freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Trump America First

$TRUMPUSFIRST

18/05/2023

TOKEN OVERVIEW

Fees

- Buy fees: N/A
- Sell fees: N/A

Fees privileges

- Can’t change fees

Ownership

- Owned

Minting

- Mint function detected

Max Tx Amount / Max Wallet Amount

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

Blacklist

- Blacklist function not detected

Other privileges

- N/A

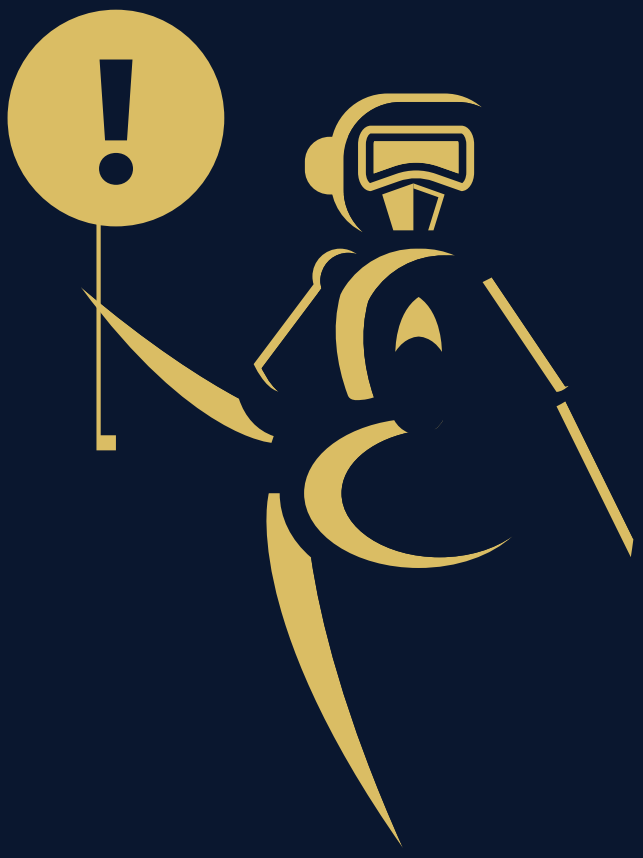
TABLE OF CONTENTS

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
Trump America First (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x10B05488080E3F9912C3eeD2cD95B9193dE920fE

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 18/05/2023

WEBSITE DIAGNOSTIC

https://trumpamericafrist.xyz/

0-49 50-89 90-100

Performance | Accessibility | Best Practices | SEO | Progressive Web App

Socials

Twitter

https://twitter.com/Trumptoken1st

Telegram

https://t.me/Trumptoken1st

AUDIT OVERVIEW

62

Security Score
HIGH RISK
Audit FAIL

93

Static Scan
Automatic scanning for common vulnerabilities

79

ERC Scan
Automatic checks for ERC's conformance

1	High
0	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	Passed
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 exclude an address from transactions
- Contract owner can mint tokens after initial contract deploy

The options "isBlacklistEnabled," "isMaxAmountOfTokensSet," and "isWhitelistEnabled" are all set to False, while "isMintable" is set to True.

```
function mint(address to, uint256 amount) external onlyOwner whenNotPaused {
    if (!isMintable()) {
      revert MintingNotEnabled();
    }
    if (isMaxAmountOfTokensSet()) {
      if (balanceOf(to) + amount > maxTokenAmountPerAddress) {
        revert DestBalanceExceedsMaxAllowed(to);
      }
    }
    if (isBlacklistEnabled()) {
      if (_isBlacklisted[to]) {
        revert RecipientBlacklisted(to);
      }
    }
    if (isWhitelistEnabled()) {
      if (!whitelist[to]) {
        revert RecipientNotWhitelisted(to);
      }
    }

    super._mint(to, amount);
}

function _mint(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: mint to the zero address");

        _beforeTokenTransfer(address(0), account, amount);

        _totalSupply += amount;
        _balances[account] += amount;
        emit Transfer(address(0), account, amount);

        _afterTokenTransfer(address(0), account, amount);
}
```

1. The function has a modifier onlyOwner, which implies that only the contract owner can call this function.
2. There is a check for isMintable() function, which, returns true. Therefore, the condition if (!isMintable()) will evaluate to false, and the code inside the block will not execute. As a result, the execution will proceed to the next condition.
3. The condition if (isMaxAmountOfTokensSet()) checks whether the maximum token amount per address is set. However, it is set to false. Therefore, the code inside this block will also not execute.
4. The following condition checks whether the recipient (to) is blacklisted (_isBlacklisted[to]). However, since isBlacklistEnabled() is set to false, this block will be skipped as well.
5. The next condition checks if the recipient (to) is whitelisted (whitelist[to]). Again, since isWhitelistEnabled() is set to false, this block will not be executed.
6. If none of the conditions above trigger a revert, the super._mint(to, amount) function will be called, which presumably mints new tokens and assigns them to the specified address (to).

In summary, if the isMintable option is set to true and all other options (isBlacklistEnabled, isMaxAmountOfTokensSet, isWhitelistEnabled) are set to false, then the owner can mint new tokens.

Contract owner can renounce ownership

```
function renounceOwnership() public override onlyOwner whenNotPaused {
    super.renounceOwnership();
}

function renounceOwnership() public virtual onlyOwner {
        _transferOwnership(address(0));
}

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

Contract owner can transfer ownership

```
function transferOwnership(address newOwner)
    public
    override
    onlyOwner
    whenNotPaused
  {
    super.transferOwnership(newOwner);
}
```

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:	N/A
Sell fees:	N/A
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

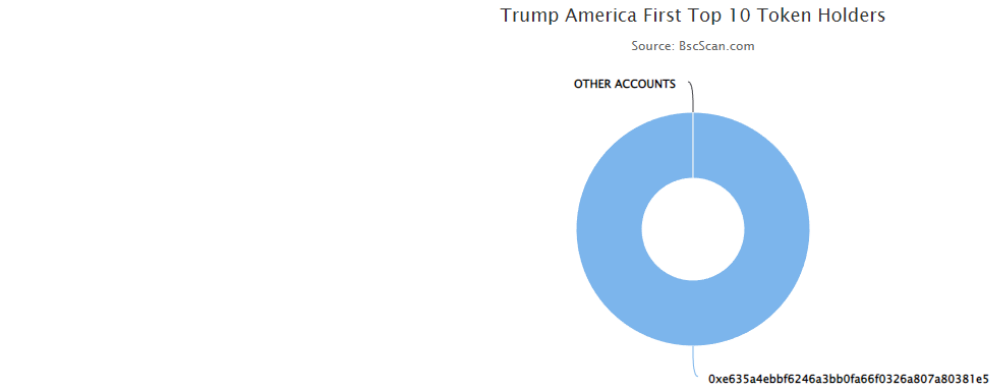
Rug Pull Risk

Liquidity:	N/A
Holders:	100% unlocked tokens

TRUMPUSFIRST TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (4,200,000,000,000,000.00 Tokens) of Trump America First

Token Total Supply: 4,200,000,000,000,000.00 Token | Total Token Holders: 1



(A total of 4,200,000,000,000,000.00 tokens held by the top 10 accounts from the total supply of 4,200,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xe635a4ebbf6246a3bb0fa66f0326a807a80381e5	4,200,000,000,000,000	100.0000%

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.