Cyberscope

Audit Report

X Capital

June 2022

Type	BEP20
Network	BSC
Address	0x3fa9b0b2ce48666c5be52e0325eece35aa6221a1
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	XToken
Compiler Version	v0.6.8+commit.0bbfe453
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0x3fa9b0b2ce48666c5be52e0325eece35aa6221a1
Symbol	XCAP
Decimals	9
Total Supply	10,000,000,000
Domain	xcap.finance

Source Files

Filename	SHA256
contract.sol	809d0220c3f41f6adf0405bb985931ae70d2bfb6912c4ae237bf1dfa2083fa4c

Audit Updates

Initial Audit	31st May 2022
Corrected phase 1	10th June 2022
Corrected phase 2	12th June 2022

Contract Analysis

🔴 Critical 🟠 Medium ⚪ Minor 🔵 Pass

Severity	Code	Description
🔵	ST	Contract Owner is not able to stop or pause transactions
🔵	OCTD	Contract Owner is not able to transfer tokens from specific address
🔵	OTUT	Owner Transfer User's Tokens
🔵	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
🔵	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
🔵	MT	Contract Owner is not able to mint new tokens
🔵	BT	Contract Owner is not able to burn tokens from specific wallet
🔵	BC	Contract Owner is not able to blacklist wallets from selling

Contract Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor

Severity	Code	Description
⚪	STC	Succeeded Transfer Check
⚪	MC	Missing Check (1/2)
🟠	MC	Missing Check (2/2)
⚪	L01	Public Function could be Declared External
⚪	L02	State Variables could be Declared Constant
⚪	L04	Conformance to Solidity Naming Conventions
⚪	L09	Dead Code Elimination

STC - Succeeded Transfer Check

Criticality	minor
Location	contract.sol

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
IBEP20(usdt).transfer(address(rewardPool), X);
```

Recommendation

The contract should check if the result of the transfer methods is successful.

MC - Missing Check (1/2)

Criticality	minor
Location	contract.sol#L910

Description

The contract is processing variables that have not properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The `nftAddr` could be any address. The setter method `setMintNft()` should implement some typical checks like zero value equality.

```
OriginNFT(nftAddr).mint(accountPair[to], XId1);
```

Recommendation

The contract should properly check the variables according to the required specifications

MC - Missing Check (2/2)

Criticality	medium
Location	contract.sol#L1048

Description

The contract is processing variables that have not properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The swapTokensForX enables the swapUnlock but it does not disable. Additionally, the swap does not check if it is already in swap. The `swapTokensForX` calls the `initialAccount` that calls the `OriginNFT(nftAddr).mint(accountPair[to], XId1);` if the `external OriginNFT(nftAddr).mint(...)` calls the swap, then a re-enter attack may caused.

```
function swapTokensForX(uint256 _amount, address tokenAddress)
    public
    payable
{
    swapUnlock = true;
    initialAccount(baseAccount, msg.sender);
```

Recommendation

The contract should prevent the swaps if the swap flag is enabled. The contract should also keep the swap flag updated.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L463,472,478,483,491,791,795,799,803,807,811,816,820,825,831,836,939,974,988,998,1008,1018,1027,1046,1105,1163,1171,1179,1187,1206,1212,1235

Description

Public functions that are never called by the contract should be declared external to save gas.

```
getUSDT
removeWhiteList
addWhiteList
getSellNotXFee
getBuyNotXFee
getSellXFee
getBuyXFee
swapXForToken
swapTokensForX
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L737,735,736,733

Description

Constant state variables should be declared constant to save gas.

```
_tTotal
_symbol
_name
_decimals
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L131,133,530,531,548,568,918,929,940,941,942,943,944,975,976,977,998,1008,1018,1027,1036,1046,760,761,762,763,764,765,767,768,769,770,773,774

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
XId1
XId0
Y3
X3
Y2
X2
Z1
Y1
X1
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L401,361,371,386,396,308,335,704

Description

Functions that are not used in the contract, and make the code's size bigger.

```
random
sendValue
isContract
functionCallWithValue
functionCall
_functionCallWithValue
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC165	Interface			
	supportsInterface	External		-
IERC721	Interface	IERC165		
	balanceOf	External		-
	ownerOf	External		-
	safeTransferFrom	External	✓	-
	transferFrom	External	✓	-
	approve	External	✓	-
	getApproved	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
IERC721Metadata	Interface	IERC721		
	name	External		-
	symbol	External		-
	tokenURI	External		-
IERC721Enum	Interface	IERC721		

erable				
	totalSupply	External		-
	tokenOfOwnerByIndex	External		-
	tokenByIndex	External		-
IERC721Receiver	Interface			
	onERC721Received	External	✓	-
OriginNFT	Interface			
	XIds	External		-
	mint	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	

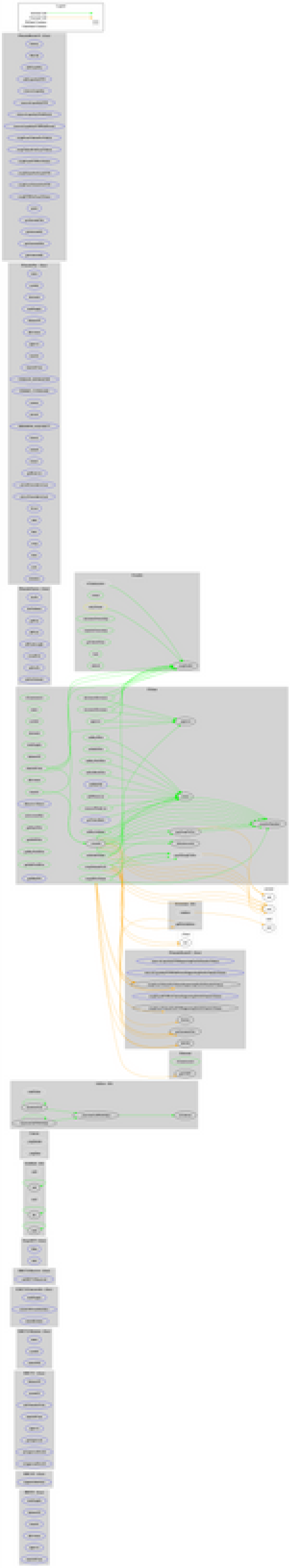
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	geUnlockTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
IPancakeFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IPancakePair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-

	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IPancakeRouter01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-

IPancakeRouter02	Interface	IPancakeRouter01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
XCommon	Library			
	random	Internal		
	getPairAddress	Internal		
XToken	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	<Receive Ether>	External	Payable	-
	_approve	Private	✓	
	_transfer	Private	✓	
	initialAccount	Internal	✓	
	_transferStandard	Private	✓	
	payXSwapTxFee	Internal	✓	

	paySwapTxFee	Internal	✓	
	setInitialToken	Public	✓	-
	getTokenBack	External	✓	-
	setKeyAddress	Public	✓	-
	setAccountPair	Public	✓	-
	setBuyXFee	Public	✓	-
	setSellXFee	Public	✓	-
	setBuyNotXFee	Public	✓	-
	setSellNotXFee	Public	✓	-
	setMintNft	External	✓	-
	swapTokensForX	Public	Payable	-
	swapXForToken	Public	✓	-
	getBuyXFee	Public		-
	getSellXFee	Public		-
	getBuyNotXFee	Public		-
	getSellNotXFee	Public		-
	getMintNft	External		-
	addWhiteList	Public	✓	-
	removeWhiteList	Public	✓	-
XInternal	Implementation			
	<Constructor>	Public	✓	-
	getUSDT	Public	✓	-

Contract Flow



Domain Info

Domain Name	xcap.finance
Registry Domain ID	63f6bd3e84e64fe1b6d13524713136c0-DONUTS
Creation Date	2022-03-18T02:02:15Z
Updated Date	2022-04-15T22:58:35Z
Registry Expiry Date	2024-03-18T02:02:15Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 2 months before the creation of the audit. It will expire in almost 2 years.

There is no public billing information, the creator is protected by the privacy settings.

Summary

X Capital is an interesting project that has a friendly and growing community. The audit mentions some vulnerability concerns and potential improvement. The fees can be set up to 25%.

Disclaimer

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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io