CakeCrypt Token & Farm - Audit Report

S U M M A R Y

CakeCrypt intends to build a yield aggregator on the Binance Smart Chain.

For this audit we reviewed the project's Farm contract and StratX strategy contract. We reviewed the contracts at the following addresses on the Binance Smart Chain mainnet:

- Farm: 0xf3d5217d144201a7198a312dd08b6f9eb58b0403
- StratX: 0x19E34B8eE8b6D41edee57Cb79089EF3D75fc86eF

Notes of the Contracts:

- *User's deposited tokens will be forwarded to Strategy contract to earn yield while the user earns rewards.*
- *There are a 0.1% fee associated with making a deposit to or withdrawing from the contract.*
- *Funds held in the Strategy contract will then be forwarded for deposit into Pancakeswap farms for yield.*
- *Yield from deposits will be denominated in the deposit asset and is additional to a user's earned native token rewards.*
- *Rewards are generated via minting of the project's native token. 5.5% of rewards will be minted to the team.*
- *An emergency withdraw function is present, allowing users to withdraw their tokens while ignoring rewards in case of an issue.*
- *The project team can add different types of tokens for staking, and can update the reward rates for each token.*
- *The team can pause deposits to the contract, but not withdrawals.*
- *The team can also remove any token except the reward token from the Farm contract; and any token from the Strategy contract.*
- *Utilization of SafeMath (or similarily safe functions) to prevent overflow issues.*

Audit Findings Summary

- *No issues from external attackers were identified.*
- *Ensure trust in the team as they have some control in the ecosystem.*
- *Date: May 27th, 2021.*

Vulnerability Category	Notes	Result
Arbitrary Storage Write	N/A	PASS
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Flash Loans	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Oracles	N/A	PASS
Suicide	N/A	PASS

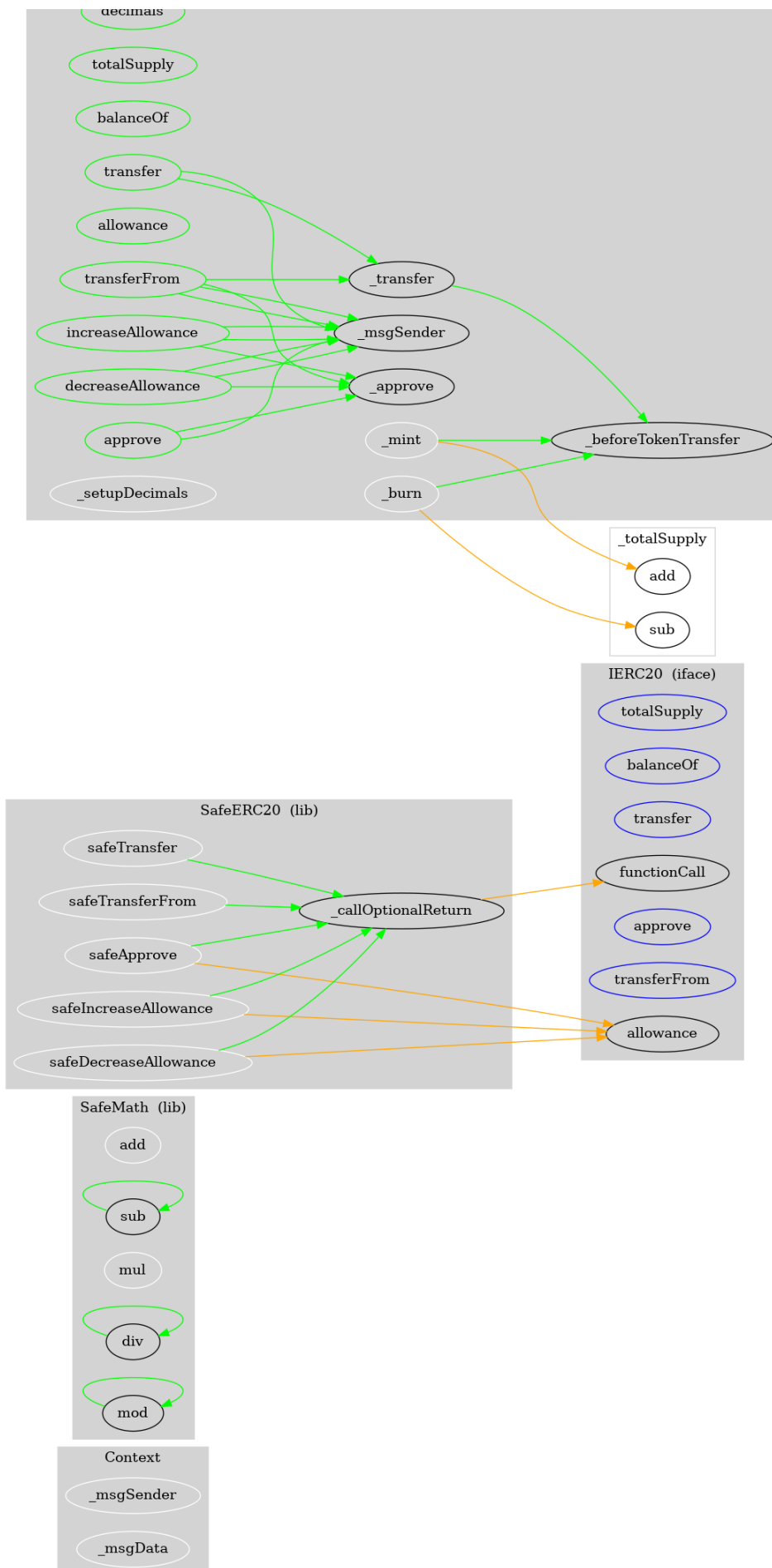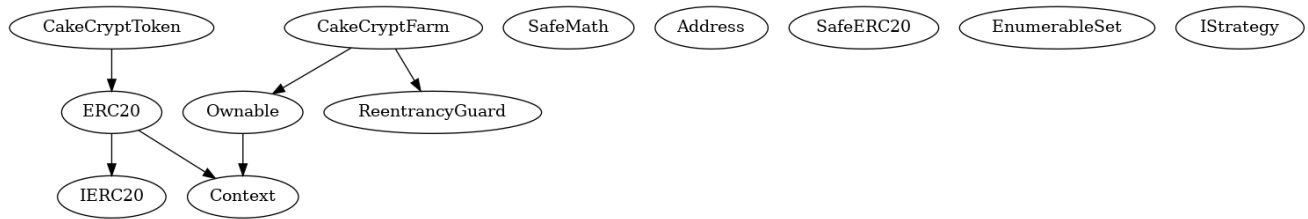| Vulnerability Category	Notes	Result
Unchecked Retval	N/A	PASS
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety		PASS

Details: CakeCyrpt Farm Contract
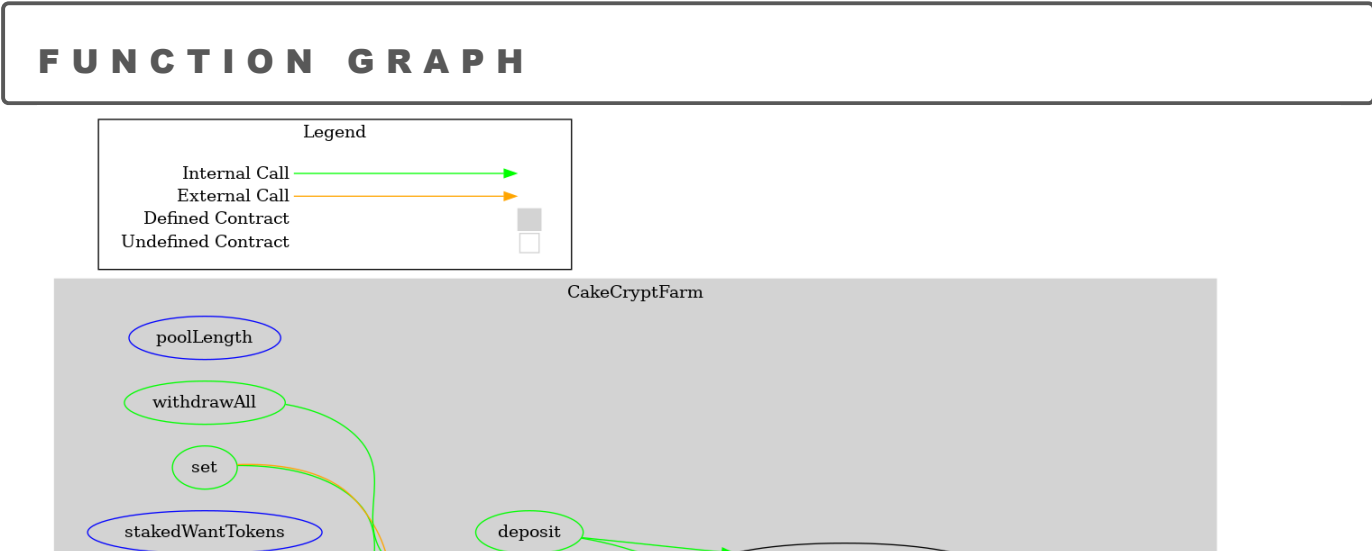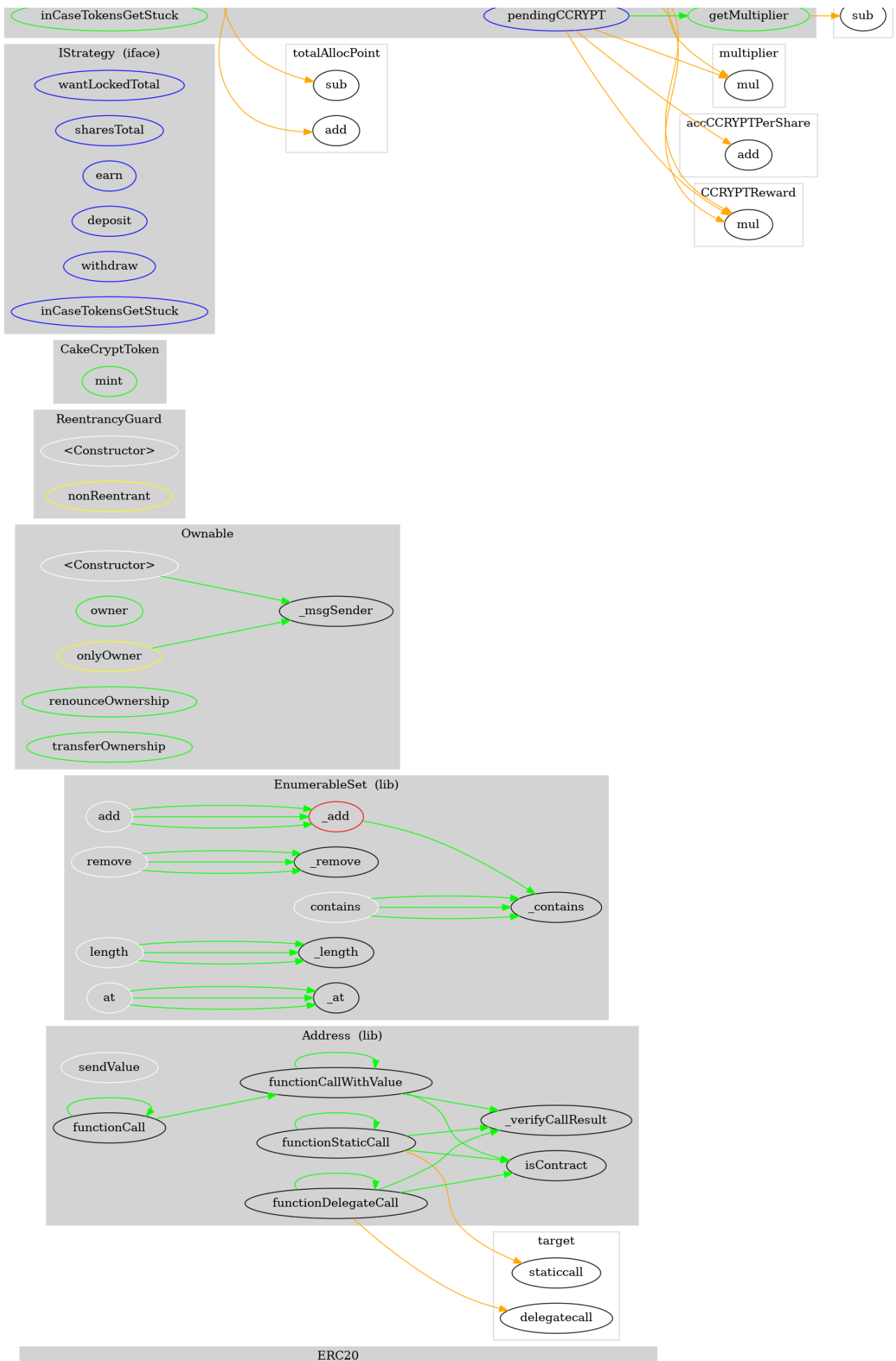
FUNCTION GRAPH

inCaseTokensGetStuck

IStrategy (iface)
- wantLockedTotal
- sharesTotal
- earn
- deposit
- withdraw
- inCaseTokensGetStuck

CakeCryptToken
- mint

ReentrancyGuard
- <Constructor>
- nonReentrant

Ownable
- <Constructor>
- owner
- onlyOwner
- _msgSender
- renounceOwnership
- transferOwnership

EnumerableSet (lib)
- add → _add
- remove → _remove
- contains → _contains
- length → _length
- at → _at

Address (lib)
- sendValue
- functionCallWithValue
- functionCall
- functionStaticCall
- functionDelegateCall
- _verifyCallResult
- isContract

pendingCCRYPT
- getMultiplier → sub
- multiplier → mul
- accCCRYPTPerShare → add
- CCRYPTReward → mul

totalAllocPoint
- sub
- add

target
- staticcall
- delegatecall

ERC20

FUNCTIONS OVERVIEW

```
($) = payable function

# = non-constant function


Int = Internal

Ext = External

Pub = Public


  +  Context

     -  [Int] _msgSender

     -  [Int] _msgData


  + [Lib] SafeMath

     -  [Int] add

     -  [Int] sub

     -  [Int] sub

     -  [Int] mul

     -  [Int] div

     -  [Int] div

     -  [Int] mod

     -  [Int] mod


  + [Int] IERC20

       -  [Ext] totalSupply

       -  [Ext] balanceOf
```

```
         - [Ext] transferFrom #

    +  ERC20 (Context, IERC20)
       - [Pub]   #
       - [Pub] name
       - [Pub] symbol
       - [Pub] decimals
       - [Pub] totalSupply
       - [Pub] balanceOf
       - [Pub] transfer #
       - [Pub] allowance
       - [Pub] approve #
       - [Pub] transferFrom #
       - [Pub] increaseAllowance #
       - [Pub] decreaseAllowance #
       - [Int] _transfer #
       - [Int] _mint #
       - [Int] _burn #
       - [Int] _approve #
       - [Int] _setupDecimals #
       - [Int] _beforeTokenTransfer #

    + [Lib] Address
       - [Int] isContract
       - [Int] sendValue #
       - [Int] functionCall #
       - [Int] functionCall #
       - [Int] functionCallWithValue #
       - [Int] functionCallWithValue #
       - [Int] functionStaticCall
       - [Int] functionStaticCall
       - [Int] functionDelegateCall #
```

```
            - [Int] safeTransfer #
            - [Int] safeTransferFrom #
            - [Int] safeApprove #
            - [Int] safeIncreaseAllowance #
            - [Int] safeDecreaseAllowance #
            - [Prv] _callOptionalReturn #


    + [Lib] EnumerableSet
            - [Prv] _add #
            - [Prv] _remove #
            - [Prv] _contains
            - [Prv] _length
            - [Prv] _at
            - [Int] add #
            - [Int] remove #
            - [Int] contains
            - [Int] length
            - [Int] at
            - [Int] add #
            - [Int] remove #
            - [Int] contains
            - [Int] length
            - [Int] at
            - [Int] add #
            - [Int] remove #
            - [Int] contains
            - [Int] length
            - [Int] at


    +  Ownable (Context)
            - [Int]   #
            - [Pub] owner
```

```
   +  ReentrancyGuard
      - [Int]  #


   +  CakeCryptToken (ERC20)
      - [Pub] mint #


   + [Int] IStrategy
      - [Ext] wantLockedTotal
      - [Ext] sharesTotal
      - [Ext] earn #
      - [Ext] deposit #
      - [Ext] withdraw #
      - [Ext] inCaseTokensGetStuck #


   +  CakeCryptFarm (Ownable, ReentrancyGuard)
      - [Ext] poolLength
      - [Pub] add #
         - modifiers: onlyOwner
      - [Pub] set #
         - modifiers: onlyOwner
      - [Pub] getMultiplier
      - [Ext] pendingCCRYPT
      - [Ext] stakedWantTokens
```

Details: StratX Stategy Contract

INHERITENCE CHART

FUNCTIONS OVERVIEW

GO HOME