Audit Report for **GHCrowdFund**
Date: 03 February 2024
Audit result: **Passed with High Risk**

Token Address: --

Name: --

Symbol: --

Decimals: --

Network: --

Token Type: --

Owner: --

Deployer: --

Token Supply: --

Checksum: A2032c616934aeb47e6039f76b20d2h5

Testnet:
https://testnet.bscscan.com/address/0x6c84fc477c39884685d9af962cb07afc786597a1#code

Token Overview:

Buy Fee: 0%

Sell Fee: 0%

Transfer Fee: 0%

Fee Privilege: Owner

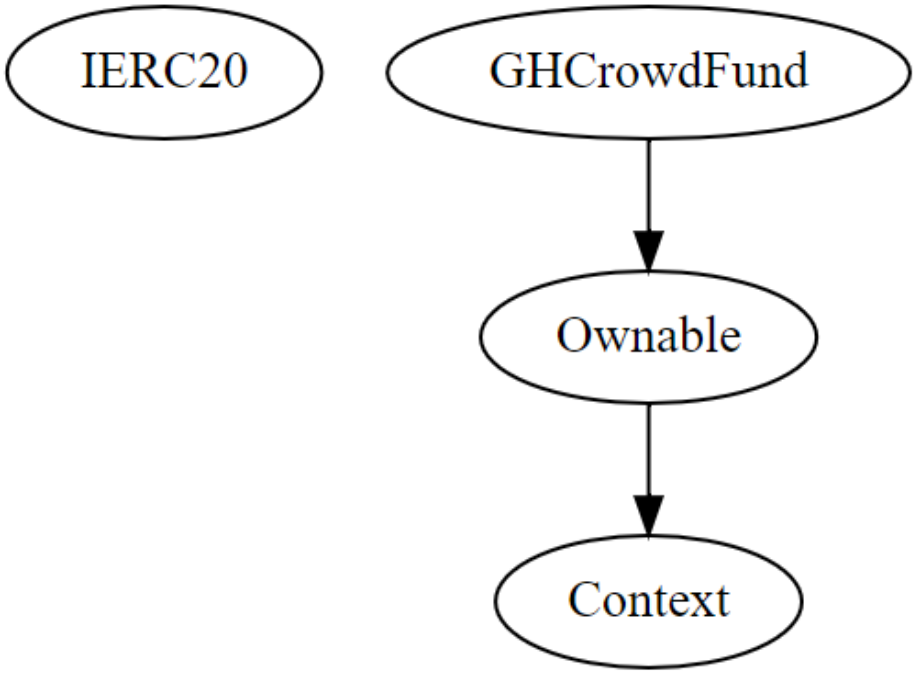
Ownership: Owned

Minting: None

Max Tx: No

Blacklist: No

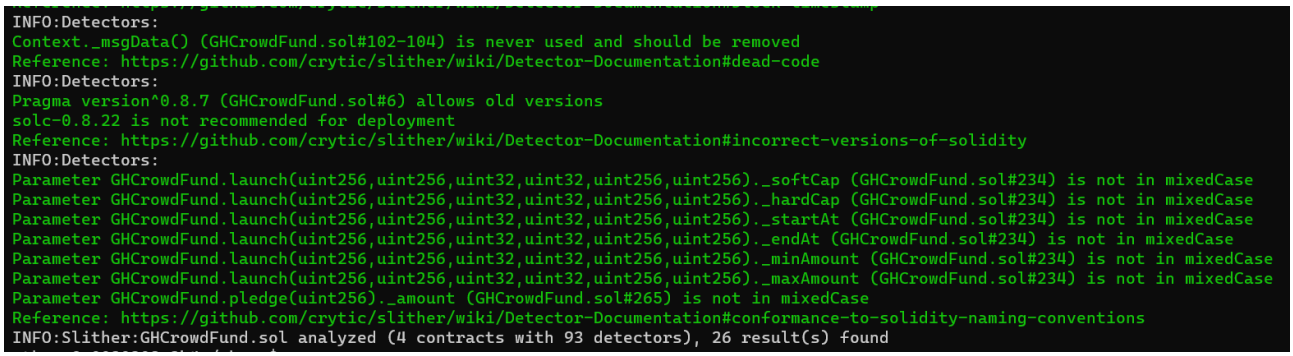
Inheritance Tree



Static Analysis

A static analysis of the code was performed using Slither. No issues were found.

```
INFO:Detectors:
Reentrancy in GHCrowdFund.pledge(uint256) (GHCrowdFund.sol#265-289):
        External calls:
        - token.transferFrom(msg.sender,address(this),_amount) (GHCrowdFund.sol#276)
        State variables written after the call(s):
        - pledged += _amount (GHCrowdFund.sol#284)
        GHCrowdFund.pledged (GHCrowdFund.sol#196) can be used in cross function reentrancies:
        - GHCrowdFund.claim() (GHCrowdFund.sol#292-304)
        - GHCrowdFund.launch(uint256,uint256,uint32,uint32,uint256,uint256) (GHCrowdFund.sol#234-252)
        - GHCrowdFund.pledge(uint256) (GHCrowdFund.sol#265-289)
        - GHCrowdFund.pledged (GHCrowdFund.sol#196)
        - GHCrowdFund.refund() (GHCrowdFund.sol#307-320)
        - GHCrowdFund.refundTo(address) (GHCrowdFund.sol#323-336)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-1
INFO:Detectors:
Reentrancy in GHCrowdFund.pledge(uint256) (GHCrowdFund.sol#265-289):
        External calls:
        - token.transferFrom(msg.sender,address(this),_amount) (GHCrowdFund.sol#276)
        State variables written after the call(s):
        - pledgeList.push(msg.sender) (GHCrowdFund.sol#280)
        - pledgedAmount[msg.sender] += _amount (GHCrowdFund.sol#285)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
```



Functional Tests

Router (PCS V2):

1- Approve (passed):
https://testnet.bscscan.com/tx/0x395e4a739ec63f3c1759dffd5223e093d0504c9cd50f2d73f6270b7110849395

2- Set Fee (passed):
https://testnet.bscscan.com/tx/0xe3d54dddbf60854d1bb700260f2502479343310c472848c0001fbeb6239e0c68

3- Set open trade (passed):
https://testnet.bscscan.com/tx/0x4e582d8ed44dede8b0cfee12a6fd4fa69fdabfedf54f759a465e47c135db90f4

4- Set dev (passed):
https://testnet.bscscan.com/tx/0x71b8d8eab8f9b6d0e4ca5bdd9a73f7d260dc1782dcf5ca819bc5fadefb8b6d55

5- Set Dividend (passed):
https://testnet.bscscan.com/tx/0x94c0eb916aceced03f6a18c6948fec97fc619c332f2f2be9b2114e86bc75739e

Ownership Privileges:

- The owner can transfer ownership.
- The owner can renounce ownership.
- The owner can launch.
- The owner can cancel.
- The owner can claim.
- The owner can refundTo.

Findings:
Critical: 0
High: 1
Medium: 0
Low: 0
Informational & Optimizations: 1

Centralization – The owner can lock the token.

Severity: High
Function: Launch
Status: Open
Overview:
The owner can lock user funds by changing these values. For example, if the end time and hardcap is manipulated after the campaign has started then in that case the funds will be locked and all the claims and refunds in the contract will be under the owner's discretion.

```
function launch(uint256 _softCap, uint256 _hardCap, uint32 _startAt, uint32 _endAt,
uint256 _minAmount, uint256 _maxAmount) external onlyOwner {
        // Validation checks for start and end Campaign

        require(_startAt >= block.timestamp, "Start time is less than current Block
Timestamp");
        require(_endAt > _startAt, "End time is less than Start time");

        // Set campaign parameters
        softCap = _softCap;
        hardCap = _hardCap;
        pledged = 0;
        startAt = _startAt;
        endAt = _endAt;
        minAmount = _minAmount;
        maxAmount = _maxAmount;
        claimed = false;
        canceled = false;

        // Emit Launch event
        emit Launch(msg.sender, _softCap, _hardCap, _startAt, _endAt, _minAmount,
_maxAmount);
    }
```

Suggestion:
It is recommended not to change these values once the campaign is launched.

Optimization

Severity: **Optimization**
Subject: Remove unused code.
Status: Open
Overview:
Unused variables are allowed in Solidity, and they do. not pose a direct security issue. It is the best practice. though to avoid them.

```
function _msgData() internal view virtual returns (bytes calldata) {
        return msg.data;
    }
```