freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Molly Bot

$MOLLY

14/01/2024

TOKEN OVERVIEW

Fees

- Buy fees: 7%
- Sell fees: 7%

Fees privileges

- Can change buy fees up to 11% and sell fees up to 11%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can’t change max tx amount and max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
- Contract owner has the ability to update the marketing wallet without requiring any additional checks

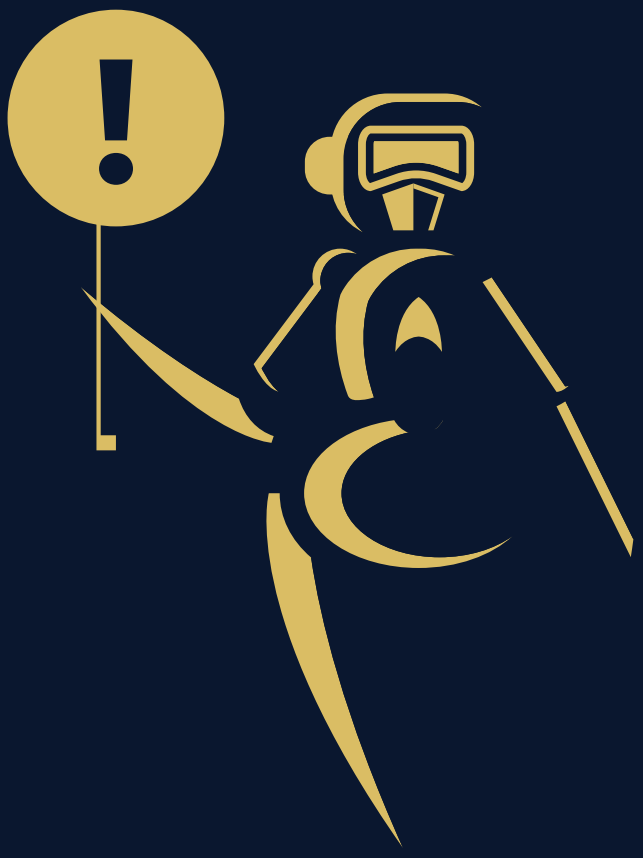
TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



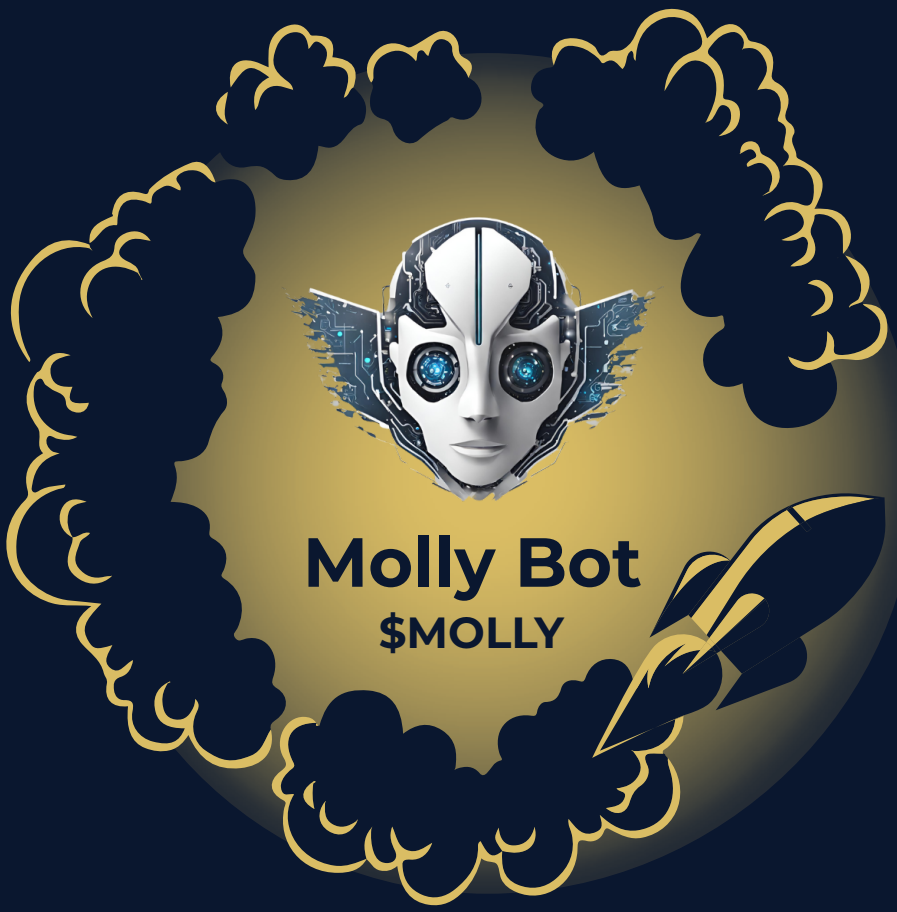
INTRODUCTION

FreshCoins (Consultant) was contracted by
Molly Bot (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x0dc51Ad750c18d30C2070062CF5411C751E4a78a

Network: Binance Smart Chain (BSC)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 14/01/2024



WEBSITE DIAGNOSTIC

https://www.mollybot.tech/


0-49


50-89


90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials


Twitter

https://twitter.com/mollybot_bsc


Telegram

https://t.me/mollybot_portal

AUDIT OVERVIEW

56

Security Score
HIGH RISK
Audit FAIL

93

Static Scan
Automatic scanning for common vulnerabilities

60

ERC Scan
Automatic checks for ERC's conformance

1 High

1 Medium

0 Low

0 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Low
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES

- Contract owner can't mint tokens after initial contract deploy

- Contract owner can't exclude addresses from transactions

- Contract owner can change marketing wallet and / or dev address

  Since the function lacks additional checks, the contract owner could potentially set the marketing wallet or dev wallet to a contract address that is unable to receive ETH or BNB, leading to the transformation of the token contract into a honeypot. This scenario would render selling impossible for users

  _developmentAddress: 0x6fC836d34aCa9D2DC044aFF03C23B427480bb9dC

  _marketingAddress: 0x6fC836d34aCa9D2DC044aFF03C23B427480bb9dC

```
event devAddressUpdated(address indexed previous, address indexed adr);
function setNewDevAddress(address payable dev) public onlyDev() {
    emit devAddressUpdated(_developmentAddress, dev);
    _developmentAddress = dev;
    _isExcludedFromFee[_developmentAddress] = true;
}

event marketingAddressUpdated(address indexed previous, address indexed adr);
function setNewMarketingAddress(address payable markt) public onlyDev() {
    emit marketingAddressUpdated(_marketingAddress, markt);
    _marketingAddress = markt;
    _isExcludedFromFee[_marketingAddress] = true;
}
```

- Contract owner can exclude/include wallet(s) from tax

```
function excludeMultipleAccountsFromFees(address[] calldata accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFee[accounts[i]] = excluded;
    }
}
```

- Contract owner can change swap settings

```
function toggleSwap(bool _swapEnabled) public onlyDev {
    swapEnabled = _swapEnabled;
}
```

Contract owner can change buy fees up to 11% and sell fees up to 11%

```
function setFee(uint256 redisFeeOnBuy, uint256 redisFeeOnSell, uint256 taxFeeOnBuy, uint256 taxFeeOnSell)
public onlyDev {
            require(redisFeeOnBuy < 3, "Redis cannot be more than 2.");
            require(redisFeeOnSell < 3, "Redis cannot be more than 2.");
            require(taxFeeOnBuy < 10, "Tax cannot be more than 9.");
            require(taxFeeOnSell < 10, "Tax cannot be more than 9.");
    _redisFeeOnBuy = redisFeeOnBuy;
    _redisFeeOnSell = redisFeeOnSell;
    _taxFeeOnBuy = taxFeeOnBuy;
    _taxFeeOnSell = taxFeeOnSell;
}
```

Contract owner has ability to retrieve any token held by the contract

Native tokens NOT excluded

```
event tokensRescued(address indexed token, address indexed to, uint amount);
function rescueForeignTokens(address _tokenAddr, address _to, uint _amount) public onlyDev() {
    emit tokensRescued(_tokenAddr, _to, _amount);
    Token(_tokenAddr).transfer(_to, _amount);
}
```

Contract owner can transfer ownership

```
event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
function transferOwnership(address newOwner) public virtual onlyOwner {
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}
```

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

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

Found 1 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	7%
Sell fees:	7%
Max TX:	N/A
Max Wallet:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

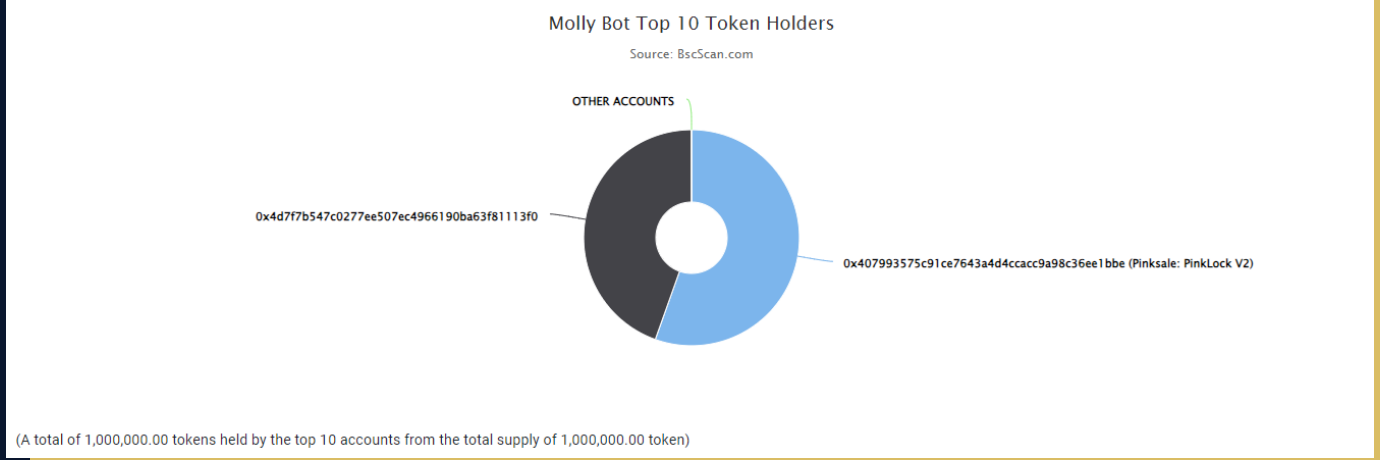
Rug Pull Risk

Liquidity:	N/A
Holders:	Clean

MOLLY TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,000,000.00 Tokens) of Molly Bot

Token Total Supply: 1,000,000.00 Token | Total Token Holders: 2



(A total of 1,000,000.00 tokens held by the top 10 accounts from the total supply of 1,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Pinksale: PinkLock V2	554,650	55.4650%
2	0x4d7f7b...F81113f0	445,350	44.5350%

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 its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.