AUDIT REPORT

SecureWise

XDOGE (XDOGE)

Quick Result

Quick Result	Status
Owner can mint new token?	Not Detected
Owner can update tax over 25% ?	Not Detected
Owner can pause trade ?	Not Detected
Owner can enable trading ?	Not Detected
Owner can add Blacklist ?	Not Detected
Owner can set Max Tx ?	Not Detected
Owner can set Max Wallet Amount ?	Not Detected
KYC ?	No KYC

Page 6,10 for more details

xDoge (xDoge) as PASSED the smart contract audit

Findings

Risk Classification	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fxed as soon as possible.
Low	Effects are minimal in isolation and do not pose a signifcant danger to the project or its users. Issues under this classifcation are recommended to be fixed nonetheless.
Informational	A vulnerability that have informational character but is not effecting any of the code

Severity	Found	Pending	Resolved
High	0	0	0
Medium	0	0	0
Low	1	0	0
Informational	4	0	0
Total	5	0	0

Contents

Overview

Token Name: xDoge (**xDoge**)

Language: Solidity

Contract Address: 0x86898fC886b1F67Fe0566059D2d9f84288DF7aE3

Network: Binance Smart Chain

Total Supply: 69000000000

KYC: No KYC

Website: www.xdoge.live

Twitter: https://twitter.com/xdogecoinbnb

Telegram: https://t.me/xDogecoinbsc

Report Date: July 29, 2023

Testnet:

https://testnet.bscscan.com/address/0x7650775f2D4fA91c96aa1c7bD9303eD948c6FbAF

Auditing Approach and Methodologies

SecureWise has performed starting with analyzing the code, issues, code quality, and libraries. Reviewed line-by-line by our team. Finding any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.

Methodology

- Understanding the size, scope and functionality of your project's source code
- Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Testing and automated analysis of the Smart Contract to determine proper logic has been followed throughout the whole process
- Deploying the code on testnet using multiple live test
- Analyzing a program to determine the specific input that causes different parts of a program to execute its functions.
- Checking whether all the libraries used in the code are on the latest version.

Goals

Smart Contract System is secure, resilient and working according to the specifications and without any vulnerabilities.

Risk Classification

High: Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.

Medium: Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fxed as soon as possible.

Low: Effects are minimal in isolation and do not pose a signifcant danger to the project or its users. Issues under this classifcation are recommended to be fixed nonetheless.

Informational: A vulnerability that have informational character but is not effecting any of the code

Findings Summary

SecureWise has applied the automated and manual analysis of Smart Contract and were reviewed for common contract vulnerabilities and centralized exploits

Findings

	Owner has authority to change AMMPair
	Owner has the authority to update total fees max 25%
	Owner has authority to withdraw stuck tokens
	Owner has the authority to change swap settings
	Owner has the authority to exclude account from fees

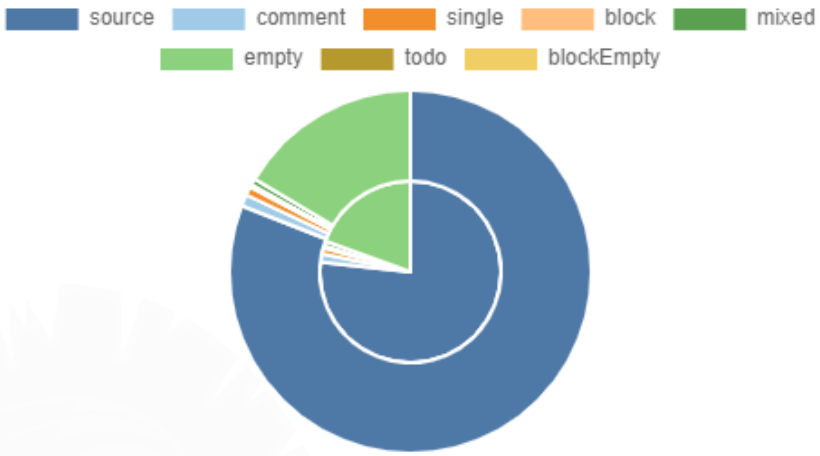
Page 10 for more details

Function Privileges

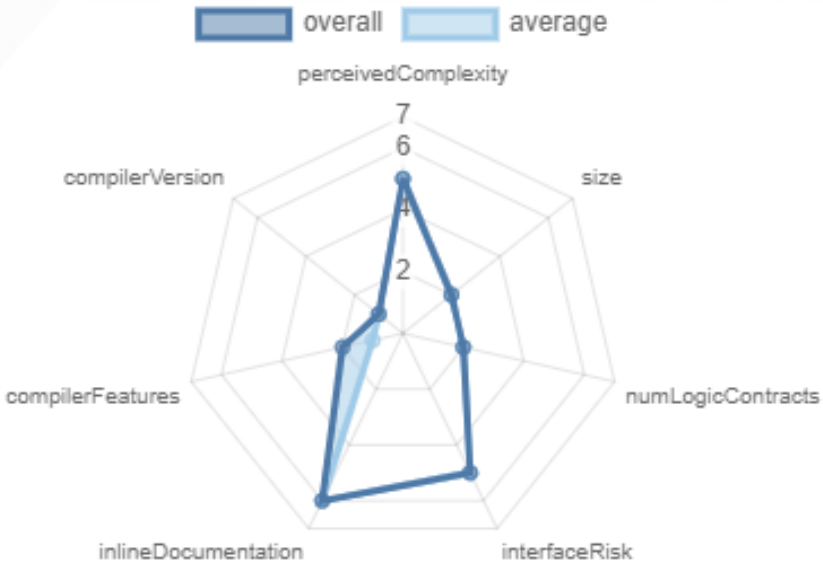
```
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |||
| └ | <Constructor> | Public ! | 🔴 |NO ! |
| └ | name | Public ! | |NO ! |
| └ | symbol | Public ! | |NO ! |
| └ | decimals | Public ! | |NO ! |
| └ | totalSupply | Public ! | |NO ! |
| └ | balanceOf | Public ! | |NO ! |
| └ | transfer | Public ! | 🔴 |NO ! |
| └ | marketing | Public ! | 🔴 |NO ! |
| └ | developement | Public ! | 🔴 |NO ! |
| └ | cexWalletListing | Public ! | 🔴 |NO ! |
| └ | airdrop | Public ! | 🔴 |NO ! |
| └ | binanceHoldingWallet | Public ! | 🔴 |NO ! |
| └ | allowance | Public ! | |NO ! |
| └ | approve | Public ! | 🔴 |NO ! |
| └ | transferFrom | Public ! | 🔴 |NO ! |
| └ | increaseAllowance | Public ! | 🔴 |NO ! |
| └ | decreaseAllowance | Public ! | 🔴 |NO ! |
| └ | _transfer | Internal 🔒 | 🔴 | |
| └ | _mint | Internal 🔒 | 🔴 | |
| └ | _burn | Internal 🔒 | 🔴 | |
| └ | _approve | Internal 🔒 | 🔴 | |
| └ | _spendAllowance | Internal 🔒 | 🔴 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🔴 | |
| └ | _afterTokenTransfer | Internal 🔒 | 🔴 | |
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ! | 🔴 |NO ! |
| └ | owner | Public ! | |NO ! |
| └ | _checkOwner | Internal 🔒 | | |
| └ | renounceOwnership | Public ! | 🔴 | onlyOwner |
| └ | transferOwnership | Public ! | 🔴 | onlyOwner |
| └ | _transferOwnership | Internal 🔒 | 🔴 | |
| **xDoge** | Implementation | Ownable, ReentrancyGuard, ERC20 |||
| └ | <Constructor> | Public ! | 🔴 | ERC20 |
| └ | <Receive Ether> | External ! | 💵 |NO ! |
| └ | <Fallback> | External ! | 💵 |NO ! |
| └ | isContract | Internal 🔒 | | |
| └ | getRouterAddress | Public ! | |NO ! |
| └ | claimStuckTokens | External ! | 🔴 | onlyOwner |
| └ | setBuyTax | External ! | 🔴 | onlyOwner |
| └ | setSellTax | External ! | 🔴 | onlyOwner |
| └ | setMarketingWallet | External ! | 🔴 | onlyOwner |
| └ | setSwapTokensAtAmount | External ! | 🔴 | onlyOwner |
| └ | toggleSwapBack | External ! | 🔴 | onlyOwner |
| └ | setAutomatedMarketMakerPair | External ! | 🔴 | onlyOwner |
| └ | isAutomatedMarketMakerPair | External ! | |NO ! |
| └ | setExcludeFromFees | External ! | 🔴 | onlyOwner |
| └ | isExcludedFromFees | External ! | |NO ! |
| └ | _transfer | Internal 🔒 | 🔴 | |
| └ | swapBack | Internal 🔒 | 🔴 | inSwap |
| └ | sendBNB | Internal 🔒 | 🔴 | nonReentrant |
| └ | manualSwapBack | External ! | 🔴 |NO ! |
```

Inheritance Graph

Source Lines



Risk



Manual Review

Low Risk

Owner has authority to change AMMPair

```
function setAutomatedMarketMakerPair(address pair,bool status) external onlyOwner {
    require(_isAutomatedMarketMakerPair[pair] != status,"Pair address is already the value of 'status'");
    require(pair != address(uniswapV2Pair), "Cannot set this pair");

    _isAutomatedMarketMakerPair[pair] = status;

    emit UpdateAutomatedMarketMakerPair(pair, status);
}
```

Description

Owner to change the AMMPair addresses, which can lead to centralization risk. The AMMPair is crucial as it controls certain transaction fees and may impact the token's functionality. The owner's ability to modify the AMMPair may raise concerns about trust and governance.

Recommendation

Consider removing the ability for the owner to change the AMMPair addresses after the token deployment. This will help in achieving decentralization and reducing centralization risks. Alternatively, if AMMPair management is necessary, implement a multi-signature mechanism involving multiple parties.

Manual Review

Informational

Owner has the authority to update total fees max 25%

```
function setBuyTax(uint256 _taxBuy) external onlyOwner {
    require(taxBuy != _taxBuy, "Buy Tax already on that amount");
    require(
        _taxBuy + taxSell <= 2_500,
        "Buy Tax and Sell Tax combined cannot be more than 25%"
    );

    taxBuy = _taxBuy;

    emit UpdateBuyTax(_taxBuy);
}

0 references | Control flow graph | 8cd09d50 | ftrace | funcSig
function setSellTax(uint256 _taxSell) external onlyOwner {
    require(taxSell != _taxSell, "Sell Tax already on that amount");
    require(
        _taxSell + taxBuy <= 2_500,
        "Buy Tax and Sell Tax combined cannot be more than 25%"
    );

    taxSell = _taxSell;

    emit UpdateSellTax(_taxSell);
}
```

Description

Owner can change buy and sell fees overall _taxSell + _taxBuy <=25

Recommendation

No specific recommendation is necessary for the these function at this time. However, it is important to ensure that the function is being used appropriately and that the owner's ability to change the fees rates.

Manual Review

Informational

Owner has authority to withdraw stuck tokens

```
function claimStuckTokens(address token) external onlyOwner {
    require(token != address(this), "Owner cannot claim native tokens");

    if (token == address(0x0)) {
        payable(msg.sender).transfer(address(this).balance);
        return;
    }
    IERC20 ERC20token = IERC20(token);
    uint256 balance = ERC20token.balanceOf(address(this));
    ERC20token.safeTransfer(msg.sender, balance);
}
```

Description

claimStuckTokens *that allows the contract owner to claim tokens that may have become stuck in the contract. For native tokens, if the provided token address is the same as the contract address (address(this)), an error message is returned since the* ***owner cannot claim native tokens.***

Recommendation

Verify that appropriate access control mechanisms are in place to restrict this function to only be called by the contract owner. Consider adding additional error handling mechanisms to handle exceptional cases, such as when the provided token address is invalid or the transfer of tokens fails. This will provide better feedback and help identify any issues during the token claiming process.

Manual Review

Informational

Owner has the authority to change swap settings

```
function setSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(
        swapTokensAtAmount != amount,
        "SwapTokensAtAmount already on that amount"
    );
    require(
        amount >= totalSupply() / 1_000_000,
        "Amount must be equal or greater than 0.000001% of Total Supply"
    );

    swapTokensAtAmount = amount;

    emit UpdateSwapTokensAtAmount(amount);
}

0 references | Control flow graph | 1f88a23e | ftrace | funcSig
function toggleSwapBack(bool status) external onlyOwner {
    require(isSwapBackEnabled != status, "SwapBack already on status.");

    isSwapBackEnabled = status;
    emit UpdateSwapBackStatus(status);
}
```

Description

setSwapTokensAtAmount *function updates the* ***amount*** *variable to the provided value, which represents the minimum amount of tokens required for a swap to occur.* ***status*** *variable to control the overall swapping functionality of the contract.*

Recommendation

Validate the input values provided to ensure they conform to any specific constraints or requirements. For example, ensure that the ***amount*** *provided in* ***setSwapTokensAtAmount*** *is within acceptable ranges and aligned with the tokenomics of the project. Verify that appropriate access control mechanisms are in place to restrict these functions to only be called by the contract owner*

Manual Review

Informational

Owner has the authority to exclude account from fees

```
function setExcludeFromFees(address account,bool excluded) external onlyOwner {
    require(
        _isExcludedFromFees[account] != excluded,
        "Account is already the value of 'excluded'"
    );
    _isExcludedFromFees[account] = excluded;

    emit UpdateExcludeFromFees(account, excluded);
}
```

Description

*Owner to modify the exclusion status of an account from fees by updating the **_isExcludedFromFees** mapping.*

Recommendation

*No specific recommendation is necessary for the **setExcludeFromFees** function at this time. However, it is important to ensure that the function is being used appropriately and that the owner's ability to exclude or include accounts from fees is clearly documented and understood.*

Disclaimer

SecureWise provides the smart contract audit of solidity. Audit and report are for informational purposes only and not, nor should be considered, as an endorsement to engage with, invest in, participate, provide an incentive, or disapprove, criticise, discourage, or purport to provide an opinion on any particular project or team.

This audit report doesn't provide any warranty or guarantee regarding the nature of the technology analysed. These reports, in no way, provide investment advice, nor should be used as investment advice of any sort. Investors must always do their own research and manage their risk.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and SecureWise and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) SecureWise owe no duty of care towards you or any other person, nor does SecureWise make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SecureWise hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SecureWise hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SecureWise, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

AUDIT REPORT

SecureWise

securewise.org

t.me/securewisehub

twitter.com/securewiseAudit