



Smart Contract Audit

FOR

Baby Aliens

DATED : 30 JAN 23'



AUDIT SUMMARY

Project name – Baby Aliens

Date: 30 January , 2023

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

Audit Status: **Passed** (Contract is developed by Pinksale safu dev)

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	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 done on BSC Testnet network, each test has its transaction has attached to it. . You can check this tests in “**functionality tests**” section of the report.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

<https://testnet.bscscan.com/token/0x95f6c0f3cab303b55429a32ea580c0f69e8fe747>



Token Information

Token Name : BabyAliens

Token Symbol: BAP

Decimals: 18

Token Supply: 100,000,000,000

Token Address: Not deployed

Checksum:

4c3ff1d73018dc5a5cdd9721f536546adea313f505a8
a5f83b0a2935a19c5a85

Deployer: not deployed

Owner: not deployed



TOKEN OVERVIEW

Fees:

Buy Fees: -

Sell Fees: -

Transfer Fees: -

Fees Privilege: Owner

Ownership : Owned

Minting: No mint function

Max Tx Amount: No

Blacklist: No

Other Privileges: setting max buy & sell amounts



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

0

◆ Low-Risk

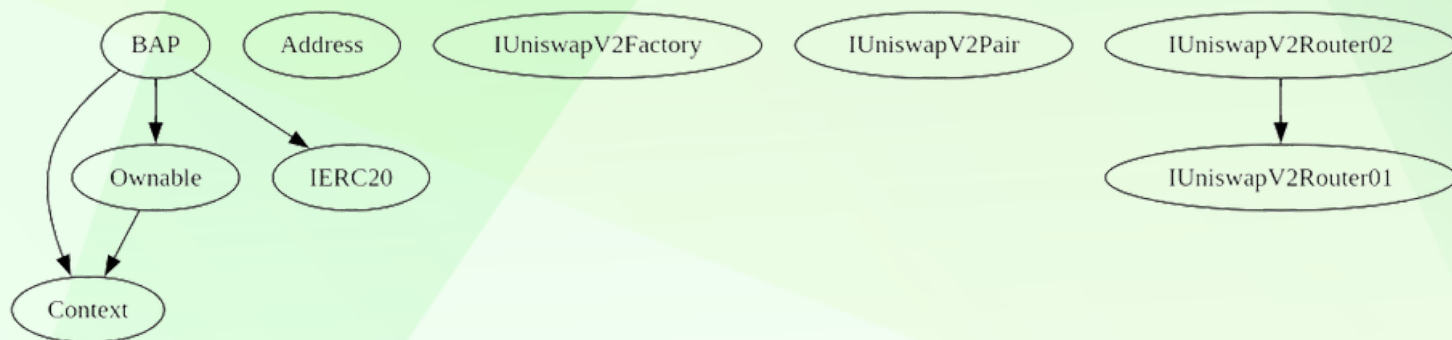
0

◆ Gas Optimization / Suggestions

0



INHERITANCE TREE





POINTS TO NOTE





















- **Owner is not able to set sell taxes over 12% and buy taxes over 8%**
 - **Owner is not able to blacklist an arbitrary wallet**
 - **Owner is not able to set max buy/sell/transfer amounts**
 - **Owner is not able to disable trades**
 - **Owner is not able to mint new tokens**
-



CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
	Context	Implementation			
L	_msgSender	Internal			
L	_msgData	Internal			
	Ownable	Implementation	Context		
L	<Constructor>	Public	!		NO !
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 !
	Address	Library			
L	isContract	Internal			
L	sendValue	Internal			
L	functionCall	Internal			
L	functionCall	Internal			
L	functionCallWithValue	Internal			
L	functionCallWithValue	Internal			
L	_functionCallWithValue	Private			
	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			

CONTRACT ASSESMENT

```
|  | name | External ! | | NO ! |
|  | symbol | External ! | | NO ! |
|  | decimals | External ! | | NO ! |
|  | totalSupply | External ! | | NO ! |
|  | balanceOf | External ! | | NO ! |
|  | allowance | External ! | | NO ! |
|  | approve | External ! |  | NO ! |
|  | transfer | External ! |  | NO ! |
|  | transferFrom | External ! |  | NO ! |
|  | DOMAIN_SEPARATOR | External ! | | NO ! |
|  | PERMIT_TYPEHASH | External ! | | NO ! |
|  | nonces | External ! | | NO ! |
|  | permit | External ! |  | NO ! |
|  | MINIMUM_LIQUIDITY | External ! | | NO ! |
|  | factory | External ! | | NO ! |
|  | token0 | External ! | | NO ! |
|  | token1 | External ! | | NO ! |
|  | getReserves | External ! | | NO ! |
|  | price0CumulativeLast | External ! | | NO ! |
|  | price1CumulativeLast | External ! | | NO ! |
|  | kLast | External ! | | NO ! |
|  | burn | External ! |  | NO ! |
|  | swap | External ! |  | NO ! |
|  | skim | External ! |  | NO ! |
|  | sync | External ! |  | NO ! |
|  | initialize | External ! |  | NO ! |
| | | |
| **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 ! |
```














































CONTRACT ASSESMENT

```

|  | 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! |
|  |  |
| **BAP** | Implementation | Context, IERC20, Ownable |  |
|  | <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! |
|  | isExcludedFromReward | Public ! | | NO! |
|  | totalReflectionDistributed | Public ! | | NO! |
|  | deliver | Public ! |  | NO! |
|  | reflectionFromToken | Public ! | | NO! |
|  | tokenFromReflection | Public ! | | NO! |
|  | excludeFromReward | Public ! |  | onlyOwner |
|  | includeInReward | External ! |  | onlyOwner |
|  | <Receive Ether> | External ! |  | NO! |
|  | claimStuckTokens | External ! |  | onlyOwner |
|  | _reflectFee | Private  |  |  |
|  | _getValues | Private  | |  |
|  | _getTValues | Private  | |  |
|  | _getRValues | Private  | |  |
|  | _getRate | Private  | |  |


```

CONTRACT ASSESMENT

^L	_getCurrentSupply	Private 			
^L	_takeLiquidity	Private 			
^L	_takeMarketing	Private 			
^L	calculateTaxFee	Private 			
^L	calculateLiquidityFee	Private 			
^L	calculateMarketingFee	Private 			
^L	removeAllFee	Private 			
^L	setBuyFee	Private 			
^L	setSellFee	Private 			
^L	isExcludedFromFee	Public 		NO 	
^L	_approve	Private 			
^L	_transfer	Private 			
^L	swapAndLiquify	Private 			
^L	swapAndSendMarketing	Private 			
^L	setSwapTokensAtAmount	External 		onlyOwner	
^L	setSwapEnabled	External 		onlyOwner	
^L	_tokenTransfer	Private 			
^L	_transferStandard	Private 			
^L	_transferToExcluded	Private 			
^L	_transferFromExcluded	Private 			
^L	_transferBothExcluded	Private 			
^L	excludeFromFees	External 		onlyOwner	
^L	changeMarketingWallet	External 		onlyOwner	
^L	setBuyFeePercentages	External 		onlyOwner	
^L	setSellFeePercentages	External 		onlyOwner	

| Symbol | Meaning |

| :-----: |-----|

|  | Function can modify state |

|  | Function is payable |



STATIC ANALYSIS

```
Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Ace_Testing_BSC.sol#117-138) is never used and should be removed
Address.functionCall(address,bytes) (contracts/Ace_Testing_BSC.sol#100-102) is never used and should be removed
Address.functionCall(address,bytes,string) (contracts/Ace_Testing_BSC.sol#104-106) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (contracts/Ace_Testing_BSC.sol#108-110) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Ace_Testing_BSC.sol#112-115) is never used and should be removed
Address.isContract(address) (contracts/Ace_Testing_BSC.sol#81-90) is never used and should be removed
Context._msgData() (contracts/Ace_Testing_BSC.sol#26-29) is never used and should be removed
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#dead-code

BAP._tTotal (contracts/Ace_Testing_BSC.sol#358) is set pre-construction with a non-constant function or state variable:
- 100_000_000_000 * (10 ** _decimals)
BAP._rTotal (contracts/Ace_Testing_BSC.sol#359) is set pre-construction with a non-constant function or state variable:
- (MAX - (MAX % _tTotal))
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#function-initializing-state

Pragma version0.8.17 (contracts/Ace_Testing_BSC.sol#19) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.17 is not recommended for deployment
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Ace_Testing_BSC.sol#92-98):
- (success) = recipient.call{value: amount}() (contracts/Ace_Testing_BSC.sol#96)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Ace_Testing_BSC.sol#117-138):
- (success,returndata) = target.call{value: weiValue}(data) (contracts/Ace_Testing_BSC.sol#121)
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Ace_Testing_BSC.sol#172) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Ace_Testing_BSC.sol#173) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Ace_Testing_BSC.sol#189) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Ace_Testing_BSC.sol#208) is not in mixedCase
Parameter BAP.calculateTaxFee(uint256)._amount (contracts/Ace_Testing_BSC.sol#634) is not in mixedCase
Parameter BAP.calculateLiquidityFee(uint256)._amount (contracts/Ace_Testing_BSC.sol#638) is not in mixedCase
Parameter BAP.calculateMarketingFee(uint256)._amount (contracts/Ace_Testing_BSC.sol#642) is not in mixedCase
Parameter BAP.setSwapEnabled(bool)._enabled (contracts/Ace_Testing_BSC.sol#781) is not in mixedCase
Parameter BAP.changeMarketingWallet(address)._marketingWallet (contracts/Ace_Testing_BSC.sol#865) is not in mixedCase
Parameter BAP.setBuyFeePercentages(uint256,uint256,uint256)._liquidityFeeonBuy (contracts/Ace_Testing_BSC.sol#872) is not in mixedCase
Parameter BAP.setBuyFeePercentages(uint256,uint256,uint256)._marketingFeeonBuy (contracts/Ace_Testing_BSC.sol#872) is not in mixedCase
Parameter BAP.setSellFeePercentages(uint256,uint256,uint256)._taxFeeonSell (contracts/Ace_Testing_BSC.sol#881) is not in mixedCase
Parameter BAP.setSellFeePercentages(uint256,uint256,uint256)._liquidityFeeonSell (contracts/Ace_Testing_BSC.sol#881) is not in mixedCase
Parameter BAP.setSellFeePercentages(uint256,uint256,uint256)._marketingFeeonSell (contracts/Ace_Testing_BSC.sol#881) is not in mixedCase
Variable BAP._taxFee (contracts/Ace_Testing_BSC.sol#371) is not in mixedCase
Variable BAP._liquidityFee (contracts/Ace_Testing_BSC.sol#372) is not in mixedCase
Variable BAP._marketingFee (contracts/Ace_Testing_BSC.sol#373) is not in mixedCase
Variable BAP.DEAD (contracts/Ace_Testing_BSC.sol#380) is not in mixedCase
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Ace_Testing_BSC.sol#27)" inContext (contracts/Ace_Testing_BSC.sol#21-30)
Reference: https://github.com/crytic/sliether/wiki/Detector-Documentation#redundant-statements
```

Result => A static analysis of contract's source code has been performed using slither, no major issues were found



FUNCTIONAL TESTING

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

0- Deploying (Passed):

<https://testnet.bscscan.com/tx/0x528c78f4ee4bdbedc8ab9815f7b2680e17a4287af795e24edd7c33cebedc0b7a>

1- Adding Liquidity (Passed):

liquidity added on Pancakeswap V2:

<https://testnet.bscscan.com/tx/0x40b1649a19395452e1e04aa4cca36128e783bbc0a2e472b9749bf4beca1e284c>

no issue were found on adding liquidity.

2- Excluding deployer's wallet from taxes (to test taxes) (Passed):

<https://testnet.bscscan.com/tx/0xc10652f51e0459f45a33dc31adf4c55a944f4c25bda207ae0936db7931117a38>

3- Setting buy and sell fees (Passed):

<https://testnet.bscscan.com/tx/0x1f3f8404485c65825d2ac773095deb7250c17b28633d7b37604ae6174e74d3c5>

<https://testnet.bscscan.com/tx/0x9a24afc5e67263d8c5111c2d0bdf047036a611dce8e568c57aa06c2cc56cdac1>



FUNCTIONAL TESTING

4- Buying from a non-whitelisted wallet (Passed):

<https://testnet.bscscan.com/tx/0x53674b43d37effbd3e8f4d38db069b186da40289c2a9595f7c212fd94aa5c04d>

8% tax applied

5- Selling from a non-whitelisted wallet (Passed):

<https://testnet.bscscan.com/tx/0xb0e3e8cf27684df16aed07752730957574d08c7f96117cf4bb6e3f6ec99fee94>

12% static tax on sells

6- Internal Swap (Passed):

taxes were swapped to BNB and sent to staking and marketing wallets:

marketing:

<https://testnet.bscscan.com/address/0x23a01037deeed9f2fd84400ae8a1d5f84a91ea16#internaltx>



MANUAL TESTING

NO ISSUES WERE FOUND





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 specializes 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://twitter.com/auditace_



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