

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT







TOKEN OVERVIEW

Fees

• Buy fees: 0%

• Sell fees: 0%

Fees privileges

Can't change / set fees

Ownership

Owned

Minting

No mint function

Max Tx Amount / Max Wallet Amount

· Can't change max tx amount and / or max wallet amount

Blacklist

Blacklist function not detected

Other privileges

- · Can exclude / include from fees
- Contract owner has to call enableTrading function to enable trade

TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- **3** WEBSITE + SOCIALS
- (4-5) AUDIT OVERVIEW
- 6-8) OWNER PRIVILEGES
- 9 CONCLUSION AND ANALYSIS
- (10) TOKEN DETAILS
- BETMEN TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS
- (12) TECHNICAL DISCLAIMER

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

Betmen (Customer) to conduct a Smart Contract Code Review and

Security Analysis.

0xB5C518c01D04B96cA8345b27ea85D950039F910A

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 23/03/2024



WEBSITE DIAGNOSTIC

https://betmencoin.com/



0-49



50-89



90-100



Performance



Accessibility



Best Practices



SEO



Progressive Web App

Socials



Twitter

https://twitter.com/Betmensbsc



Telegram

https://t.me/BetmensCave

AUDIT OVERVIEW





Static Scan Automatic scanning for common vulnerabilities



ERC Scan
Automatic checks for ERC's conformance

- 1 High
- 0 Medium
- O Low
- Optimizations
- o 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	Passed	
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 an address from transactions
- Contract owner can whitelist wallet address

```
function setWhitelistStatus(
    address _wallet,
    bool _status
) external onlyOwner {
    whitelisted[_wallet] = _status;
    emit Whitelist(_wallet, _status);
}
```

Contract owner has to call enableTrading function to enable trade

Please note that any whitelisted wallet address retains the ability to engage in trading, even in situations where trading has been disabled

```
function enableTrading() external onlyOwner {
    require(!tradingEnabled, "Trading is already enabled");
    tradingEnabled = true;
    startTradingBlock = block.number;
}

_transferFrom function line 533
.
.
.
.
.
if (!whitelisted[_from] && !whitelisted[_to] ) {
    require(tradingEnabled, "Trading not active");
}
.
.
.
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "Ownable: new owner is the zero address");
    _transferOwnership(newOwner);
}

function _transferOwnership(address newOwner) internal virtual {
    address oldOwner = _owner;
    _owner = newOwner;
    emit OwnershipTransferred(oldOwner, newOwner);
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    _transferOwnership(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: 0%

Sell fees: 0%

Max TX: N/A

Max Sell: N/A

Honeypot Risk

Ownership: Owned

Blacklist: Not detected

Modify Max TX: Not detected

Modify Max Sell: Not detected

Disable Trading: Not detected

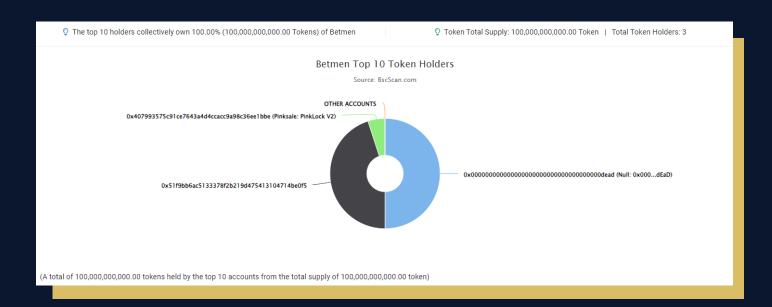
Rug Pull Risk

Liquidity: N/A

Holders: Clean



BETMEN TOKEN ANALYTICS& TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	Null: 0x000dEaD @	50,000,000,000	50.0000%
2	☐ 0x51F9bB6a4714Be0F5	44,986,080,000	44.9861%
3	☐ Pinksale: PinkLock V2 □	5,013,920,000	5.0139%

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.

