



# expelee

A Secure Place For Web3

## **SMART CONTRACT AUDIT OF**

MAN OF WEALTH (MOW)



**Contract Address** 

0x2B22d7d9587b50F38052C07de707702be3ef0ACE

www.expelee.com | Page 1 |





## **Audit Summary**

Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

**Audit Result: PASSED** 

**Ownership: NOT RENOUNCED** 

KYC Verification: Not done till date of audit

Audit Date: 09/07/2022

**Audit Team: EXPELEE** 

Be aware that smart contracts deployed on the blockchain aren't resistant to internal exploit, external vulnerability, or hack. For a detailed understanding of risk severity, source code vulnerability, functional hack, and audit disclaimer, kindly refer to the audit.

www.expelee.com | Page 2 |





## **DISCLAMER**

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

www.expelee.com Page 3 |



## **Contract Review**

Contract Name	Token			
Compiler Version	v0.8.13+commit.abaa5c0e			
Optimization	Yes with 200 runs			
License	MIT license			
Explorer	https://bscscan.com/address/0x2B22d 7d9587b50F38052C07de707702be3ef0 ACE#code			
Symbol	MOW			
Decimals	18			
Total Supply	10,000,000,000			
Domain				

www.expelee.com | Page 4 |



# **Project Review**

Token Name: Man Of Wealth

Twitter: https://twitter.com/gateofwealth?s=09

Telegram: https://t.me/manofwealth\_CN

**Contract Address:** 

0x2B22d7d9587b50F38052C07de707702be3ef0ACE

**Platform: Binance Smart Chain** 

Token Type: BEP 20

Language: SOLIDITY

www.expelee.com Page 5 |





## **Audit Methodology**

The scope of this report is to audit the smart contract source code. We have scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

## Category

- Unhandled Exceptions

- Transaction Order Dependency

Smart Contract Vulnerabilities

- Integer Overflow

- Unrestricted Action

- Incorrect Inheritance Order

- Typographical Errors

- Requirement Violation

Source Code Review

- Gas Limit and Loops

- Deployment Consistency

- Repository Consistency

- Data Consistency

- Token Supply Manipulation

Functional Assessment - Operations Trail & Event Generation

- Assets Manipulation

- Liquidity Access

www.expelee.com | Page 6 |





# **Vulnerability Checklist**

Nō	Description.	Result
1	Compiler warnings.	Passed
2	Race conditions and Re-entrancy. Cross-function raceconditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

www.expelee.com | Page 7 |

## **Manual Audit**

- Low-Risk
- 4 low-risk code issues found
  - Medium-Risk
- 0 medium-risk code issues found
  - High-Risk
  - 0 high-risk code issues found

www.expelee.com | Page 8 |



## **Audit Summary**

Compiled with solc

Number of lines: 451 (+ 0 in dependencies, + 0 in tests)

Number of assembly lines: 0

Number of contracts: 8 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 17 Number of informational issues: 23

Number of low issues: 4
Number of medium issues: 0

Number of high issues: 0

ERCs: ERC20

+	# functions	ERCS	ERC20 info	Complex code	+   Features
IPancakeRouter02     IUniswapV2Factory	24 8			   No   No	Receive ETH
Token	42	ERC20	No Minting	No No	Receive ETH
			Approve Race Cond.	 	Send ETH     Tokens interaction
<u> </u>					Assembly

www.expelee.com | Page 9





#### 1) Contract contains Reentrancy vulnuerabilities

Detection of the reentrancy bug. Do not report reentrancies that involve Ether (see reentrancy-eth).

```
function transferFrom(
    address sender, address recipient, uint256 amount
) public virtual override returns (bool) {
    _transfer(sender, recipient, amount);

    uint256 currentAllowance = _allowances[sender][_msgSender()];
    require(currentAllowance >= amount, "ERC20: transfer amount exceeds allowance");
    unchecked {
        _approve(sender, _msgSender(), currentAllowance - amount);
    }

    return true;
}
```

#### Recommendation

Apply the check-effects-interaction pattern

www.expelee.com Page 10 |



#### 2) No zero address validation for some functions

Detect missing zero address validation.

```
function setAddrs(address mark, address wrap) public onlyOwner {
    _mark = mark;
    _wrap = wrap;
}

function setPool(address pool) public onlyOwner {
    _pool = pool;
}
```

#### Recommendation

Check that the new address is not zero.

www.expelee.com Page 11|



#### 3)Unchecked transfer

The return value of an external transfer is not checked.

#### Recommendation

Ensure that an arbitary user cannot withdraw unauthorized funds

www.expelee.com | Page 12 |



#### 4) Functions could be declared external

Functions are not declared externally

#### Recommendation

Make sure to declare functions externally for better code optimization

www.expelee.com Page 13 |





## Manual Audit (Contract Function)

```
contract Token is Ownable, IERC20Metadata {
   mapping(address => bool) public whites;
   mapping(address => uint256) private _balances;
   mapping(address => mapping(address => uint256)) private _allowances;
   string private _name;
   string private _symbol;
   uint256 private _totalSupply;
   uint256 public _maxsell;
   uint256 public _maxusdt;
   address public router;
   address public wbnb;
   address public _usdt;
   address public _gow;
   address public _pair;
   address public _main;
   address public _mark;
   address public _pool;
   address public _wrap;
   address public _dead;
          private _swapping;
   constructor() {
       _name = "Man of Wealth";
       _symbol = "MOW";
       _wbnb = 0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c;
       _gow = 0x7e6226F726e01692A4740C22b11bCcb1757254d3;
       main = 0xefe1bA9b1804196be109aA9d31C0e03955CB670D;
       _mark = 0x66f38194180917F55321Bc8A01bc7dCf45e33534;
       pool = 0xacce44ddAA68C2729DC8df4cc925F16252aeB4c4;
       _usdt = 0x55d398326f99059fF775485246999027B3197955;
       _whites[_dead] = true;
       _whites[_main] = true;
       _whites[_mark] = true;
       whites[ pool] = true;
       _whites[address(this)] = true;
       _maxsell = 10000000 * 10 ** decimals();
       maxusdt = 100 * 10 ** 18;
       _mint(_main, 10000000000000 * 10 ** decimals());
```

www.expelee.com Page 14 |





## Important Points To Consider

- √ The owner cannot mint tokens after Initial
  - ✓ The owner cannot stop Trading.
    - ✓ Verified contract source
- ✓Owner/creator wallet contains less than 10% of circulating token supply (0%)
  - X Token is sellable (not a honeypot) at this time
- X Ownership renounced or source does not contain an owner contract
  - X Source does not contain a fee modifier

    The source code contains a function which can modify the transaction fee.

www.expelee.com Page 15 |





## About Expelee

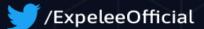
Expelee is a community driven organisation dedicated to fostering an antirug movement. We're here to keep investment safe from fraudsters. We've encountered several rug pulls and know how it feels to be duped, which is why we don't want anybody else to go through the same experience. We are here to raise awareness through our services so that the future of cryptocurrency can be rug-free.

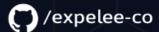
The auditing process focuses to the following considerations with collaboration of an expert team:

- Functionality test of the Smart Contract to determine if proper logic has been followed throughout the whole process.
- Manually detailed examination of the code line by line by experts.
- Live test by multiple clients using Test net.
- Analysing failure preparations to check how the Smart
- Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.

### Social Media







www.expelee.com Page 16 |