CatGirl

Smart Contract Audit Report

SYSFIXED

01 Jun 2021

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
CatGirl	CATGIRL	Binance Smart Chain

Addresses

Contract address	0x79ebc9a2ce02277a4b5b3a768b1c0a4ed75bd936
Contract deployer address	0x79eBC9A2ce02277A4b5b3A768b1C0A4ed75Bd936

Project Website

https://www.catgirl.io/

Codebase

https://bscscan.com/address/0x79ebc9a2ce02277a4b5b3a768b1c0a4ed75bd936#code

SUMMARY

Catgirl combines the limitless potential of crypto and NFTs into one modern, colorful, and interactive experience.

Contract Summary

Documentation Quality

CatGirl provides a very good documentation with standard of solidity base code.

- The technical description is provided clearly and structured and also dont have any high risk issue.

Code Quality

The Overall quality of the basecode is standard.

- Standard solidity basecode and rules are already followed by CatGirl with the discovery of several low issues.

Test Coverage

Test coverage of the project is 100% (Through Codebase)

Audit Findings Summary

- SWC-100 SWC-108 | Explicitly define visibility for all state variables on lines 662 and 663.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 96, 125, 145, 146, 178, 211, 416, 635, 635, 639, 639, 639, 639, 640, 640, 668, 668, 668, 668, 669, 669, 669, 669, 670, 670, 670, 670, 673, 673, 673, 673, 818, 820, 890, 945, 990, 1019, 1025, 1031, 1036 and 820.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 8.
- SWC-110 SWC-123 | It is recommended to use of revert(), assert(), and require() in Solidity, and the new REVERT opcode in the EVM on lines 819, 820, 820, 946, 946, 947, 948, 968, 971, 1156 and 1157.
- SWC-120 | It is recommended to use external sources of randomness via oracles on lines 962.

CONCLUSION

We have audited the CatGirl project released on May 2021 to discover issues and identify potential security vulnerabilities in CatGirl Project. This process is used to find technical issues and security loopholes which might be found in the smart contract.

The security audit report provides satisfactory results with low-risk issues.

The issues found in the CatGirl smart contract code do not pose a considerable risk. The writing of the contract is close to the standard of writing contracts in general. The low-risk issues found are some arithmetic operation issues, a floating pragma is set, a state variable visibility is not set, the potential use of "block.number" as a source of randomness, and out-of-bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value.

AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	ISSUE FOUND
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	ISSUE FOUND
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	PASS
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASS
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	PASS
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASS
Signature Unique ID	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	PASS
Incorrect Constructor Name	SWC-118	Constructors are special functions that are called only once during the contract creation.	PASS
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASS
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	ISSUE FOUND
Write to Arbitrary Storage Location	SWC-124	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	PASS
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	PASS
Insufficient Gas Griefing	SWC-126	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	PASS
Arbitrary Jump Function	SWC-127	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	PASS

Typographical Error	SWC-129	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	PASS
Override control character	SWC-130	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	PASS
Unused variables	SWC-131 SWC-135	Unused variables are allowed in Solidity and they do not pose a direct security issue.	PASS
Unexpected Ether balance	SWC-132	Contracts can behave erroneously when they strictly assume a specific Ether balance.	PASS
Hash Collisions Variable	SWC-133	Using abi.encodePacked() with multiple variable length arguments can, in certain situations, lead to a hash collision.	PASS
Hardcoded gas amount	SWC-134	The transfer() and send() functions forward a fixed amount of 2300 gas.	PASS
Unencrypted Private Data	SWC-136	It is a common misconception that private type variables cannot be read.	PASS

SMART CONTRACT ANALYSIS

Started	Monday May 31 2021 07:15:40 GMT+0000 (Coordinated Universal Time)
Finished	Tuesday Jun 01 2021 09:01:49 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	CatGirlCoin.sol

Detected Issues

ID	Title	Severity	Status
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-120	POTENTIAL USE OF "BLOCK.NUMBER" AS SOURCE OF RANDOMNESS.	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 96

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
95   function add(uint256 a, uint256 b) internal pure returns (uint256) {
96   uint256 c = a + b;
97   require(c >= a, "SafeMath: addition overflow");
98   return c;
99   }
100
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 125

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
124   require(b <= a, errorMessage);
125   uint256 c = a - b;
126   return c;
127   }
128   /**
129
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 145

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
144   }
145   uint256 c = a * b;
146   require(c / a == b, "SafeMath: multiplication overflow");
147   return c;
148   }
149
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 146

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
145   uint256 c = a * b;
146   require(c / a == b, "SafeMath: multiplication overflow");
147   return c;
148   }
149   /**
150
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 178

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
177   require(b > 0, errorMessage);
178   uint256 c = a / b;
179   // assert(a == b * c + a % b); // There is no case in which this doesn't hold
180   return c;
181   }
182
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 211

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
210   require(b != 0, errorMessage);
211   return a % b;
212   }
213   }
214   abstract contract Context {
215
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 416

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
415   _owner = address(0);
416   _lockTime = block.timestamp + time;
417   emit OwnershipTransferred(_owner, address(0));
418   }
419
420
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 635

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
634
635   uint256 private _minLottoBalance = 1000000000 * 10**9;
636
637
638   uint256 private constant MAX = ~uint256(0);
639
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 635

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
634
635   uint256 private _minLottoBalance = 1000000000 * 10**9;
636
637
638   uint256 private constant MAX = ~uint256(0);
639
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 639

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
638   uint256 private constant MAX = ~uint256(0);
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 639

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
638   uint256 private constant MAX = ~uint256(0);
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 639

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
638   uint256 private constant MAX = ~uint256(0);
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 639

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
638   uint256 private constant MAX = ~uint256(0);
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 640

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643   string private _name = "CatGirl";
644
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 640

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
639   uint256 private _tTotal = 100000 * 10**12 * 10**9;
640   uint256 private _rTotal = (MAX - (MAX % _tTotal));
641
642   uint256 private _tFeeTotal;
643   string private _name = "CatGirl";
644
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 668

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
667
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 668

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
667
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 668

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
667
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 668

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
667
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 669

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 669

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 669

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 669

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
668   uint256 public _maxTxAmount = 100000 * 10**12 * 10**9;
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 670

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 670

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 670

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 670

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
669   uint256 private numTokensSellToAddToLiquidity = 500 * 10**12 * 10**9;
670   uint256 public lotteryThreshold = 10 * 10**12 * 10**9;
671   // anti whale
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 673

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
675   struct TData {
676   uint256 tAmount;
677
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 673

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
675   struct TData {
676   uint256 tAmount;
677
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 673

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
675   struct TData {
676   uint256 tAmount;
677
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 673

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
672   bool    public _isAntiWhaleEnabled = true;
673   uint256 public _antiWhaleThreshold = 1 * 10**15 * 10**9;
674
675   struct TData {
676   uint256 tAmount;
677
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 818

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
817   require(_isExcluded[account], "Account is already excluded");
818   for (uint256 i = 0; i < _excluded.length; i++) {
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 820

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822   _isExcluded[account] = false;
823   _excluded.pop();
824
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 890

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
889   _maxTxAmount = _tTotal.mul(maxTxPercent).div(
890   10**2
891   );
892   }
893   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
894
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 945

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
944   uint256 tSupply = _tTotal;
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 990

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
989   _totalLottoPrize = _totalLottoPrize.add(amount);
990   ++_lottoDrawCount;
991   emit DrawLotto(amount, _lottoDrawCount);
992   }
993
994
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1019

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
1018   return _amount.mul(_lottoFee).div(
1019   10**2
1020   );
1021   }
1022
1023
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1025

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
1024   return _amount.mul(_devFee).div(
1025   10**2
1026   );
1027   }
1028
1029
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1031

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
1030   return _amount.mul(_taxFee).div(
1031   10**2
1032   );
1033   }
1034   function calculateLiquidityFee(uint256 _amount) private view returns (uint256) {
1035
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1036

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
1035   return _amount.mul(_liquidityFee).div(
1036   10**2
1037   );
1038   }
1039
1040
```

SWC-101 | COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED

LINE 820

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CatGirlCoin.sol

Locations

```
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822   _isExcluded[account] = false;
823   _excluded.pop();
824
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 8

low SEVERITY

The current pragma Solidity directive is ""^0.8.4"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source File

- CatGirlCoin.sol

Locations

```
7   */
8   pragma solidity ^0.8.4;
9   // SPDX-License-Identifier: Unlicensed
10   interface IBEP20 {
11   function totalSupply() external view returns (uint256);
12
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 662

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "inSwapAndLiquify" is internal. Other possible visibility settings are public and private.

Source File

- CatGirlCoin.sol

Locations

```
661
662   bool inSwapAndLiquify;
663   bool inLotteryDraw;
664   bool public swapAndLiquifyEnabled = true;
665   bool public lottoEnabled = true;
666
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 663

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "inLotteryDraw" is internal. Other possible visibility settings are public and private.

Source File

- CatGirlCoin.sol

Locations

```
662   bool inSwapAndLiquify;
663   bool inLotteryDraw;
664   bool public swapAndLiquifyEnabled = true;
665   bool public lottoEnabled = true;
666   bool public _shouldSwapToBNB = false;
667
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 819

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
818   for (uint256 i = 0; i < _excluded.length; i++) {
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822   _isExcluded[account] = false;
823
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 820

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822   _isExcluded[account] = false;
823   _excluded.pop();
824
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 820

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
819   if (_excluded[i] == account) {
820   _excluded[i] = _excluded[_excluded.length - 1];
821   _tOwned[account] = 0;
822   _isExcluded[account] = false;
823   _excluded.pop();
824
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 946

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 946

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 947

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
951
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 948

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
951   return (rSupply, tSupply);
952
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 968

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
967
968   uint256 ownedAmount = _rOwned[_addressList[randomNumber]];
969
970   if (ownedAmount >= _minLottoBalance) {
971   return _addressList[randomNumber];
972
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 971

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
970   if (ownedAmount >= _minLottoBalance) {
971   return _addressList[randomNumber];
972   }
973   return _devWallet;
974   }
975
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1156

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
1155   address[] memory path = new address[](2);
1156   path[0] = address(this);
1157   path[1] = uniswapV2Router.WETH();
1158   _approve(address(this), address(uniswapV2Router), tokenAmount);
1159   // make the swap
1160
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1157

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CatGirlCoin.sol

Locations

```
1156   path[0] = address(this);
1157   path[1] = uniswapV2Router.WETH();
1158   _approve(address(this), address(uniswapV2Router), tokenAmount);
1159   // make the swap
1160   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
1161
```

SWC-120 | POTENTIAL USE OF "BLOCK.NUMBER" AS SOURCE OF RANDOMNESS.

LINE 962

low SEVERITY

The environment variable "block.number" looks like it might be used as a source of randomness. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicious miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment variables as sources of randomness and be aware that use of these variables introduces a certain level of trust into miners.

Source File

- CatGirlCoin.sol

Locations

```
961   function random() private view returns (uint) {
962   return uint(keccak256(abi.encodePacked(block.difficulty, block.timestamp,
block.number)));
963   }
964
965   function lotterize() private view returns(address) {
966
```

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to, or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without Sysfixed's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Sysfixed to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model, or legal compliance.

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.