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	1
Total nSLOC	40

Files Details

Filepath	nSLOC
src/URSWAP.sol	40
Total	**40**

Issue Summary

Category	No. of Issues
High	0
Low	4

Low Issues

L-1: Centralization Risk for trusted owners

Contracts have owners with privileged rights to perform admin tasks and need to be trusted to not perform malicious updates or drain funds.

3 Found Instances

- Found in src/URSWAP.sol Line: 21

```
function burn(uint256 amount) public onlyOwner {
```

- Found in src/URSWAP.sol Line: 27

```
function setWhitelist(address account, bool status) public onlyOwner {
```

- Found in src/URSWAP.sol Line: 32

```
function disableWhitelist() public onlyOwner {
```

L-2: Unsafe ERC20 Operations should not be used

ERC20 functions may not behave as expected. For example: return values are not always meaningful. It is recommended to use OpenZeppelin's SafeERC20 library.

2 Found Instances

- Found in src/URSWAP.sol Line: 41

```
return super.transfer(to, amount);
```

- Found in src/URSWAP.sol Line: 53

```
return super.transferFrom(msg.sender, to, amount);
```

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/URSWAP.sol Line: 12

```
function initialize(address initialOwner) public initializer {
```

- Found in src/URSWAP.sol Line: 21

```
function burn(uint256 amount) public onlyOwner {
```

- Found in src/URSWAP.sol Line: 27

```
function setWhitelist(address account, bool status) public onlyOwner {
```

- Found in src/URSWAP.sol Line: 32

```
function disableWhitelist() public onlyOwner {
```

- Found in src/URSWAP.sol Line: 37

```
function transfer(address to, uint256 amount) public override returns (bool) {
```

- Found in src/URSWAP.sol Line: 45

```
function transferFrom(
```

L-4: Large literal values multiples of 10000 can be replaced with scientific notation

Use `e` notation, for example: `1e18`, instead of its full numeric value.

1 Found Instances

- Found in src/URSWAP.sol Line: 17

```
_mint(initialOwner, 500000000 * 10 ** decimals());
```