Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	Catpay Token
Website:	https://catpay.io
Platform:	Binance Smart Chain
Language:	Solidity
Date:	March 24th, 2022

Table of contents

Email: audit@EtherAuthority.io

`

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

EtherAuthority was contracted by the Catecoin team to perform the Security audit of the CatPay Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on March 24th, 2022.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

The CatPay Contract is a smart contract Having functions like set buy and sell taxes, swap And Liquify, add Liquidity, etc.

Audit scope

Name	**Code Review and Security Analysis Report for Catpay Token Smart Contract**
Platform	**BSC / Solidity**
File	catpay-whitelist.sol
File MD5 Hash	0F5D539DCC8E1391BD2039D5BCF3ECF6
Audit Date	March 24th, 2022

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: Catpay • Symbol: Catpay • Decimals: 9 • Anti Whale Amount: 500 Trillion • Swap Tokens at Amount: 20 Trillion • Maximum Sell Amount per Cycle: 500 Trillion • Anti Dump Cycle: 8 hours • Total Supply: 100 Quadrillion	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secured”**. This token contract does contain owner control, which does not make it fully decentralized.

We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 2 low and some very low level issues.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Moderated
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Moderated
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 1 smart contract file. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in Catpay Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Catpay Token.

The Catpay Token team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **not well** commented on smart contracts.

Documentation

We were given a Catpay Token smart contract code in the form of a File. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **not well** commented. So it is not easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website https://catpay.io which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	name	write	Passed	No Issue
3	symbol	write	Passed	No Issue
4	decimals	write	Passed	No Issue
5	totalSupply	read	Passed	No Issue
6	balanceOf	read	Passed	No Issue
7	transfer	write	Passed	No Issue
8	allowance	read	Passed	No Issue
9	approve	write	Passed	No Issue
10	transferFrom	write	Passed	No Issue
11	increaseAllowance	write	Passed	No Issue
12	decreaseAllowance	write	Passed	No Issue
13	isExcludedFromReward	read	Passed	No Issue
14	reflectionFromToken	read	Passed	No Issue
15	setTradingStatus	external	access only Owner	No Issue
16	tokenFromReflection	read	Passed	No Issue
17	excludeFromReward	write	access only Owner	No Issue
18	includeInReward	external	Infinite loops possibility	Refer Audit Findings
19	excludeFromFee	write	access only Owner	No Issue
20	includeInFee	write	access only Owner	No Issue
21	isExcludedFromFee	read	Passed	No Issue
22	setTaxes	write	access only Owner	No Issue
23	setBuyTaxes	write	access only Owner	No Issue
24	setSellTaxes	write	access only Owner	No Issue
25	_reflectRfi	write	Passed	No Issue
26	_takeLiquidity	write	Passed	No Issue
27	_takeMarketing	write	Passed	No Issue
28	_takeBurn	write	Passed	No Issue
29	_getValues	read	Passed	No Issue
30	_getTValues	read	Passed	No Issue
31	_getRValues	write	Passed	No Issue
32	_getRate	read	Passed	No Issue
33	_getCurrentSupply	read	Infinite loops possibility	Refer Audit Findings
34	_approve	write	Passed	No Issue
35	_transfer	write	Passed	No Issue
36	_tokenTransfer	write	Passed	No Issue
37	swapAndLiquify	write	access by lock The Swap	No Issue
38	addLiquidity	internal	Centralized risk in addLiquidity	Refer Audit Findings

39	swapTokensForBNB	write	Passed	No Issue
40	updateMarketingWallet	external	access only Owner	No Issue
41	updateAntiWhaleAmt	external	Function input parameters lack of check	Refer Audit Findings
42	updateSwapTokensAtAmount	external	Function input parameters lack of check	Refer Audit Findings
43	updateSwapEnabled	external	access only Owner	No Issue
44	setAntibot	external	access only Owner	No Issue
45	bulkAntiBot	external	Infinite loops possibility	Refer Audit Findings
46	setAllowWhitelistTrading	external	access only Owner	No Issue
47	bulkPancakeSwapWhitelist	external	Infinite loops possibility	Refer Audit Findings
48	updateRouterAndPair	external	access only Owner	No Issue
49	updateAntiDump	external	access only Owner	No Issue
50	isBot	read	Passed	No Issue
51	taxFreeTransfer	internal	Passed	No Issue
52	aidropTokens	external	Infinite loops possibility	Refer Audit Findings
53	rescueBNB	external	access only Owner	No Issue
54	rescueAnyBEP20Tokens	write	access only Owner	No Issue
55	receive	external	Passed	No Issue
56	owner	read	Passed	No Issue
57	onlyOwner	modifier	Passed	No Issue
58	renounceOwnership	write	access only Owner	No Issue
59	transferOwnership	write	access only Owner	No Issue
60	_setOwner	write	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Centralized risk in addLiquidity:

```
function addLiquidity(uint256 tokenAmount, uint256 bnbAmount) private {
    // approve token transfer to cover all possible scenarios
    _approve(address(this), address(router), tokenAmount);

    // add the liquidity
    router.addLiquidityETH{value: bnbAmount}(
        address(this),
        tokenAmount,
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        owner(),
        block.timestamp
    );
}
```

In addLiquidityETH function, the owner gets Catpay Tokens from the Pool. If the private key of the owner's wallet is compromised, then it will create a problem.

Resolution: Ideally this can be a governance smart contract. On another hand, the owner can accept this risk and handle the private key very securely.

(2) Infinite loops possibility:
As array elements will increase, then it will cost more and more gas. And eventually, it will stop all the functionality. After several hundreds of transactions, all those functions

depending on it will stop. We suggest avoiding loops. For example, use mapping to store the array index. And query that data directly, instead of looping through all the elements to find an element.

Functions are listed below:

- includeInReward
- _getCurrentSupply
- bulkAntiBot
- aidropTokens
- bulkPancakeSwapWhitelist

Resolution: Adjust logic to replace loops with mapping or other code structure.

Very Low / Informational / Best practices:

(1) Function input parameters lack of check:

Some functions require validation before execution.

Functions are:

- updateSwapTokensAtAmount
- updateAntiWhaleAmt

Resolution: We suggest using validation like variables should be greater than 0.

(2) Unused event:

```
event UpdatedRouter(address oldRouter, address newRouter);
```

UpdatedRouter event is defined but not used in code.

Resolution: We suggest removing unused events.

(3) Two variables are set with the same values:

```
address public marketingAddress = 0x000000000000000000000000000000000000dEaD;
address public constant deadAddress = 0x000000000000000000000000000000000000dEaD;
```

There are two variables "marketingAddress" and "deadAddress" set with the same values.

Resolution: We suggest set marketingAddress is different from deadAddres.

(4) Variable visibility:

```
mapping (address => bool) private _isPancakeSwapWhitelisted;
```

There is a variable "_isPancakeSwapWhitelisted" that is defined with private. User cannot confirm whether he is whitelisted or not.

Resolution: We suggest defining the variable with the "public" keyword. So each user can check his own state for whitelisted.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- setTradingStatus: The Owner can set trending status.
- excludeFromReward: The Owner can check the account is already excluded and set a reward token.
- includeInReward: The Owner can check that the account is already excluded.
- excludeFromFee: The Owner can set an exclude account address.
- includeInFee: The Owner can set an account address.
- setTaxes: The Owner can set taxes like (RFI taxes, marketing, liquidity taxes, burn taxes).
- setBuyTaxes: The Owner can set buy taxes like: RFI taxes, marketing, liquidity taxes, burn taxes.
- setSellTaxes: The Owner can set sell taxes like: RFI taxes, marketing, liquidity taxes, burn taxes.
- updateMarketingWallet: The Owner can update the marketing wallet address.
- updateAntiWhaleAmt: The Owner can update the Anti whale amount.
- updateSwapTokensAtAmount: The Owner can update swap tokens at amount.
- updateSwapEnabled: The Owner can update swap enabled status.

- setAntibot: The Owner can set the antibot address and state.
- bulkAntiBot: The Owner can bulk anti bot account addresses and state.
- setAllowWhitelistTrading: The Owner can set allow whitelist trading status.
- bulkPancakeSwapWhitelist: The Owner can set bulk pancake swap whitelist address and status.
- updateRouterAndPair: The Owner can update router address and pair address.
- updateAntiDump: The Owner can update maximum sell amount per cycle, time in minutes.
- aidropTokens: The Owner can set aidrop amount using wallet address.
- rescueBNB: The Owner can access this function when BNB are sent to the contract by mistake.
- rescueAnyBEP20Tokens: This Function to allow admin to claim *other* BEP20 tokens sent to this contract (by mistake). The Owner cannot transfer out catpay from this smart contract.

Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We have observed some issues and some of them are critical. So, **it's good to go to production**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is **"Secured"**.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

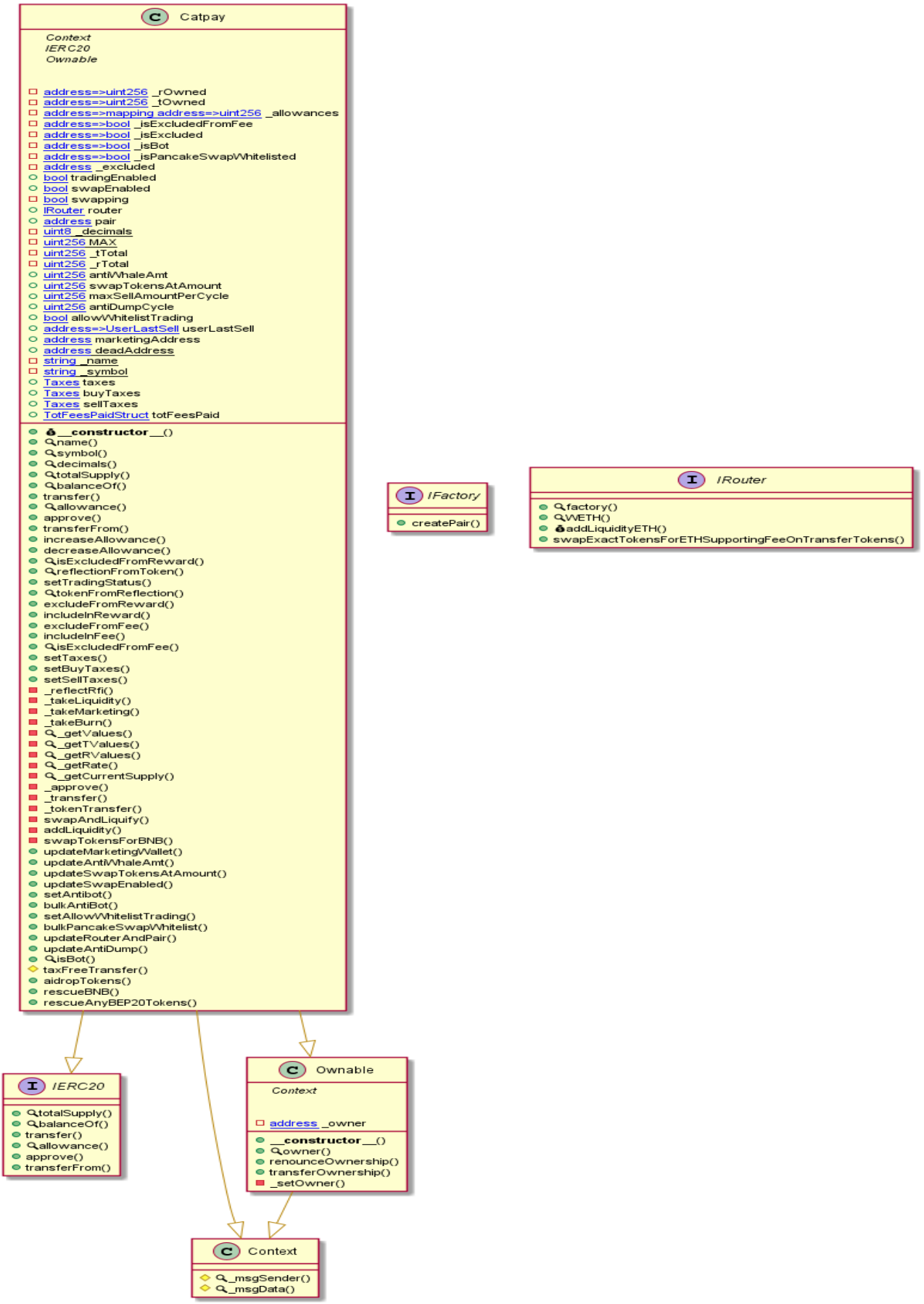
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Catpay Token



Slither Results Log

Slither log >> catpay-whitelist.sol

```
INFO:Detectors:
Catpay.addLiquidity(uint256,uint256) (catpay-whitelist.sol#544-557) sends eth to arbitrary user
        Dangerous calls:
        - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
Catpay.rescueBNB(uint256) (catpay-whitelist.sol#654-657) sends eth to arbitrary user
        Dangerous calls:
        - address(msg.sender).transfer(weiAmount) (catpay-whitelist.sol#656)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#functions-that-send-ether-to-arbitrary-destinations
INFO:Detectors:
Reentrancy in Catpay._transfer(address,address,uint256) (catpay-whitelist.sol#452-499):
        External calls:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catpay-whitelist.sol#568-574)
        External calls sending eth:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
        State variables written after the call(s):
        - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#498)
                - _rOwned[marketingAddress] += rMarketing (catpay-whitelist.sol#375)
                - _rOwned[deadAddress] += rBurn (catpay-whitelist.sol#385)
                - _rOwned[address(this)] += rLiquidity (catpay-whitelist.sol#365)
                - _rOwned[sender] = _rOwned[sender] - s.rAmount (catpay-whitelist.sol#514)
                - _rOwned[recipient] = _rOwned[recipient] + s.rTransferAmount (catpay-whitelist.sol#515)
        - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#498)
                - _rTotal -= rRfi (catpay-whitelist.sol#354)
        - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#498)
                - _tOwned[sender] = _tOwned[sender] - tAmount (catpay-whitelist.sol#508)
                - _tOwned[marketingAddress] += tMarketing (catpay-whitelist.sol#373)
                - _tOwned[deadAddress] += tBurn (catpay-whitelist.sol#383)
                - _tOwned[address(this)] += tLiquidity (catpay-whitelist.sol#363)
                - _tOwned[recipient] = _tOwned[recipient] + s.tTransferAmount (catpay-whitelist.sol#511)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities
```

```
INFO:Detectors:
Catpay.rescueAnyBEP20Tokens(address,address,uint256) (catpay-whitelist.sol#661-664) ignores return value by IERC20(_tokenAddr).transfer(_to,_amount) (catpay-whitelist.sol#663)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer
INFO:Detectors:
Catpay._transfer(address,address,uint256).category (catpay-whitelist.sol#493) is a local variable never initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-local-variables
INFO:Detectors:
Catpay.addLiquidity(uint256,uint256) (catpay-whitelist.sol#544-557) ignores return value by router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
Catpay.allowance(address,address).owner (catpay-whitelist.sol#230) shadows:
        - Ownable.owner() (catpay-whitelist.sol#46-48) (function)
Catpay._approve(address,address,uint256).owner (catpay-whitelist.sol#445) shadows:
        - Ownable.owner() (catpay-whitelist.sol#46-48) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Catpay.constructor(address)._pair (catpay-whitelist.sol#187-188) lacks a zero-check on :
                - pair = _pair (catpay-whitelist.sol#191)
Catpay.updateRouterAndPair(address,address).newPair (catpay-whitelist.sol#616) lacks a zero-check on :
                - pair = newPair (catpay-whitelist.sol#618)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in Catpay._transfer(address,address,uint256) (catpay-whitelist.sol#452-499):
        External calls:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catpay-whitelist.sol#568-574)
        External calls sending eth:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#549-556)
        State variables written after the call(s):
        - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#498)
```

```
                - totFeesPaid.burn += tBurn (catpay-whitelist.sol#379)
                - totFeesPaid.marketing += tMarketing (catpay-whitelist.sol#369)
                - totFeesPaid.liquidity += tLiquidity (catpay-whitelist.sol#359)
                - totFeesPaid.rfi += tRfi (catpay-whitelist.sol#355)
Reentrancy in Catpay.constructor(address) (catpay-whitelist.sol#185-202):
        External calls:
        - _pair = IFactory(_router.factory()).createPair(address(this),_router.WETH()) (catpay-whitelist.sol#187-188)
        State variables written after the call(s):
        - excludeFromReward(pair) (catpay-whitelist.sol#193)
                - _excluded.push(account) (catpay-whitelist.sol#296)
        - excludeFromReward(deadAddress) (catpay-whitelist.sol#194)
                - _excluded.push(account) (catpay-whitelist.sol#296)
        - excludeFromReward(pair) (catpay-whitelist.sol#193)
                - _isExcluded[account] = true (catpay-whitelist.sol#295)
        - excludeFromReward(deadAddress) (catpay-whitelist.sol#194)
                - _isExcluded[account] = true (catpay-whitelist.sol#295)
        - _isExcludedFromFee[owner()] = true (catpay-whitelist.sol#197)
        - _isExcludedFromFee[marketingAddress] = true (catpay-whitelist.sol#198)
        - _isExcludedFromFee[deadAddress] = true (catpay-whitelist.sol#199)
        - _rOwned[owner()] = _rTotal (catpay-whitelist.sol#196)
        - excludeFromReward(pair) (catpay-whitelist.sol#193)
                - _tOwned[account] = tokenFromReflection(_rOwned[account]) (catpay-whitelist.sol#293)
        - excludeFromReward(deadAddress) (catpay-whitelist.sol#194)
                - _tOwned[account] = tokenFromReflection(_rOwned[account]) (catpay-whitelist.sol#293)
        - pair = _pair (catpay-whitelist.sol#191)
        - router = _router (catpay-whitelist.sol#190)
Reentrancy in Catpay.swapAndLiquify(uint256) (catpay-whitelist.sol#534-542):
```

```
        External calls:
        - swapTokensForBNB(tokensToSwap,address(this)) (catpay-whitelist.sol#539)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catp
ay-whitelist.sol#568-574)
        - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        External calls sending eth:
        - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        State variables written after the call(s):
        - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
                - _allowances[owner][spender] = amount (catpay-whitelist.sol#448)
Reentrancy in Catpay.transferFrom(address,address,uint256) (catpay-whitelist.sol#239-247):
        External calls:
        - _transfer(sender,recipient,amount) (catpay-whitelist.sol#240)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catp
ay-whitelist.sol#568-574)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (catpay-whitelist.sol#240)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        State variables written after the call(s):
        - _approve(sender,_msgSender(),currentAllowance - amount) (catpay-whitelist.sol#244)
                - _allowances[owner][spender] = amount (catpay-whitelist.sol#448)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in Catpay._transfer(address,address,uint256) (catpay-whitelist.sol#452-499):
        External calls:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catp
ay-whitelist.sol#568-574)
```

```
        External calls sending eth:
        - swapAndLiquify(swapTokensAtAmount) (catpay-whitelist.sol#490)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        Event emitted after the call(s):
        - Transfer(sender,address(this),s.tLiquidity) (catpay-whitelist.sol#520)
                - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#4
98)
        - Transfer(sender,marketingAddress,s.tMarketing) (catpay-whitelist.sol#524)
                - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#4
98)
        - Transfer(sender,deadAddress,s.tBurn) (catpay-whitelist.sol#528)
                - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#4
98)
        - Transfer(sender,recipient,s.tTransferAmount) (catpay-whitelist.sol#530)
                - _tokenTransfer(from,to,amount,! (_isExcludedFromFee[from] || _isExcludedFromFee[to]),category) (catpay-whitelist.sol#4
98)
Reentrancy in Catpay.constructor(address) (catpay-whitelist.sol#185-202):
        External calls:
        - _pair = IFactory(_router.factory()).createPair(address(this),_router.WETH()) (catpay-whitelist.sol#187-188)
        Event emitted after the call(s):
        - Transfer(address(0),owner(),_tTotal) (catpay-whitelist.sol#201)
Reentrancy in Catpay.swapAndLiquify(uint256) (catpay-whitelist.sol#534-542):
        External calls:
        - swapTokensForBNB(tokensToSwap,address(this)) (catpay-whitelist.sol#539)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catp
ay-whitelist.sol#568-574)
        - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        External calls sending eth:
        - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        Event emitted after the call(s):
        - Approval(owner,spender,amount) (catpay-whitelist.sol#449)
                - addLiquidity(otherHalfOfTokens,newBalance) (catpay-whitelist.sol#541)
```

```
Reentrancy in Catpay.transferFrom(address,address,uint256) (catpay-whitelist.sol#239-247):
        External calls:
        - _transfer(sender,recipient,amount) (catpay-whitelist.sol#240)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
                - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(recipient),block.timestamp) (catp
ay-whitelist.sol#568-574)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (catpay-whitelist.sol#240)
                - router.addLiquidityETH{value: bnbAmount}(address(this),tokenAmount,0,0,owner(),block.timestamp) (catpay-whitelist.sol#
549-556)
        Event emitted after the call(s):
        - Approval(owner,spender,amount) (catpay-whitelist.sol#449)
                - _approve(sender,_msgSender(),currentAllowance - amount) (catpay-whitelist.sol#244)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Catpay._transfer(address,address,uint256) (catpay-whitelist.sol#452-499) uses timestamp for comparisons
        Dangerous comparisons:
        - newCycle = block.timestamp - userLastSell[from].lastSellTime >= antiDumpCycle (catpay-whitelist.sol#476)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Context._msgData() (catpay-whitelist.sol#31-34) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Catpay._rTotal (catpay-whitelist.sol#118) is set pre-construction with a non-constant function or state variable:
        - (MAX - (MAX % _tTotal))
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state-variables
INFO:Detectors:
Pragma version^0.8.4 (catpay-whitelist.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
Function IRouter.WETH() (catpay-whitelist.sol#77) is not in mixedCase
Struct Catpay.valuesFromGetValues (catpay-whitelist.sol#162-174) is not in CapWords
Parameter Catpay.setTaxes(uint256,uint256,uint256,uint256)._rfi (catpay-whitelist.sol#326) is not in mixedCase
Parameter Catpay.setTaxes(uint256,uint256,uint256,uint256)._marketing (catpay-whitelist.sol#326) is not in mixedCase
Parameter Catpay.setTaxes(uint256,uint256,uint256,uint256)._liquidity (catpay-whitelist.sol#326) is not in mixedCase
Parameter Catpay.setTaxes(uint256,uint256,uint256,uint256)._burn (catpay-whitelist.sol#326) is not in mixedCase
Parameter Catpay.setBuyTaxes(uint256,uint256,uint256,uint256)._rfi (catpay-whitelist.sol#335) is not in mixedCase
Parameter Catpay.setBuyTaxes(uint256,uint256,uint256,uint256)._marketing (catpay-whitelist.sol#335) is not in mixedCase
Parameter Catpay.setBuyTaxes(uint256,uint256,uint256,uint256)._liquidity (catpay-whitelist.sol#335) is not in mixedCase
Parameter Catpay.setBuyTaxes(uint256,uint256,uint256,uint256)._burn (catpay-whitelist.sol#335) is not in mixedCase
Parameter Catpay.setSellTaxes(uint256,uint256,uint256,uint256)._rfi (catpay-whitelist.sol#344) is not in mixedCase
Parameter Catpay.setSellTaxes(uint256,uint256,uint256,uint256)._marketing (catpay-whitelist.sol#344) is not in mixedCase
Parameter Catpay.setSellTaxes(uint256,uint256,uint256,uint256)._liquidity (catpay-whitelist.sol#344) is not in mixedCase
Parameter Catpay.setSellTaxes(uint256,uint256,uint256,uint256)._burn (catpay-whitelist.sol#344) is not in mixedCase
Parameter Catpay.updateSwapEnabled(bool)._enabled (catpay-whitelist.sol#591) is not in mixedCase
Parameter Catpay.setAllowWhitelistTrading(bool)._allow (catpay-whitelist.sol#606) is not in mixedCase
Parameter Catpay.updateAntiDump(uint256,uint256)._maxSellAmountPerCycle (catpay-whitelist.sol#621) is not in mixedCase
Parameter Catpay.rescueAnyBEP20Tokens(address,address,uint256)._tokenAddr (catpay-whitelist.sol#661) is not in mixedCase
Parameter Catpay.rescueAnyBEP20Tokens(address,address,uint256)._to (catpay-whitelist.sol#661) is not in mixedCase
Parameter Catpay.rescueAnyBEP20Tokens(address,address,uint256)._amount (catpay-whitelist.sol#661) is not in mixedCase
Constant Catpay._decimals (catpay-whitelist.sol#114) is not in UPPER_CASE_WITH_UNDERSCORES
Constant Catpay.deadAddress (catpay-whitelist.sol#137) is not in UPPER_CASE_WITH_UNDERSCORES
Constant Catpay._name (catpay-whitelist.sol#139) is not in UPPER_CASE_WITH_UNDERSCORES
Constant Catpay._symbol (catpay-whitelist.sol#140) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (catpay-whitelist.sol#32)" inContext (catpay-whitelist.sol#26-35)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Catpay.slitherConstructorVariables() (catpay-whitelist.sol#95-668) uses literals with too many digits:
        - marketingAddress = 0x000000000000000000000000000000000000dEaD (catpay-whitelist.sol#136)
Catpay.slitherConstructorConstantVariables() (catpay-whitelist.sol#95-668) uses literals with too many digits:
        - deadAddress = 0x000000000000000000000000000000000000dEaD (catpay-whitelist.sol#137)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

```
INFO:Detectors:
Catpay._tTotal (catpay-whitelist.sol#117) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (catpay-whitelist.sol#55-57)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (catpay-whitelist.sol#59-62)
name() should be declared external:
        - Catpay.name() (catpay-whitelist.sol#205-207)
symbol() should be declared external:
        - Catpay.symbol() (catpay-whitelist.sol#208-210)
decimals() should be declared external:
        - Catpay.decimals() (catpay-whitelist.sol#211-213)
totalSupply() should be declared external:
        - Catpay.totalSupply() (catpay-whitelist.sol#216-218)
transfer(address,uint256) should be declared external:
        - Catpay.transfer(address,uint256) (catpay-whitelist.sol#225-228)
allowance(address,address) should be declared external:
        - Catpay.allowance(address,address) (catpay-whitelist.sol#230-232)
approve(address,uint256) should be declared external:
        - Catpay.approve(address,uint256) (catpay-whitelist.sol#234-237)
transferFrom(address,address,uint256) should be declared external:
        - Catpay.transferFrom(address,address,uint256) (catpay-whitelist.sol#239-247)
increaseAllowance(address,uint256) should be declared external:
        - Catpay.increaseAllowance(address,uint256) (catpay-whitelist.sol#249-252)
decreaseAllowance(address,uint256) should be declared external:
        - Catpay.decreaseAllowance(address,uint256) (catpay-whitelist.sol#254-260)
isExcludedFromReward(address) should be declared external:
        - Catpay.isExcludedFromReward(address) (catpay-whitelist.sol#262-264)
reflectionFromToken(uint256,bool) should be declared external:
        - Catpay.reflectionFromToken(uint256,bool) (catpay-whitelist.sol#266-275)
excludeFromFee(address) should be declared external:
        - Catpay.excludeFromFee(address) (catpay-whitelist.sol#313-315)
includeInFee(address) should be declared external:
        - Catpay.includeInFee(address) (catpay-whitelist.sol#317-319)
isExcludedFromFee(address) should be declared external:
```

```
isExcludedFromFee(address) should be declared external:
        - Catpay.isExcludedFromFee(address) (catpay-whitelist.sol#322-324)
setTaxes(uint256,uint256,uint256,uint256) should be declared external:
        - Catpay.setTaxes(uint256,uint256,uint256,uint256) (catpay-whitelist.sol#326-333)
setBuyTaxes(uint256,uint256,uint256,uint256) should be declared external:
        - Catpay.setBuyTaxes(uint256,uint256,uint256,uint256) (catpay-whitelist.sol#335-342)
setSellTaxes(uint256,uint256,uint256,uint256) should be declared external:
        - Catpay.setSellTaxes(uint256,uint256,uint256,uint256) (catpay-whitelist.sol#344-351)
isBot(address) should be declared external:
        - Catpay.isBot(address) (catpay-whitelist.sol#627-629)
rescueAnyBEP20Tokens(address,address,uint256) should be declared external:
        - Catpay.rescueAnyBEP20Tokens(address,address,uint256) (catpay-whitelist.sol#661-664)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:catpay-whitelist.sol analyzed (6 contracts with 75 detectors), 73 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

catpay-whitelist.sol

Security

Check-effects-interaction:

INTERNAL ERROR in module Check-effects-interaction: Cannot read properties of undefined (reading 'name')
Pos: not available

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 476:28:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 573:12:

Gas & Economy

Gas costs:

Gas requirement of function Catpay.taxes is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 150:4:

Gas costs:

Gas requirement of function Catpay.rescueAnyBEP20Tokens is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 661:4:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.
more
Pos: 301:8:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.

more

Pos: 648:8:

Miscellaneous

Constant/View/Pure functions:

INTERNAL ERROR in module Constant/View/Pure functions: Cannot read properties of undefined (reading 'name')

Pos: not available

Similar variable names:

Catpay.(address) : Variables have very similar names "_rOwned" and "_tOwned". Note: Modifiers are currently not considered by this static analysis.

Pos: 196:8:

Similar variable names:

Catpay.(address) : Variables have very similar names "_tTotal" and "_rTotal". Note: Modifiers are currently not considered by this static analysis.

Pos: 196:27:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 284:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 291:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 596:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 622:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 647:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 655:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 407:23:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 408:18:

Solhint Linter

catpay-whitelist.sol

```
catpay-whitelist.sol:2:1: Error: Compiler version ^0.8.7 does not
satisfy the r semver requirement
catpay-whitelist.sol:42:5: Error: Explicitly mark visibility in
function (Set ignoreConstructors to true if using solidity >=0.7.0)
catpay-whitelist.sol:77:5: Error: Function name must be in mixedCase
catpay-whitelist.sol:95:1: Error: Contract has 26 states declarations
but allowed no more than 15
catpay-whitelist.sol:114:28: Error: Constant name must be in
capitalized SNAKE_CASE
catpay-whitelist.sol:137:29: Error: Constant name must be in
capitalized SNAKE_CASE
catpay-whitelist.sol:139:29: Error: Constant name must be in
capitalized SNAKE_CASE
catpay-whitelist.sol:140:29: Error: Constant name must be in
capitalized SNAKE_CASE
catpay-whitelist.sol:162:5: Error: Contract name must be in CamelCase
catpay-whitelist.sol:185:5: Error: Explicitly mark visibility in
function (Set ignoreConstructors to true if using solidity >=0.7.0)
catpay-whitelist.sol:388:94: Error: Variable name must be in
mixedCase
catpay-whitelist.sol:476:29: Error: Avoid to make time-based
decisions in your business logic
catpay-whitelist.sol:485:47: Error: Avoid to make time-based
decisions in your business logic
catpay-whitelist.sol:555:13: Error: Avoid to make time-based
decisions in your business logic
catpay-whitelist.sol:573:13: Error: Avoid to make time-based
decisions in your business logic
catpay-whitelist.sol:578:48: Error: Use double quotes for string
literals
catpay-whitelist.sol:596:43: Error: Use double quotes for string
literals
catpay-whitelist.sol:666:31: Error: Code contains empty blocks
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Email: audit@EtherAuthority.io