auditace.tech

AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Humanoid AI

DATED : 28 FEB 23'

AUDIT SUMMARY

Project name – HUMANOID AI

Date: 28 February, 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's 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 Test network, each test has its transaction has attached to it.

3- Slither : Static Analysis

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

https://testnet.bscscan.com/address/0xbbA3e7028D4dC067258F7BB8EBf3d725191D860b#code

Token Information

Token Name : HUMANOID AI

Token Symbol: HUMAI

Decimals: 18

Token Supply: 100,000,000

Token Address: Not provided

Checksum:
900adda7e7785dba36e8506d52cbc16c27be1460

Owner: Not Provided

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 isexercised 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.

auditace.tech

VULNERABILITY CHECKLIST

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

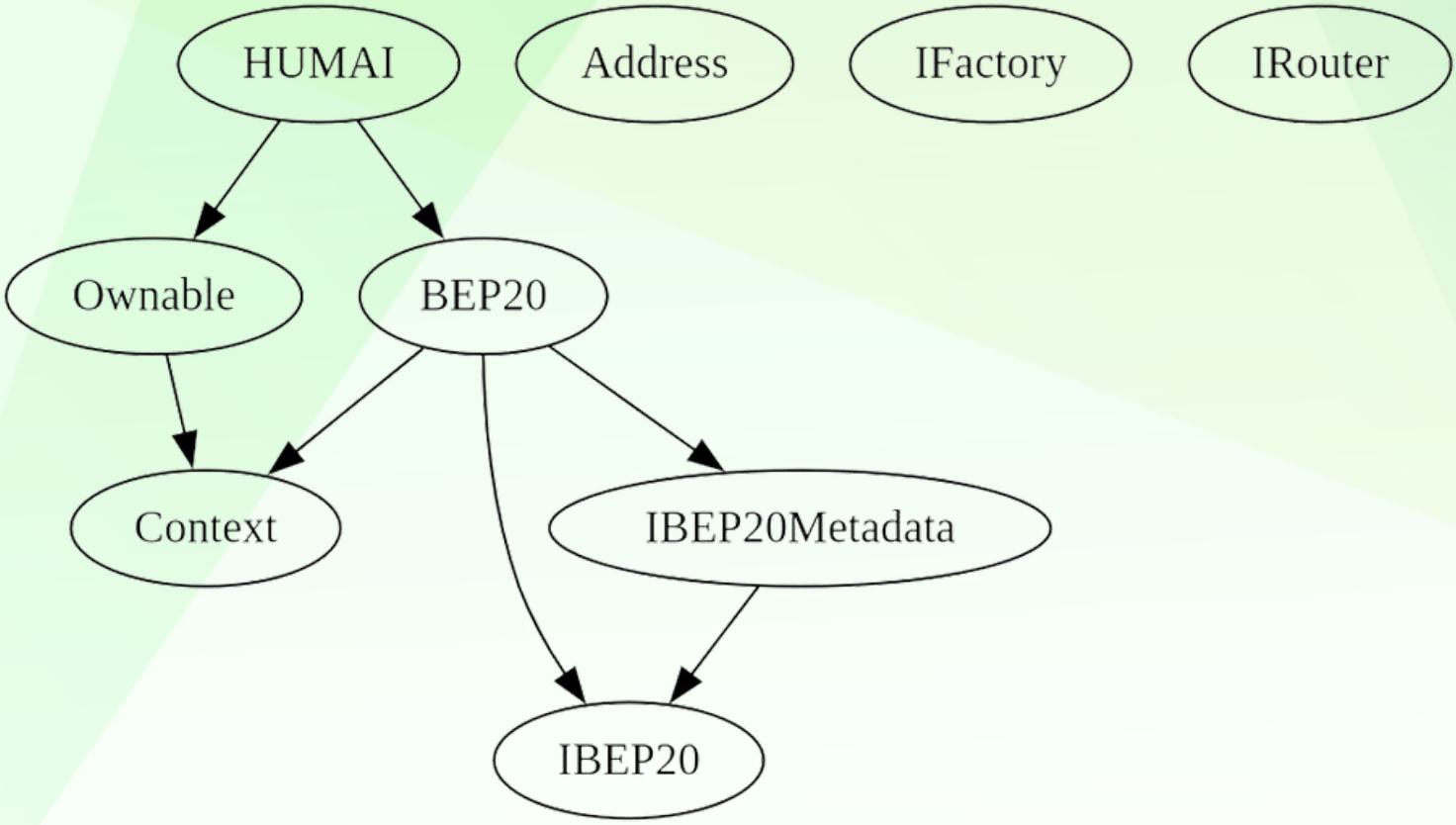
CLASSIFICATION OF RISK

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 buy/sell/transfer taxes (0% static)
- 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		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
IBEP20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IBEP20Metadata	Interface	IBEP20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
BEP20	Implementation	Context, IBEP20, IBEP20Metadata		
└	<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 🔒	🛑	
└	_tokengeneration	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
Address	Library			
└	sendValue	Internal 🔒	🛑	
Ownable	Implementation	Context		

CONTRACT ASSESMENT

└	<Constructor>	Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_setOwner	Private 🔐	🛑	
IFactory	Interface			
└	createPair	External ❗	🛑	NO❗
IRouter	Interface			
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
HUMAI	Implementation	BEP20, Ownable		
└	<Constructor>	Public ❗	🛑	BEP20
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	transfer	Public ❗	🛑	NO❗
└	_transfer	Internal 🔒	🛑	
└	EnableTrading	External ❗	🛑	onlyOwner
└	updateWhitelist	External ❗	🛑	onlyOwner
└	bulkWhitelist	External ❗	🛑	onlyOwner
└	rescueBNB	External ❗	🛑	onlyOwner
└	rescueBSC20	External ❗	🛑	onlyOwner
└	burnBSC20	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO❗

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
ue(address,uint256) (contracts/Token.sol#353-364) is never used and should be removed
() (contracts/Token.sol#29-32) is never used and should be removed
s://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

).8.17 (contracts/Token.sol#22) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
not recommended for deployment
s://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

in Address.sendValue(address,uint256) (contracts/Token.sol#353-364):
ess) = recipient.call{value: amount}() (contracts/Token.sol#359)
s://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

_balances (contracts/Token.sol#85) is not in mixedCase
_allowances (contracts/Token.sol#87) is not in mixedCase
r.WETH() (contracts/Token.sol#417) is not in mixedCase
EnableTrading() (contracts/Token.sol#526-529) is not in mixedCase
_updateWhitelist(address,bool)._address (contracts/Token.sol#531) is not in mixedCase
deadWallet (contracts/Token.sol#428-429) is not in UPPER_CASE_WITH_UNDERSCORES
s://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

ssion "this (contracts/Token.sol#30)" inContext (contracts/Token.sol#24-33)
s://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

tracts/Token.sol#424) should be immutable
ontracts/Token.sol#423) should be immutable
s://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 (Passed):
liquidity added on Pancakeswap V2:

https://testnet.bscscan.com/tx/0x14fb6f530a8935c26fdf4a3ed9a70e78fc5659188a7b19bfdbb4df5a0423c1bc

no issue were found on adding liquidity.

2- Buying (0% Tax) (Passed):

https://testnet.bscscan.com/tx/0x14fb6f530a8935c26fdf4a3ed9a70e78fc5659188a7b19bfdbb4df5a0423c1bc

3- Selling (0% Tax) (Passed):

https://testnet.bscscan.com/tx/0x8cb14d183f79ee6d4868a9469e2b8c3c40dcd8536528438e3a0f36283b0c990b

4-Transferring (0% tax)(Passed):

https://testnet.bscscan.com/tx/0x97dedddabd3c97bffe6b1498068281597dbd6ebbd0031e802b169fcf55416882

MANUAL TESTING

NO ISSUES 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