



Cyberscope

# Audit Report

## Seed

October 2022

Github <https://github.com/moonappxxx/moonapp-contracts>

Commit [849ced7b7b96948529d46f9295717ec5a1620f4f](#)

Audited by © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Roles</b>	<b>2</b>
<b>Contract Review</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Source Files</b>	<b>4</b>
<b>Contract Diagnostics</b>	<b>6</b>
<b>BLC - Business Logic Concern</b>	<b>7</b>
<b>Description</b>	<b>7</b>
<b>Recommendation</b>	<b>7</b>
<b>MC - Missing Check</b>	<b>8</b>
<b>Description</b>	<b>8</b>
<b>Recommendation</b>	<b>9</b>
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>10</b>
<b>Description</b>	<b>10</b>
<b>Recommendation</b>	<b>10</b>
<b>Contract Functions</b>	<b>11</b>
<b>Contract Flow</b>	<b>16</b>
<b>Domain Info</b>	<b>17</b>
<b>Summary</b>	<b>18</b>
<b>Disclaimer</b>	<b>19</b>
<b>About Cyberscope</b>	<b>20</b>

# Introduction

The Seed contract manages the vesting contracts for the investors.

## Roles

The “admin” role has the ability to vest a number of tokens for each investor. The investors can be added until the initialization of the vesting.

## Contract Review

<b>Contract Name</b>	Seed
<b>Compiler Version</b>	v0.8.11+commit.d7f03943
<b>Github</b>	<a href="https://github.com/moonappxxx/moonapp-contracts">https://github.com/moonappxxx/moonapp-contracts</a>
<b>Commit</b>	849ced7b7b96948529d46f9295717ec5a1620f4f
<b>Testing Deploy</b>	<a href="https://testnet.bscscan.com/token/0xD1EB5926261f849d633e7DdBBAa25DD40AB7Bf49">https://testnet.bscscan.com/token/0xD1EB5926261f849d633e7DdBBAa25DD40AB7Bf49</a>
<b>Domain</b>	<a href="https://moonapp.org">https://moonapp.org</a>

## Audit Updates

<b>Initial Audit</b>	3rd October 2022 <a href="https://github.com/cyberscope-io/audits/blob/main/1-xxx/v1/seed.pdf">https://github.com/cyberscope-io/audits/blob/main/1-xxx/v1/seed.pdf</a>
<b>Corrected</b>	7th October 2022

## Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249aa4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC20/ERC20.sol	5031430cc2613c32736d598037d3075985a2a09e61592a013dbd09a5bc2041b8
@openzeppelin/contracts/token/ERC20/extensions/draft-IERC20Permit.sol	3e7aa0e0f69eec8f097ad664d525e7b3f0a3fda8dcdd97de5433ddb131db86ef
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	0344809a1044e11ece2401b4f7288f414ea41fa9d1dad24143c84b737c9fc02e
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	fa36a21bd954262006d806b988e4495562e7b50420775e2aa0deecb596fd1902
@openzeppelin/contracts/utils/Address.sol	1e0922f6c0bf6b1b8b4d480dcabb691b1359195a297bde6dc5172e79f3a1f826

<b>@openzeppelin/contracts/utils/Context.sol</b>	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
<b>@openzeppelin/contracts/utils/math/Math.sol</b>	929523c09910460ad708c75878d89b9fbed12b65cb5d8b670200c793131072f4
<b>@openzeppelin/contracts/utils/math/SafeMath.sol</b>	0dc33698a1661b22981abad8e5c6f5ebca0dfe5ec14916369a2935d888ff257a
<b>contracts/Governed.sol</b>	216f03644d4e517caba4b44b8f3b74c358462601918a7be264790ef1cc1bde4c
<b>contracts/MoonappToken.sol</b>	bc938fcfe911c7df6871209c77bf053a2f1b4b9bab19f7c6d45a4feeae03e9d6
<b>contracts/Seed.sol</b>	fe4c012fc5babafc0ba3946fccc77d3b6b25b7f05cef69791a56f508be63fd27
<b>contracts/TokenVesting.sol</b>	66f193371f6346b5fa85acf98fbadcd29c4b5e7468728ab94d4f341d1e3c0fdc

# Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	BLC	Business Logic Concern	Unresolved
●	MC	Missing Check	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

## BLC - Business Logic Concern

<b>Criticality</b>	minor / informative
<b>Location</b>	contract.sol#L82
<b>Status</b>	Unresolved

### Description

The business logic seems peculiar. The implementation may not follow the expected behavior.

The token should give permission (approve) over the Seed address before transfer transactions.

```
SafeERC20.safeTransfer(  
    IERC20(token),  
    address(vesting),  
    tokensAmount  
);
```

### Recommendation

The team is advised to carefully check if the implementation follows the expected business logic.

The contract could approve the entire vesting amount before transfer transactions.



## MC - Missing Check

<b>Criticality</b>	minor / informative
<b>Location</b>	contract.sol#L47,57,27
<b>Status</b>	Unresolved

### 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 contract is not taking into consideration all the invested amount.

```
require(  
    amount <= availableTokens,  
    "ADD_INVESTOR: not enough tokens left."  
);
```

The following variables `_cliff`, `_releaseRate`, `_initialReleaseRate` are not properly sanitized before the vesting token initialization.

```
function releaseTokens(  
    uint256 _start,uint256 _cliff, uint256 _releaseRate, uint256 _initialReleaseRate  
) external {  
    //..  
    uint256 initialReleaseAmount = (tokensAmount / 100) *  
        _initialReleaseRate; // release % of the tokens on listing  
    TokenVesting vesting = new TokenVesting(  
        investors[i],  
        startTime,  
        _cliff,  
        _releaseRate,  
        initialReleaseAmount  
    );
```

The variable `availableTokens` is not properly sanitized before its initialization in the constructor.

```
constructor(address tokenAddress, uint256 _availableTokens) {  
    token = MoonappToken(tokenAddress);  
    admin = msg.sender;  
  
    availableTokens = _availableTokens * (10**18);  
}
```

## Recommendation

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

The contract should check if the total amount of tokens across investors is less than the available tokens.

It is recommended to pre-check variables before using them with other contracts.

- The variable `start` has to be greater than the current timestamp.
- The variable `cliff` has to be greater than zero
- The variable `releaseRate` have to be lower than 100%

The contract could embody a check on the contractor for the `availableTokens` variable to be greater than zero in order to avoid initializing the contract with zero available amount.

## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor / informative
<b>Location</b>	contracts/Seed.sol#L96,104
<b>Status</b>	Unresolved

### 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.

```
_investor
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
<b>ERC20</b>	Implementation	Context, IERC20, IERC20Met adata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	

	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>IERC20Permit</b>	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
<b>ERC20Burnable</b>	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeERC20</b>	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	safePermit	Internal	✓	
	_callOptionalReturn	Private	✓	

<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Math</b>	Library			
	max	Internal		
	min	Internal		
	average	Internal		
	ceilDiv	Internal		
	mulDiv	Internal		
	mulDiv	Internal		
	sqrt	Internal		
	sqrt	Internal		
<b>SafeMath</b>	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		

	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
<b>Governed</b>	Implementation			
	_initialize	Internal	✓	
	addOwnership	External	✓	onlyGovernor
	acceptOwnership	External	✓	-
<b>MoonappToken</b>	Implementation	ERC20, ERC20Burnable, Governed		
	<Constructor>	Public	✓	ERC20
	burnFrom	Public	✓	onlyGovernor
	mint	External	✓	onlyGovernor
<b>Seed</b>	Implementation			
	<Constructor>	Public	✓	-
	changeAdmin	External	✓	-
	addInvestor	External	✓	-
	releaseTokens	External	✓	-
	getInvestors	External		-
	getInvestorBalance	External		-
	getInvestorVestingAddress	External		-
<b>TokenVesting</b>	Implementation	Ownable		
	<Constructor>	Public	✓	-
	release	External	✓	-
	releasableAmount	Public		-
	vestedAmount	Public		-
	lockedAmount	External		-

# Contract Flow





## Domain Info

<b>Domain Name</b>	moonapp.org
<b>Registry Domain ID</b>	ebf9cc2ae696406f89ddb496f15a1e47-LROR
<b>Creation Date</b>	2022-01-23T16:44:59Z
<b>Updated Date</b>	2022-03-25T03:49:23Z
<b>Registry Expiry Date</b>	2023-01-23T16:44:59Z
<b>Registrar WHOIS Server</b>	http://whois.reg.com
<b>Registrar URL</b>	http://www.reg.com
<b>Registrar</b>	Registrar of Domain Names REG.RU LLC
<b>Registrar IANA ID</b>	1606

The domain was created 8 months before the creation of the audit. It will expire in 4 months.

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

# Summary

The smart contract analysis reported no critical or compiler issues. This audit focused on investigating security issues and potential improvements.

# 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.

Cyberscope 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>