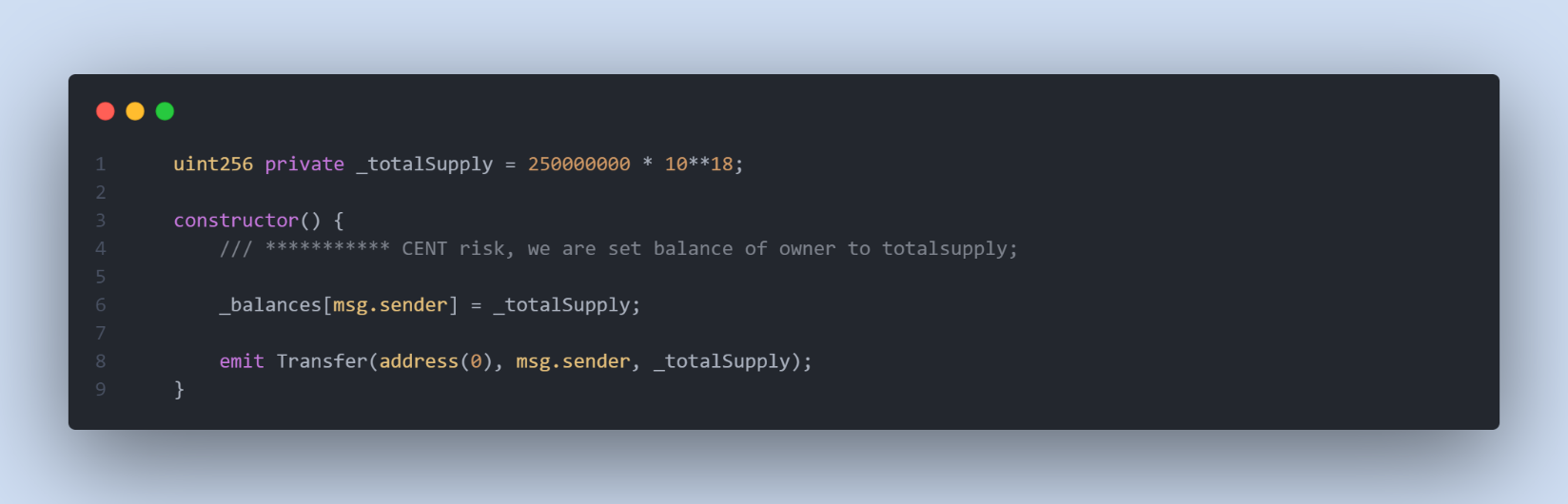
Source : https://github.com/OrcaniaEdyRepo/Orcania-DEX/

# **OCA.sol**

# **Medium severity issues**

* **Centralization Risks**

**In the constructor function, we set the deployer wallet balance to 250,000,000 tokens. This could be a centralization risk as the deployer can distribute tokens without obtaining the consensus of the community.**



Remediation

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key.

# **low severity issues**

* **Zero Address Validation check**

**Text

Description automatically generated**

**In the transfer function, we accept the recipient, as an argument. it’s important to check the value of this address before transferring any token to it.**

Remediation

**We need to check the recipient address, it should not be a zero address.**

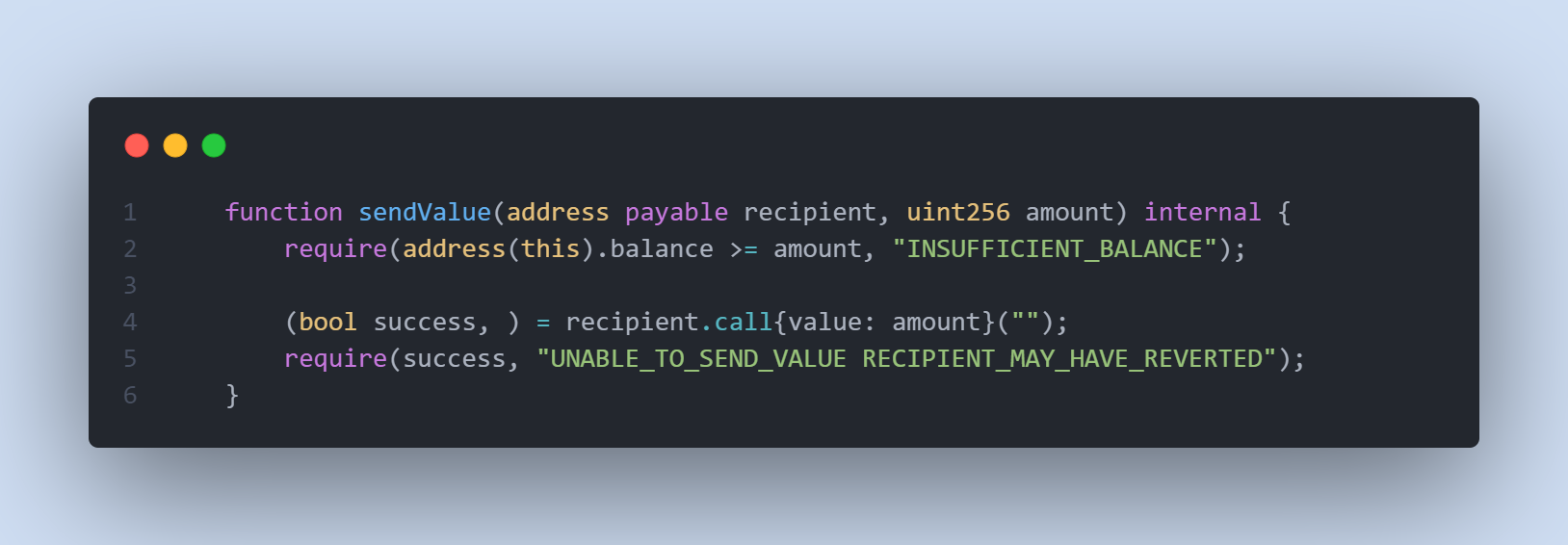
# **DEX.sol**

# **High severity issues**

* **Missing check for Reentrancy attack**

**In the multiple functions, we used .call to send ether .**

**reentrancy attack happens when a contract send ether to an unknown address. Then, an attacker could write a contract in an external address which includes malicious code in the fallback function. Thus, when a contract send ether to that address, it will invoke the malicious code. The malicious code usually executes a function in the vulnerable contract and performs non-expected operations by developers.**

****

Remediation

**We recommend applying OpenZeppelin ReentrancyGuard library nonReentrant modifier for the above functions.**

# **Medium severity issues**

* **unchecked returned value**

**we used OCA.transfer multiple times to transfer the OCA token, but we don’t check the return value from this function.**

Text

Description automatically generated

Remediation

We recommend checking returned value from this function to be true;