Aderyn Analysis Report

This report was generated by Aderyn, a static analysis tool built by Cyfrin, a blockchain security company. This report is not a substitute for manual audit or security review. It should not be relied upon for any purpose other than to assist in the identification of potential security vulnerabilities.

Table of Contents

Summary

Files Summary

Key	Value
.sol Files	2
Total nSLOC	67

Files Details

Filepath	nSLOC
src/CharityRegistry.sol	24
src/GivingThanks.sol	43
Total	**67**

Issue Summary

Category	No. of Issues
High	2
Low	7

High Issues

H-1: `abi.encodePacked()` should not be used with dynamic types when passing the result to a hash function such as `keccak256()`

Use `abi.encode()` instead which will pad items to 32 bytes, which will prevent hash collisions (e.g. `abi.encodePacked(0x123,0x456)` => `0x123456` => `abi.encodePacked(0x1,0x23456)`, but `abi.encode(0x123,0x456)` => `0x0...1230...456`). Unless there is a compelling reason, `abi.encode` should be preferred. If there is only one argument to `abi.encodePacked()` it can often be cast to `bytes()` or `bytes32()` instead. If all arguments are strings and or bytes, `bytes.concat()` should be used instead.

▶ 2 Found Instances

- Found in src/GivingThanks.sol Line: 38

```
            abi.encodePacked(
```

- Found in src/GivingThanks.sol Line: 53

```
        return string(abi.encodePacked("data:application/json;base64,",
base64Json));
```

H-2: Functions send eth away from contract but performs no checks on any address.

Consider introducing checks for `msg.sender` to ensure the recipient of the money is as intended.

▶ 1 Found Instances

- Found in src/GivingThanks.sol Line: 21

```
    function donate(address charity) public payable {
```

Low Issues

L-1: Solidity pragma should be specific, not wide

Consider using a specific version of Solidity in your contracts instead of a wide version. For example, instead of `pragma solidity ^0.8.0;`, use `pragma solidity 0.8.0;`

▶ 2 Found Instances

- Found in src/CharityRegistry.sol Line: 2

```
pragma solidity ^0.8.0;
```

- Found in src/GivingThanks.sol Line: 2

```
pragma solidity ^0.8.0;
```

L-2: Missing checks for `address(0)` when assigning values to address state variables

Check for `address(0)` when assigning values to address state variables.

▶ 2 Found Instances

- Found in src/CharityRegistry.sol Line: 29

```
        admin = newAdmin;
```

- Found in src/GivingThanks.sol Line: 57

```
        registry = CharityRegistry(_registry);
```

L-3: `public` functions not used internally could be marked `external`

Instead of marking a function as `public`, consider marking it as `external` if it is not used internally.

▶ 6 Found Instances

- Found in src/CharityRegistry.sol Line: 13

```
    function registerCharity(address charity) public {
```

- Found in src/CharityRegistry.sol Line: 17

```
    function verifyCharity(address charity) public {
```

- Found in src/CharityRegistry.sol Line: 23

```
    function isVerified(address charity) public view returns (bool) {
```

- Found in src/CharityRegistry.sol Line: 27

```
    function changeAdmin(address newAdmin) public {
```

- Found in src/GivingThanks.sol Line: 21

```
    function donate(address charity) public payable {
```

- Found in src/GivingThanks.sol Line: 56

```
    function updateRegistry(address _registry) public {
```

L-4: Using `ERC721::_mint()` can be dangerous

Using `ERC721::_mint()` can mint ERC721 tokens to addresses which don't support ERC721 tokens. Use `_safeMint()` instead of `_mint()` for ERC721.

▶ 1 Found Instances

- Found in src/GivingThanks.sol Line: 26

```
        _mint(msg.sender, tokenCounter);
```

L-5: PUSH0 is not supported by all chains

Solc compiler version 0.8.20 switches the default target EVM version to Shanghai, which means that the generated bytecode will include PUSH0 opcodes. Be sure to select the appropriate EVM version in case you intend to deploy on a chain other than mainnet like L2 chains that may not support PUSH0, otherwise deployment of your contracts will fail.

▶ 2 Found Instances

- Found in src/CharityRegistry.sol Line: 2

```
pragma solidity ^0.8.0;
```

- Found in src/GivingThanks.sol Line: 2

```
pragma solidity ^0.8.0;
```

L-6: State variable changes but no event is emitted.

State variable changes in this function but no event is emitted.

▶ 5 Found Instances

- Found in src/CharityRegistry.sol Line: 13

```
    function registerCharity(address charity) public {
```

- Found in src/CharityRegistry.sol Line: 17

```
    function verifyCharity(address charity) public {
```

- Found in src/CharityRegistry.sol Line: 27

```
    function changeAdmin(address newAdmin) public {
```

- Found in src/GivingThanks.sol Line: 21

```
    function donate(address charity) public payable {
```

- Found in src/GivingThanks.sol Line: 56

```
    function updateRegistry(address _registry) public {
```

L-7: State variable could be declared immutable

State variables that are should be declared immutable to save gas. Add the `immutable` attribute to state variables that are only changed in the constructor

▶ 1 Found Instances

- Found in src/GivingThanks.sol Line: 13

```

```

```
    address public owner;
```