



# Smart Contract Audit

FOR

# Penguins

DATED : 30 May 23'



# AUDIT SUMMARY

---

**Project name** – Penguins

**Date:** 30 May, 2023

**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	1	0	0
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/token/0xC5a75dfdB710DaE5AD54005CEe1d4D7dE91f74A2>

---



# Token Information

---

**Token Name :** Penguins

**Token Symbol:** PENGs

**Decimals:** 18

**Token Supply:** 100,000,000,000

**Token Address:**

0x750b3e301a649518D51872098F62e62699A7f987

**Checksum:**

d9679e76c1dd84cd67a772efc39be975cac44134

**Owner:**

0x39C4b04Afbf89630C7061Dd1c7001B4CCfB227c1  
(at time of writing the audit)

**Deployer:**

0x39C4b04Afbf89630C7061Dd1c7001B4CCfB227c1

---



# TOKEN OVERVIEW

---

## **Fees:**

Buy Fees: 0%

Sell Fees: 0%

Transfer Fees: 0%

---

**Fees Privilege:** Static Fees

---

**Ownership:** 0x39C4b04Afbf89630C7061Dd1c7001B4CCfB227c1

---

**Minting:** No mint function

---

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

---

**Blacklist:** No

---

**Other Privileges:** Initial distribution of the tokens

---



# 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 | ✓ Gasless Send                |
| ✓ 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                 |
-



# 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

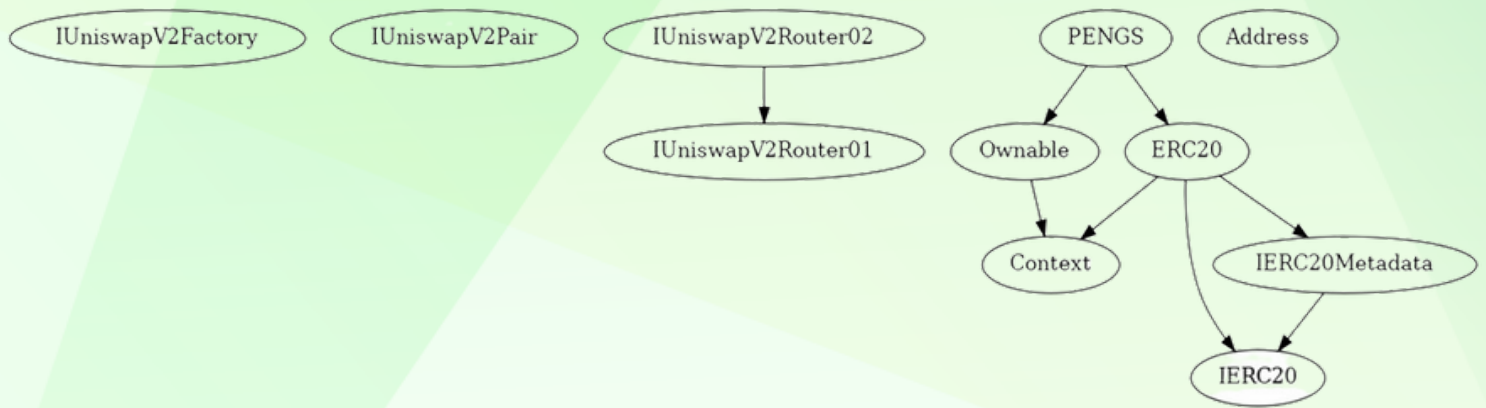
### Found

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



# INHERITANCE TREE

---





# POINTS TO NOTE

---

- **Owner is not able to change buy/sell/transfer fees (0% static)**
  - Owner is not able to blacklist an arbitrary address.
  - Owner is not able to disable trades
  - Owner is not able to set max buy/sell/transfer/hold amount to 0
  - Owner is not able to mint new tokens
-



# CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
**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 !	
**IUniswapV2Pair**   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 !	
L	sync	External !		● NO !	
L	initialize	External !		● NO !	

# CONTRACT ASSESMENT

```

**IUniswapV2Router01** | Interface | |||
└─ factory | External ! | |NO ! |
└─ WETH | External ! | |NO ! |
└─ addLiquidity | External ! | ● |NO ! |
└─ addLiquidityETH | External ! | $ |NO ! |
└─ removeLiquidity | External ! | ● |NO ! |
└─ removeLiquidityETH | External ! | ● |NO ! |
└─ removeLiquidityWithPermit | External ! | ● |NO ! |
└─ removeLiquidityETHWithPermit | External ! | ● |NO ! |
└─ swapExactTokensForTokens | External ! | ● |NO ! |
└─ swapTokensForExactTokens | External ! | ● |NO ! |
└─ swapExactETHForTokens | External ! | $ |NO ! |
└─ swapTokensForExactETH | External ! | ● |NO ! |
└─ swapExactTokensForETH | External ! | ● |NO ! |
└─ swapETHForExactTokens | External ! | $ |NO ! |
└─ quote | External ! | |NO ! |
└─ getAmountOut | External ! | |NO ! |
└─ getAmountIn | External ! | |NO ! |
└─ getAmountsOut | External ! | |NO ! |
└─ getAmountsIn | External ! | |NO ! |
|||||
**IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
└─ removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
└─ removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● |NO ! |
└─ swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● |NO ! |
└─ swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | $ |NO ! |
└─ swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● |NO ! |
|||||
**IERC20** | Interface | |||
└─ totalSupply | External ! | |NO ! |
└─ balanceOf | External ! | |NO ! |
└─ transfer | External ! | ● |NO ! |
└─ allowance | External ! | |NO ! |
└─ approve | External ! | ● |NO ! |
└─ transferFrom | External ! | ● |NO ! |
|||||
**IERC20Metadata** | Interface | IERC20 |||
└─ name | External ! | |NO ! |
└─ symbol | External ! | |NO ! |
└─ decimals | External ! | |NO ! |
|||||
**Address** | Library | |||
└─ isContract | Internal 🔒 | |

```

# CONTRACT ASSESMENT

```

└─| sendValue | Internal 🔒 | ● | |
└─| functionCall | Internal 🔒 | ● | |
└─| functionCall | Internal 🔒 | ● | |
└─| functionCallWithValue | Internal 🔒 | ● | |
└─| functionCallWithValue | Internal 🔒 | ● | |
└─| functionStaticCall | Internal 🔒 | | |
└─| functionStaticCall | Internal 🔒 | | |
└─| functionDelegateCall | Internal 🔒 | ● | |
└─| functionDelegateCall | Internal 🔒 | ● | |
└─| verifyCallResultFromTarget | Internal 🔒 | | |
└─| verifyCallResult | Internal 🔒 | | |
└─| _revert | Private 🔒 | | |
|||||
**Context** | Implementation | |||
└─| _msgSender | Internal 🔒 | | |
└─| _msgData | Internal 🔒 | | |
|||||
**Ownable** | Implementation | Context |||
└─| <Constructor> | Public ! | ● | NO ! |
└─| owner | Public ! | | NO ! |
└─| renounceOwnership | Public ! | ● | onlyOwner |
└─| transferOwnership | Public ! | ● | onlyOwner |
|||||
**ERC20** | Implementation | Context, IERC20, IERC20Metadata |||
└─| <Constructor> | Public ! | ● | NO ! |
└─| name | Public ! | | NO ! |
└─| symbol | Public ! | | NO ! |
└─| decimals | Public ! | | NO ! |
└─| totalSupply | Public ! | | NO ! |
└─| balanceOf | Public ! | | NO ! |
└─| transfer | Public ! | ● | NO ! |
└─| allowance | Public ! | | NO ! |
└─| approve | Public ! | ● | NO ! |
└─| transferFrom | Public ! | ● | NO ! |
└─| increaseAllowance | Public ! | ● | NO ! |
└─| decreaseAllowance | Public ! | ● | NO ! |
└─| _transfer | Internal 🔒 | ● | |
└─| _mint | Internal 🔒 | ● | |
└─| _burn | Internal 🔒 | ● | |
└─| _approve | Internal 🔒 | ● | |
└─| _beforeTokenTransfer | Internal 🔒 | ● | |
└─| _afterTokenTransfer | Internal 🔒 | ● | |
|||||

```



# CONTRACT ASSESMENT

```
**PENGs** | Implementation | ERC20, Ownable |||
| L | <Constructor> | Public ! | ● | ERC20 |
| L | <Receive Ether> | External ! | 💰 | NO ! |
| L | claimStuckTokens | External ! | ● | onlyOwner |
| L | excludeFromFees | External ! | ● | onlyOwner |
| L | isExcludedFromFees | Public ! | | NO ! |
| L | enableTrading | External ! | ● | onlyOwner |
| L | _transfer | Internal 🔒 | ● | |
| L | setSwapEnabled | External ! | ● | onlyOwner |
| L | setSwapTokensAtAmount | External ! | ● | onlyOwner |
| L | swapAndSendMarketing | Private 🔒 | ● | |
```

## ### Legend

```
| Symbol | Meaning |
|:-----:|:-----:|
| ● | Function can modify state |
| 💰 | Function is payable |
```



# STATIC ANALYSIS

```
Address.revert(bytes,string) (contracts/Token.sol#532-547) is never used and should be removed
Address.functionCall(address,bytes) (contracts/Token.sol#391-402) is never used and should be removed
Address.functionCall(address,bytes,string) (contracts/Token.sol#404-410) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (contracts/Token.sol#412-424) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#426-446) is never used and should be removed
Address.functionDelegateCall(address,bytes) (contracts/Token.sol#475-485) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#487-500) is never used and should be removed
Address.functionStaticCall(address,bytes) (contracts/Token.sol#448-458) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#460-473) is never used and should be removed
Address.isContract(address) (contracts/Token.sol#374-376) is never used and should be removed
Address.verifyCallResult(bool,bytes,string) (contracts/Token.sol#520-530) is never used and should be removed
Address.verifyCallResultFromTarget(address,bool,bytes,string) (contracts/Token.sol#502-518) is never used and should be removed
Context.msgData() (contracts/Token.sol#555-558) is never used and should be removed
ERC20.burn(address,uint256) (contracts/Token.sol#745-760) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#6) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#378-389):
- (success) = recipient.call{value: amount}() (contracts/Token.sol#387)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#426-446):
- (success,returndata) = target.call{value: value}(data) (contracts/Token.sol#436-438)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#460-473):
- (success,returndata) = target.staticcall(data) (contracts/Token.sol#465)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#487-500):
- (success,returndata) = target.delegatecall(data) (contracts/Token.sol#492)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#68) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#70) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#101) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#141) is not in mixedCase
Parameter PENGs.setSwapEnabled(bool).enabled (contracts/Token.sol#944) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#556)" inContext (contracts/Token.sol#550-559)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#146) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#147)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

PENGs.creator (contracts/Token.sol#795) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

PENGs.marketingFeeOnBuy (contracts/Token.sol#797) should be immutable
PENGs.marketingFeeOnSell (contracts/Token.sol#798) should be immutable
PENGs.marketingWallet (contracts/Token.sol#800) should be immutable
PENGs.uniswapV2Pair (contracts/Token.sol#791) should be immutable
PENGs.uniswapV2Router (contracts/Token.sol#790) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

**Result => A static analysis of contract's source code has been performed using slither,**

**No major issues were found in the output**





# FUNCTIONAL TESTING

---

**Router (PCS V2):**

**0xD99D1c33F9fC3444f8101754aBC46c52416550D1**

**1- Adding liquidity by owner (trades disabled) (passed):**

<https://testnet.bscscan.com/tx/0xaf6b479be649fb6a1704b80497b33242ae4dacdbada389bdb5d5f432cd8db58f>

**2- Buying when excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0x45d1b6129f19ff6a19110b7f18a233a4aed2086ea7d97f1f2155cc7b52c26c47>

**3- Selling when excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0x6dd2d86f1b05e15bfbfeb786719dec3e839df8ad8225ad7b06c5cfa440ab4651>

**4- Transferring when excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0xf2cba0b78a8ca71a4f7ae9a37520b661899e25d23c34f1a78a81e2e1cc063494>

**5- Buying when not excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0x3501a84655d84fe4f91581e02f885e370cccc7d272d258629f6143e17f88f735>

**6- Selling when not excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0x985021557d5de2b89cfbec1ef9b0777b7afc51576b70bd9b8e7f6f71f1f13d34>

---





# FUNCTIONAL TESTING

---

**7- Transferring when not excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0xcaf5951342454dcc6e1569b4f9341cdc7fe7d3e4682b6410465befa29519b149>

---

# MANUAL TESTING

---

## Optimizations – Redundant code

**Impact:** Medium

**Status:** Not Resolved

### Overview:

Marketing fee for buy/sell/transfers is set to 0 (immutable), this means some functions and implementations in the contract are considered redundant and can be removed to reduce contract size and overall gas usage on trades.

### Suggestion

Functions to remove:

- swapAndSendMarketing
  - setSwapTokensAtAmount
  - setSwapEnabled
  - enableTrading
  - isExcludedFromFees
  - excludeFromFees
  - variables and code implementations related to fee and internal swap
-



# 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>**

---