
SPYRO._transfer(address,address,uint256).feesum (SPYRO.sol#578) is a local variable never initialized
SPYRO._transfer(address,address,uint256).feeswap (SPYRO.sol#569) is a local variable never initialized
SPYRO._transfer(address,address,uint256).currentTaxes (SPYRO.sol#572) is a local variable never initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-local-variables
INFO:Detectors:
SPYRO.addLiquidity(uint256,uint256) (SPYRO.sol#673-686) ignores return value by router.addLiquidityETH(value: ethAmount)(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (SPYRO.sol#678-685)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
SPYRO._transfer(address,address,uint256).fee (SPYRO.sol#571) is written in both
fee = 0 (SPYRO.sol#588)
fee = (amount * feesum) / 100 (SPYRO.sol#596)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#write-after-write
INFO:Detectors:
SPYRO.updateLiquidityThreshold(uint256) (SPYRO.sol#692-696) should emit an event for:
- tokenLiquidityThreshold = new_amount * 10 ** decimals() (SPYRO.sol#695)
SPYRO.updateDeadline(uint256) (SPYRO.sol#785-789) should emit an event for:
- deadline = _deadline (SPYRO.sol#788)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-arithmetic
INFO:Detectors:
Modifier SPYRO.lockTheSwap() (SPYRO.sol#472-478) does not always execute _; or revertReference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-modifier
```

```
INFO:Detectors:
Modifier SPYRO.lockTheSwap() (SPYRO.sol#472-478) does not always execute _; or revertReference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-modifier
INFO:Detectors:
Reentrancy in SPYRO.Liquify(uint256,SPYRO.Taxes) (SPYRO.sol#614-653):
External calls:
- swapTokensForETH(toSwap) (SPYRO.sol#632)
- router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (SPYRO.sol#664-679)
- addLiquidity(tokensToAddLiquidityWith,ethToAddLiquidityWith) (SPYRO.sol#640)
- router.addLiquidityETH(value: ethAmount)(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (SPYRO.sol#678-685)
External calls sending eth:
- addLiquidity(tokensToAddLiquidityWith,ethToAddLiquidityWith) (SPYRO.sol#640)
- router.addLiquidityETH(value: ethAmount)(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (SPYRO.sol#678-685)
State variables written after the call(s):
- addLiquidity(tokensToAddLiquidityWith,ethToAddLiquidityWith) (SPYRO.sol#640)
- _allowances[owner][spender] = amount (SPYRO.sol#345)
Reentrancy in SPYRO.transferFrom(address,address,uint256) (SPYRO.sol#507-522):
External calls:
- _transfer(sender,recipient,amount) (SPYRO.sol#512)
- router.addLiquidityETH(value: ethAmount)(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (SPYRO.sol#678-685)
- (success) = recipient.call{value: amount}() (SPYRO.sol#357)
- router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (SPYRO.sol#664-679)
- address(marketingbWallet).sendValue(marketingbAmt) (SPYRO.sol#645)
- address(devbWallet).sendValue(devbAmt) (SPYRO.sol#650)
External calls sending eth:
- _transfer(sender,recipient,amount) (SPYRO.sol#512)
- router.addLiquidityETH(value: ethAmount)(address(this),tokenAmount,0,0,deadWallet,block.timestamp) (SPYRO.sol#678-685)
- (success) = recipient.call{value: amount}() (SPYRO.sol#357)
State variables written after the call(s):
- _approve(sender,_msgSender(),currentAllowance - amount) (SPYRO.sol#519)
- _allowances[owner][spender] = amount (SPYRO.sol#345)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
```



# STATIC ANALYSIS

```
INFO:Detectors:
Context._msgData() (SPYRO.sol#15-18) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.19 (SPYRO.sol#8) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (SPYRO.sol#351-362):
  - (success) = recipient.call{value: amount}() (SPYRO.sol#357)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IRouter.WETH() (SPYRO.sol#414) is not in mixedCase
Function SPYRO.Liquify(uint256,SPYRO.Taxes) (SPYRO.sol#614-653) is not in mixedCase
Parameter SPYRO.updateLiquidityTreshhold(uint256).new_amount (SPYRO.sol#692) is not in mixedCase
Function SPYRO.EnableTrading() (SPYRO.sol#698-703) is not in mixedCase
Parameter SPYRO.updatedeadline(uint256)._deadline (SPYRO.sol#705) is not in mixedCase
Function SPYRO.AddExemptFee(address) (SPYRO.sol#711-713) is not in mixedCase
Parameter SPYRO.AddExemptFee(address)._address (SPYRO.sol#711) is not in mixedCase
Function SPYRO.RemoveExemptFee(address) (SPYRO.sol#715-717) is not in mixedCase
Parameter SPYRO.RemoveExemptFee(address)._address (SPYRO.sol#715) is not in mixedCase
Function SPYRO.AddbulkExemptFee(address[]) (SPYRO.sol#719-723) is not in mixedCase
Function SPYRO.RemovebulkExemptFee(address[]) (SPYRO.sol#725-729) is not in mixedCase
Variable SPYRO.genesis_block (SPYRO.sol#453) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (SPYRO.sol#16)" inContext (SPYRO.sol#18-19)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
SPYRO.devbWallet (SPYRO.sol#458) should be constant
SPYRO.launchtax (SPYRO.sol#455) should be constant
SPYRO.marketingbWallet (SPYRO.sol#457) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
SPYRO.pair (SPYRO.sol#445) should be immutable
SPYRO.router (SPYRO.sol#444) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
INFO:Slither:SPYRO.sol analyzed (9 contracts with 93 detectors), 40 result(s) found
```



# FUNCTIONAL TESTING

---

## 1- Approve (passed):

<https://testnet.bscscan.com/tx/0xf28784462951ade728219b2a5521ac450aaee88ad82e32cf1dd6000d72677b55>

## 2- Increase Allowance (passed):

<https://testnet.bscscan.com/tx/0xc920f358e25ef8978ad4814b29cb138e3ce382f1fafbde92f4fbb6e32b0d0afc>

## 3- Decrease Allowance (passed):

<https://testnet.bscscan.com/tx/0x40dca66877eb39290aeb991ab4f6040888d903c0725b9881b58d3c00345646fd>

## 4- Enable Trading (passed):

<https://testnet.bscscan.com/tx/0x5511341b6ff85b45d8797e89f2c41d76b1c48ab176f095697157c86c118a4fd7>

## 5- Add Exempt Fee (passed):

<https://testnet.bscscan.com/tx/0x9c9d05e65d11fb2daf43ce3f70fa603afdafb83a28acb78ea7898f51c089639b>

## 6- Remove Exempt Fee (passed):

<https://testnet.bscscan.com/tx/0xc6ccf031c3620f76edaf5b146e9dfe5848a07f31fb046f08024944edb2af1c21>

## 7- Transfer (passed):

<https://testnet.bscscan.com/tx/0x0e47ddb708e971caafa38363f9a1b58603c823dada6ac92dbadb3f185e59de5d>

---

# POINTS TO NOTE

---

- The owner can transfer ownership.
  - The owner can renounce ownership.
  - The owner can Enable trading only once.
  - The owner can update the liquidity threshold.
  - The owner can update the deadline.
  - The owner can add/remove the address exempt fee.
  - The owner can set a whitelist address.
  - The owner can rescue BNB.
-



# CLASSIFICATION OF RISK

## Severity

## Description

◆ Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
◆ High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
◆ Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
◆ Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
◆ Gas Optimization /Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

## Findings

### Severity

### Found

◆ Critical	0
◆ High-Risk	0
◆ Medium-Risk	0
◆ Low-Risk	1
◆ Gas Optimization / Suggestions	3

# MANUAL TESTING

---

## Centralization – Missing Events

Severity: Low

Function: Missing Events

Status: Open

### Overview:

They serve as a mechanism for emitting and recording data onto the blockchain, making it transparent and easily accessible.

```
function updateLiquidityTreshhold(uint256 new_amount) external onlyOwner {
    require(new_amount >= 1e5, "Swap threshold amount should be lower or equal
to 0.01% of tokens");
    require(new_amount <= 1e7, "Swap threshold amount should be lower or equal
to 1% of tokens");
    tokenLiquidityThreshold = new_amount * 10**decimals();
}
function updatedeadline(uint256 _deadline) external onlyOwner {
    require(!tradingEnabled, "Can't change when trading has started");
    require(_deadline < 3, "Deadline should be less than 3 Blocks");
    deadline = _deadline;
}
```





# MANUAL TESTING

---

**Optimization**

**Severity:** Informational

**Subject:** marketingwallet/devwallet

**Status:** Open

**Overview:**

```
address public marketingbWallet = 0xa03a2FF3C10c68F7578E01527A6890aBc6f11d6D; //Set
address public devbWallet = 0xa03a2FF3C10c68F7578E01527A6890aBc6f11d6D;
```

**Suggestion:**

It is recommended that marketing wallet and dev wallet is set to be constant.

# MANUAL TESTING

---

## Optimization

**Severity:** Informational

**Subject:** Floating Pragma Solidity version

**Status:** Open

### Overview:

It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

```
pragma solidity ^0.8.19;
```

### Suggestion:

Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

---





# MANUAL TESTING

---

**Optimization**

**Severity:** Optimization

**Subject:** Remove unused code

**Status:** Open

**Overview:**

Unused variables are allowed in Solidity, and they do not pose a direct security issue. It is the best practice though to avoid them.

```
function _msgData() internal view virtual returns (bytes calldata) {  
    this; // silence state mutability warning without generating bytecode - see  
    https://github.com/ethereum/solidity/issues/2691  
    return msg.data;  
}
```



# DISCLAIMER

---

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.

---



# ABOUT AUDITACE

---

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



**<https://auditace.tech/>**



**[https://t.me/Audit\\_Ace](https://t.me/Audit_Ace)**



**[https://twitter.com/auditace\\_](https://twitter.com/auditace_)**



**<https://github.com/Audit-Ace>**

---