Coinsult

Advanced Manual Smart Contract Audit

Project: NFTStaking
Website: https://nftstaking.art/

Low-risk	Medium-risk	High-risk
4 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract address
0x49F85CE3071db45f37eEbD0C9174674358F40FEE

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

Rank	Address	Quantity (Token)	Percentage
1	0xd8c735a308c1d80547fe8327369381aa593e9df5	850,000,000	85.0000%
2	0x66830f5b034440ba7ce299663f013467afa168a6	70,000,000	7.0000%
3	0xde4cbc50be9a5409031204d5f690698dc22da92d	50,000,000	5.0000%
4	0xea5cf3d28679736484e76495001041c80015421c	20,000,000	2.0000%
5	0x8230a36cf1bfd9b168e3f4986cce1507a56c39c6	10,000,000	1.0000%

Source code

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

https://bscscan.com/address/0x49F85CE3071db45f37eEbD0C9174674358F40FEE#code

Manual Code Review

🟢 Low-risk

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

- Contract contains Reentrancy vulnerabilities:
  _transfer(address,address,uint256)
  Additional information: This combination increases risk of malicious intent. While it may be justified by some complex mechanics (e.g. rebase, reflections, buyback).
  More information: Slither

```
function _transfer(
    address sender,
    address recipient,
    uint256 amount
) internal virtual {
    require(sender != address(0), "ERC20: transfer from the zero address");
    require(recipient != address(0), "ERC20: transfer to the zero address");

    _beforeTokenTransfer(sender, recipient, amount);

    uint256 senderBalance = _balances[sender];
    require(senderBalance >= amount, "ERC20: transfer amount exceeds balance");
    unchecked {
        _balances[sender] = senderBalance - amount;
    }
    _balances[recipient] += amount;

    emit Transfer(sender, recipient, amount);

    _afterTokenTransfer(sender, recipient, amount);
}
```

- Literals with many digits are difficult to read and review.
  Use: Ether suffix, Time suffix, or The scientific notation

```
constructor(string memory name, string memory symbol) ERC20(name, symbol) {
  _mint(msg.sender, 1000000000 * 1 ether);
  sellTax = 5;
  buyTax = 5;
  transferTax = 5;
  tradeCooldown = 15;
}
```

- Contract contains empty functions
  Remove empty functions.

```
  function _afterTokenTransfer(
      address from,
      address to,
      uint256 amount
  ) internal virtual {}
```

- No zero address validation
  Check if the new address is not the zero address.

```
function updateDepositWallet(address newDepositWallet) external onlyOwner {
  depositWallet = newDepositWallet;
}

function updateRewardWallet(address newWallet) external onlyOwner {
  rewardWallet = newWallet;
}
```

🟡 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

- Owner can blacklist
- Owner can add trading cooldown without a limit

```
function setCooldownForTrades(uint8 _tradeCooldown) external onlyOwner {
  tradeCooldown = _tradeCooldown;
  emit changeCooldown(_tradeCooldown);
}
```

- Owner can change taxes with a limit

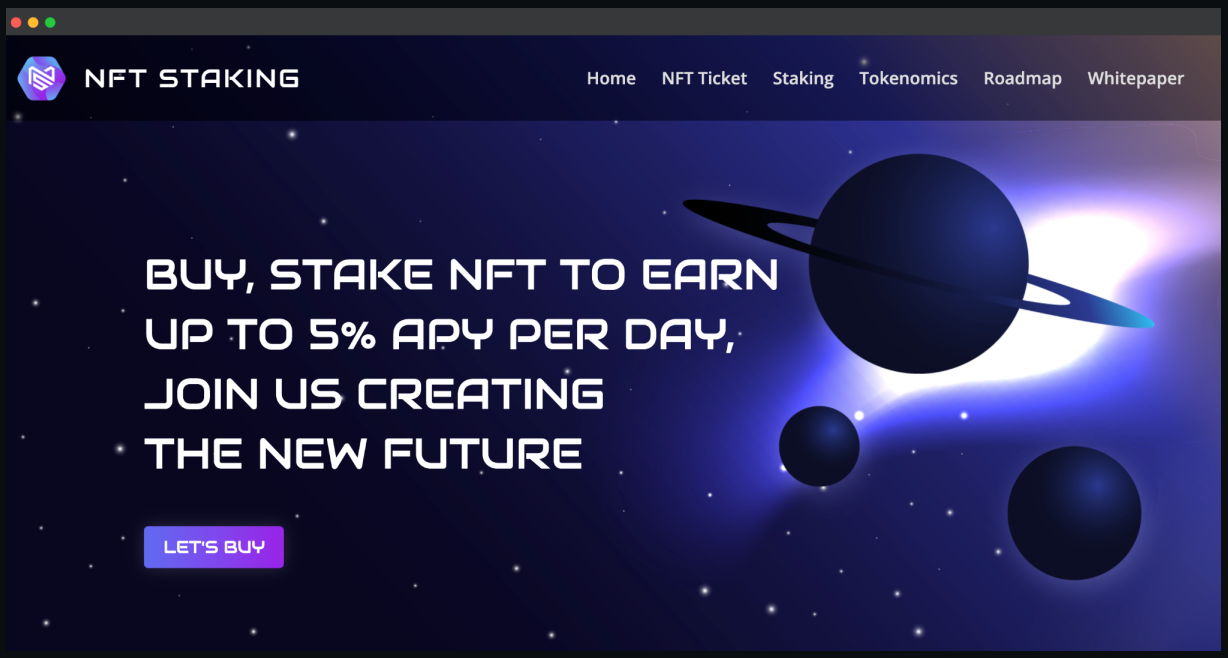
```
function setTaxes(uint8 _sellTax, uint8 _buyTax, uint8 _transferTax) external
onlyOwner {
  require(_sellTax < 10);
  require(_buyTax < 10);
  require(_transferTax < 10);
  sellTax = _sellTax;
  buyTax = _buyTax;
  transferTax = _transferTax;
  emit changeTax(_sellTax,_buyTax,_transferTax);
}
```

- Owner can exclude from fees
- There are a lot of dev notes (commented code) which can be removed

Contract Snapshot

```
contract ERC20 is Context, IERC20, IERC20Metadata {
    mapping(address => uint256) private _balances;

    mapping(address => mapping(address => uint256)) private _allowances;

    uint256 private _totalSupply;

    string private _name;
    string private _symbol;

    /**
     * @dev Sets the values for {name} and {symbol}.
     *
     * The default value of {decimals} is 18. To select a different value for
     * {decimals} you should overload it.
     *
     * All two of these values are immutable: they can only be set once during
     * construction.
     */
    constructor(string memory name_, string memory symbol_) {
        _name = name_;
        _symbol = symbol_;
    }

    /**
     * @dev Returns the name of the token.
     */
    function name() public view virtual override returns (string memory) {
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a shorter version of the
     * name.
     */
    function symbol() public view virtual override returns (string memory) {
        return _symbol;
    }

    /**
     * @dev Returns the number of decimals used to get its user representation.
     * For example, if `decimals` equals `2`, a balance of `505` tokens should
```

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: 91%

Rug-pull Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Locked Liquidity (no liquidity yet)

🟡 Large unlocked wallets

- Note: Tokens not distributed yet

🔴 No doxxed Team

Honeypot Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Ability to sell

🟡 Owner is not able to pause the contract

🟡 Owner can add trading cooldown without a limit

Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.