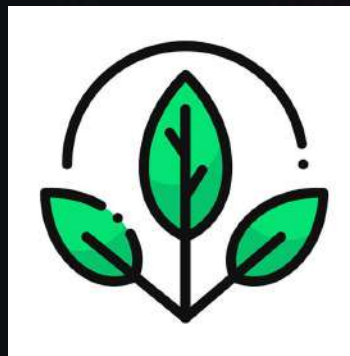




Coinsult

Advanced Manual Smart Contract Audit



Project: Merit

Website: <https://merit.global/>

Low-Risk

2 low-risk code
issues found

Medium-Risk

0 medium-risk code
issues found

High-Risk

0 high-risk code
issues found

Contract Address

0xA8f446e24eE7fCA342f4162C2932fB184C797a38

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

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	0xceecbe05aa5aa5f973e972d41ed168d63d12baf2	100,000,000	100.0000%

Source Code

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

<https://bscscan.com/address/0xa8f446e24ee7fca342f4162c2932fb184c797a38#code>

Manual Code Review

In this audit report we will highlight all these issues:

Low-Risk

2 low-risk code
issues found

Medium-Risk

0 medium-risk code
issues found

High-Risk

0 high-risk code
issues found

The detailed report continues on the next page...

● **Low-Risk:** Could be fixed, will not bring problems.

No zero address validation for some functions

Detect missing zero address validation.

```
function setAddress(address _stakingAddress,address _lpAddress,address _burnAddress) public onlyOwner {
    stakingAddress = _stakingAddress;
    lpAddress = _lpAddress;
    burnAddress = _burnAddress;
}
```

Recommendation

Check that the new address is not zero.

Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }

    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

Bob calls updateOwner without specifying the newOwner, so Bob loses ownership of the contract.

● **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function setFee(uint256 _stakingFee,uint256 _lpFee,uint256 _burnFee) public onlyOwner{
    stakingFee = _stakingFee;
    lpFee = _lpFee;
    burnFee = _burnFee;
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }

    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

updateOwner() has no event, so it is difficult to track off-chain changes in the buy price.

Owner privileges

- Owner can change max transaction amount
- Owner can set fees higher than 25%
- Owner can exclude from fees
- Owner can pause the contract
- Owner can blacklist addresses

Extra notes by the team

No notes

Contract Snapshot

```
contract StandardToken is IERC20, Ownable, BaseToken {
    using SafeMath for uint256;

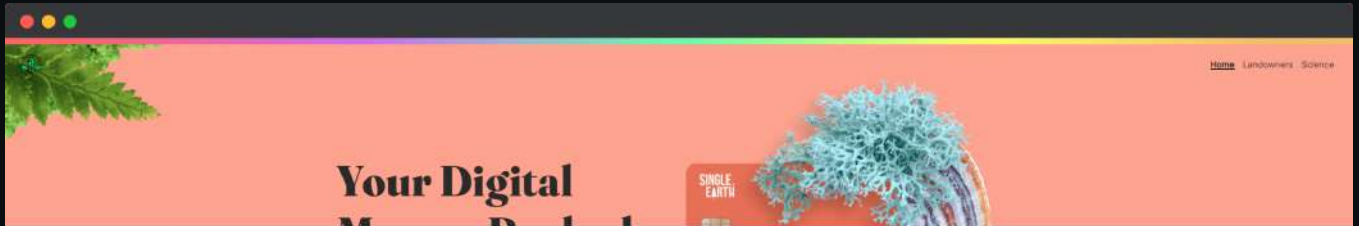
    uint256 public constant VERSION = 1;

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

    string private _name;
    string private _symbol;
    uint8 private _decimals;
    uint256 private _totalSupply;
    uint256 public stakingFee;
    uint256 public lpFee;
    uint256 public burnFee;
    address public stakingAddress;
    address public lpAddress;
    address public burnAddress;
    mapping (address => bool) public isExcludedFromFee;
    mapping (address => bool) public blacklist;
```

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
- Does not contain jQuery errors
- SSL Secured
- No major spelling errors

Project Overview

● Not KYC verified by Coinsult

AUDITED
BY COINSULT.NET

