smart state

new generation of
smart contract audit

CYBER ARENA

METAVERSE

Cyber Arena

Oct 05

2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

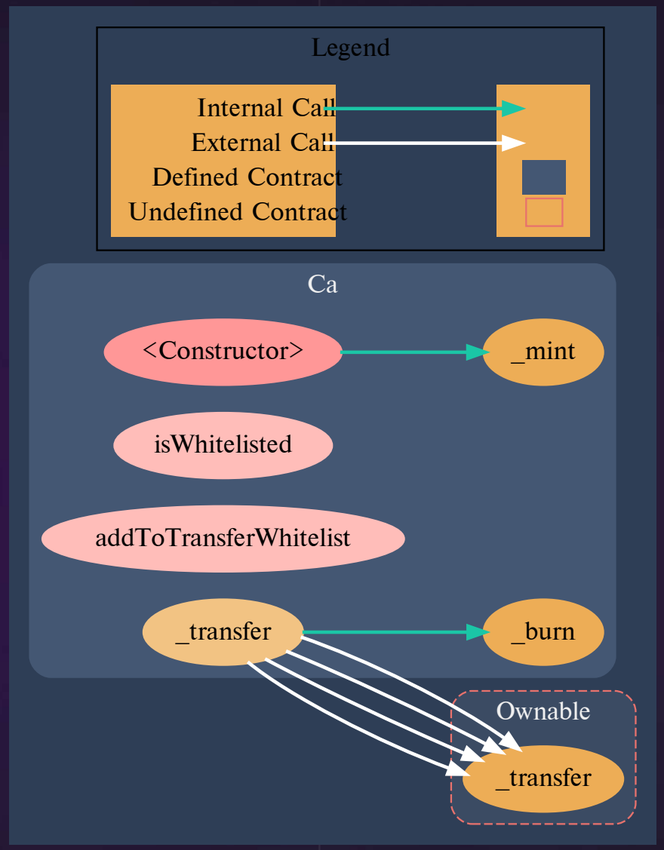
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool Asset Security (backdoors in the underlying ERC-20)
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

STRUCTURE OF CONTRACT

CA.SOL

CONTRACT METHODS ANALYSIS:

- isWhitelisted(address owner) public view returns (bool)
  Vulnerabilities not detected
- addToTransferWhitelist(address[] calldata addresses)
  Vulnerabilities not detected
- transfer(address to, uint256 amount) public virtual override returns (bool)
  Vulnerabilities not detected



Pic. 1.1
Ca.sol

STRUCTURE OF CONTRACT

STAKING.SOL

CONTRACT METHODS ANALYSIS:

- initialize(IERC20Upgradeable _stakingToken, uint16 _penaltyDays, uint16 _penaltyBP, address _treasury)
  Vulnerabilities not detected

TOKEN FLOW

- stake(uint128 _amount)
  Vulnerabilities not detected

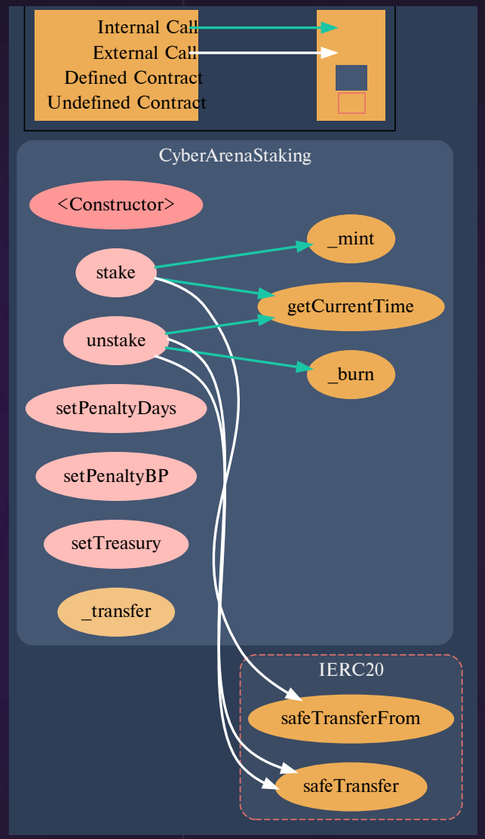
Tokens in, public

TOKEN FLOW

- unstake(uint256 _stakeIndex)
  Vulnerabilities not detected

Tokens out, public

- setPenaltyDays(uint16 _penaltyDays)
  Vulnerabilities not detected



Pic. 1.2
Staking.sol

- `setPenaltyBP(uint16 _penaltyBP)`
  Vulnerabilities not detected

- `setTreasury(address _treasury)`
  Vulnerabilities not detected

- `_transfer(address _from, address _to, uint256 _amount)`
  Vulnerabilities not detected

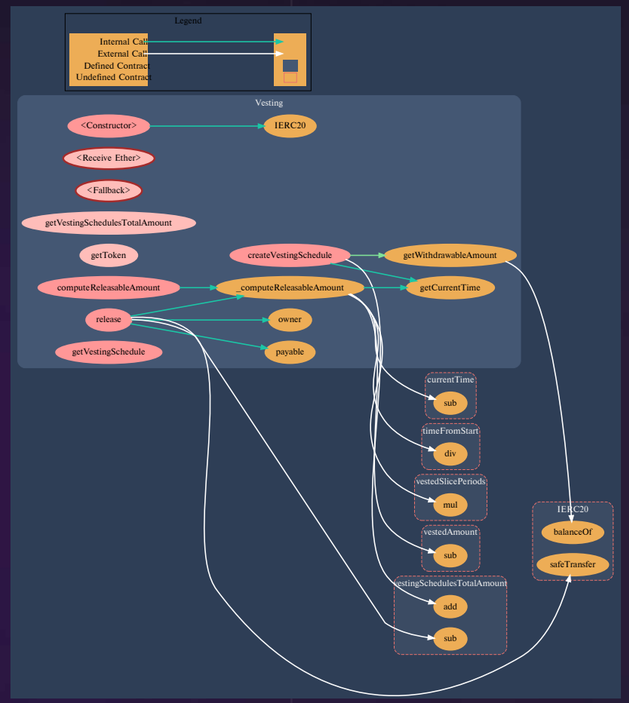
- `getCurrentTime()`
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

VESTING.SOL

CONTRACT METHODS ANALYSIS:

- onlyIfVestingScheduleExists(address addr)
  Vulnerabilities not detected
- etVestingSchedulesTotalAmount()
  Vulnerabilities not detected
- getToken()
  Vulnerabilities not detected
- createVestingSchedule(address _beneficiary, uint256 _start, uint256 _duration, uint256 _slicePeriodSeconds, uint256 _amount)
  Vulnerabilities not detected



Pic. 1.3
Vesting.sol

TOKEN FLOW

- release(address addr, uint256 amount)
  Vulnerabilities not detected

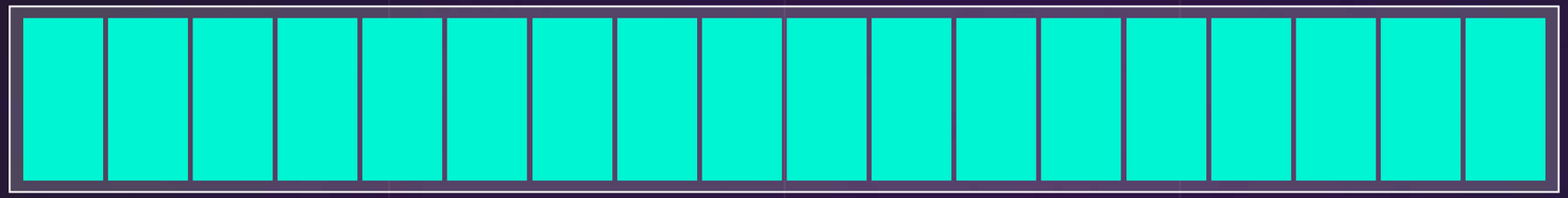
Tokens out, public

- computeReleasableAmount(address addr)
  Vulnerabilities not detected
- getVestingSchedule(address addr)
  Vulnerabilities not detected
- getWithdrawableAmount()
  Vulnerabilities not detected
- _computeReleasableAmount(VestingSchedule memory vestingSchedule)
  Vulnerabilities not detected
- getCurrentTime()
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimization	Bytecode hash (SHA 256)
Ca.sol	0.8.7	200	070ab3d3547130f57d49d9430c77ab5475830ae0d598c236fde5356ee01ee3b5
Staking.sol	0.8.7	200	7a79263f974df1e205d32d4c3b24ab1a79149f3cfffae0df5988e08d93edcac5
Vesting.sol	0.8.7	200	ba92dc482592808c20c23da84774f624e859e671e8204b758ae345d29b96f2fd

PROJECT EVALUATION



10/10

GET IN TOUCH

info@smartstate.tech
smartstate.tech

View this report on smartstate.tech