freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

ARMswap

$ARMSP

22/01/2025

TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

Fees privileges

- Can’t change or 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 detected

Other privileges

- Pausable contract
- Contract owner has to call enableTokenTransfer function to enable trade

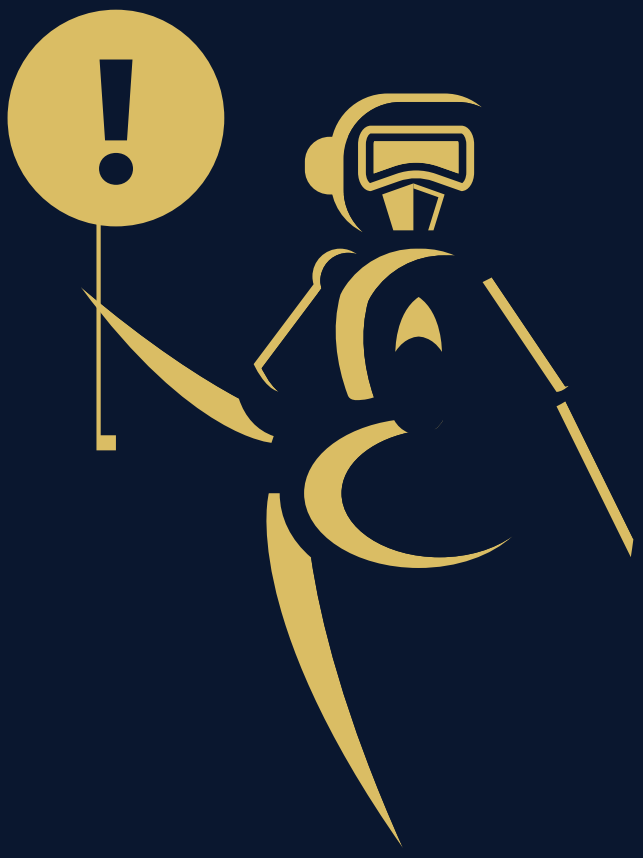
TABLE OF CONTENTS

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 ARMswap (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x35FD6CCB662E5Ea865575143433DB18f0a79bbfb

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 22/01/2025

WEBSITE DIAGNOSTIC

https://armswap.com/

0-49 50-89 90-100

Performance	Accessibility	Best Practices	SEO	Progressive Web App
98	95	92	92	NA

Socials

X (Twitter)

https://x.com/armswapofficial

Telegram

https://t.me/arm_swap

AUDIT OVERVIEW

62

Security Score

HIGH RISK

91

Static Scan

Automatic scanning for common vulnerabilities

56

ERC Scan

Automatic checks for ERC's conformance

2 High

1 Medium

0 Low

0 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Low
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 exclude an address from transactions

```
function addToBlackList(address account) external onlyOwner {
        _addToBlackList(account);
    }

    function removeFromBlackList(address account) external onlyOwner {
        _removeFromBlackList(account);
    }
```

- Contract owner has to call enableTokenTransfer function to enable trade

Any wallet added to the isTransferAllowed list will retain the ability to trade, even when trading is otherwise disabled in the project. The addToTransferAllowed function provides this exception, enabling specified wallets to bypass the trading restriction.

```
function _enableTokenTransfer() internal virtual {
        _isTokenTransferEnabled = true;
        emit TokenTransferEnabled();
    }

    function transfer(address to, uint256 value) public virtual override
        whenNotPaused
        requireNonZeroValue(value)
        requireTokenTransferEnabled(_msgSender())
        whenNotBlackListed(_msgSender(), to)
        returns (bool)
    {
        address sender = _msgSender();
        _transfer(sender, to, value);

        return true;
    }
```

- Contract owner has ability to manage a list of wallets that are allowed to bypass trading restrictions

```
function addToTransferAllowed(address account) external onlyOwner {
        _addToTransferAllowed(account);
    }

    function removeFromTransferAllowed(address account) external onlyOwner {
        _removeFromTransferAllowed(account);
    }
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    if (newOwner == address(0)) {
        revert OwnableInvalidOwner(address(0));
    }
    _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));
}
```

The presale token raises several concerns about centralization and investor safety:

The blacklist function allows the owner to disable trading for any wallet at will, with or without reason, which could be misused.
Trading is disabled by default, requiring investors to trust the owner to enable it.
The manual listing of liquidity after the fair launch adds another layer of reliance on the owner's actions.
Only a small fraction of tokens (<1%) is allocated for public sale, raising concerns about fair distribution.
Over 99% of tokens remain unlocked, posing a significant risk of potential misuse or dumping.

These factors highlight risks tied to the owner's control and a lack of safeguards for investors.

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 2 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:	Detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

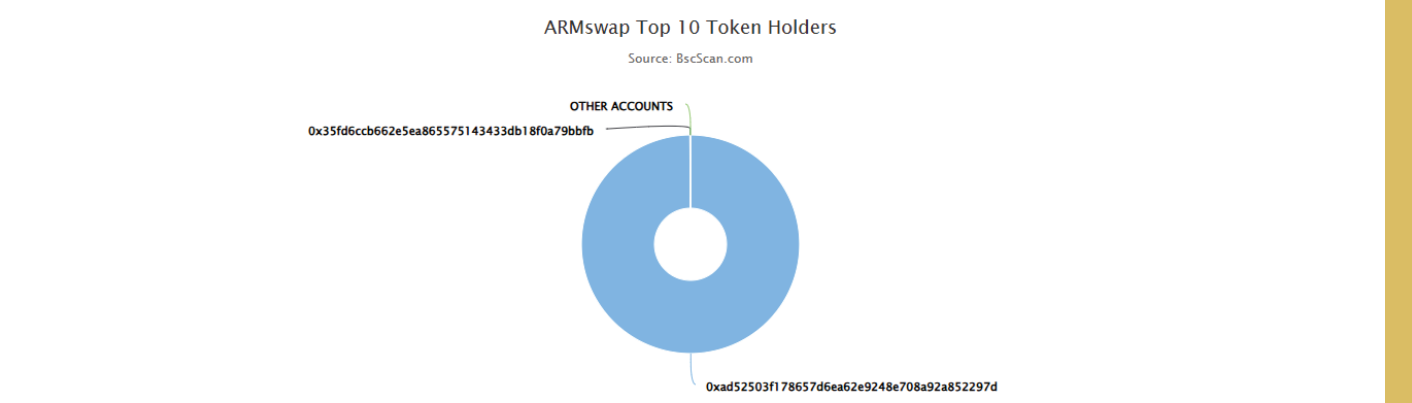
Rug Pull Risk

Liquidity:	N/A
Holders:	99.92% unlocked tokens

ARMSP TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,250,000,000.00 Tokens) of ARMswap

Token Total Supply: 1,250,000,000.00 Token | Total Token Holders: 2



(A total of 1,250,000,000.00 tokens held by the top 10 accounts from the total supply of 1,250,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xad52503F...2A852297D	1,249,000,000	99.9200%
2	0x35FD6CCB...f0a79bbfb	1,000,000	0.0800%

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.