Coinsult

Advanced Manual Smart Contract Audit

Project: Moox (StakeManager)
Website: https://moox.one

🟢 **Low-risk**
1 low-risk code issues found

🟡 **Medium-risk**
0 medium-risk code issues found

🔴 **High-risk**
0 high-risk code issues found

Contract address
0xBb6e7648182298cC6DCFB5781eF8084eB1FD0de1

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Not deployed yet

Source code

Coinsult was commissioned by Moox to perform an audit based on the following smart contract:

https://github.com/mooxtoken/moox-contract/blob/master/contracts/Stake Manager.sol (private)

Note: This project uses openzeppelin imports. While we do check the full contract for vulnerabilities at the time of the audit, we can not ensure the correctness of these imported modules.

Manual Code Review

🟢 **Low-risk**

1 low-risk code issues found.
Could be fixed, will not bring problems.

- The return value of an external transfer/transferFrom call is not checked

```solidity
function safeBusdTransfer(address _to, uint256 _amount) private {
    uint256 busdBalance = BUSD.balanceOf(address(this));

    if (_amount > busdBalance) {
        BUSD.transfer(_to, busdBalance);
    } else {
        BUSD.transfer(_to, _amount);
    }
}
```

🟡 **Medium-risk**

0 medium-risk code issues found.
Should be fixed, could bring problems.

🔴 **High-risk**

0 high-risk code issues found
Must be fixed, and will bring problems.

Extra notes by the team

Note: This project uses openzeppelin imports. While we do check the full contract for vulnerabilities at the time of the audit, we can not ensure the correctness of these imported modules.

🟡 Dev notes can be deleted upon deployment

Contract Snapshot

```solidity
contract StakeManager is ReentrancyGuard {
    using SafeMath for uint256;

    IBEP20 public constant BUSD =
IBEP20(0xe9e7CEA3DedcA5984780Bafc599bD69ADd087D56);

    // The Moox token
    Moox public moox;

    // The LP token for MOOX/WBNB
    IPancakeswapPair public lpToken;

    // Total deposited BUSD for awarding
    uint256 public totalDepositedBusd;

    // Deposited BUSD amount on the last reward update
    uint256 public lastRewardDepositedBusd;

    // Accumulated BUSD per share
    uint256 public accBusdPerShare;

    // Info of each user that stakes tokens
    mapping(address => UserInfo) public userInfo;

    struct UserInfo {
        uint256 amount; // How many MOOX/WBNB LP tokens the user has
provided
        uint256 rewardDebt; // Reward debt
    }

    event Deposit(address indexed user, uint256 amount);
    event EmergencyWithdraw(address indexed user, uint256 amount);
    event Withdraw(address indexed user, uint256 amount);

    constructor(Moox _moox, IPancakeswapPair _lpToken) {
        moox = _moox;
        lpToken = _lpToken;
    }

    function busdDeposit(uint256 _amount) external nonReentrant {
```
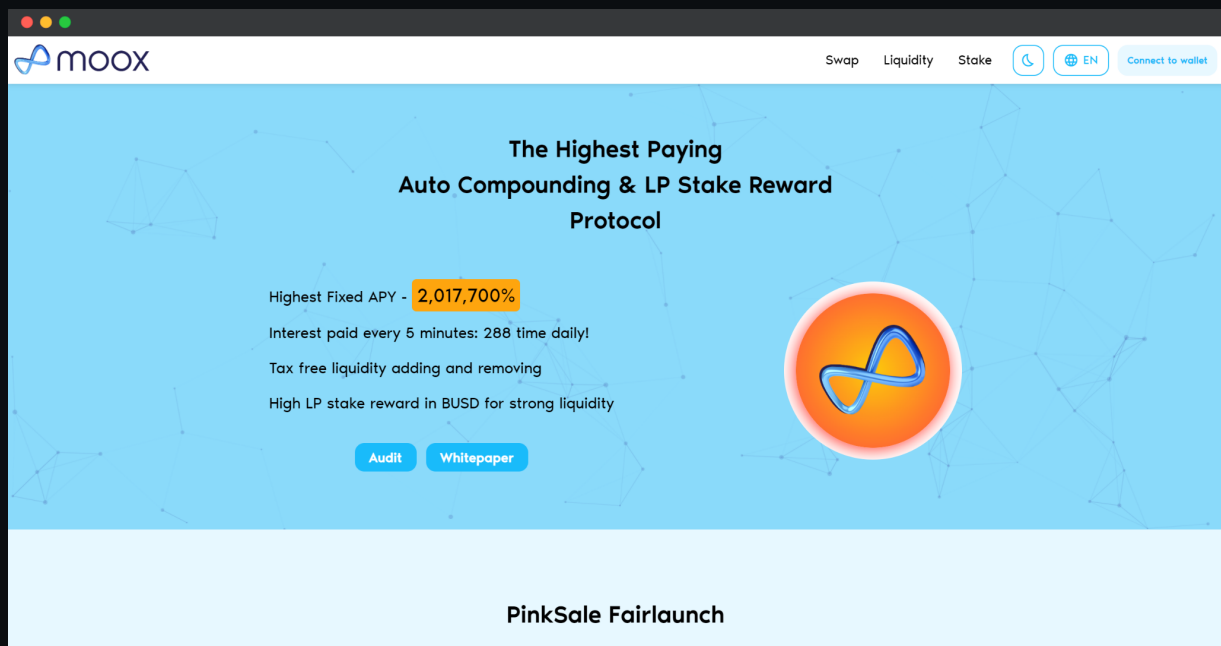
Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.

- 🟢 Mobile Friendly
- 🟢 Contains no jQuery errors
- 🟢 SSL Secured
- 🟢 No major spelling errors

Loading speed: 86%