Coinsult

Advanced Manual Smart Contract Audit

Project: Tribalwars
Website: http://www.tribalwars.world

● **Low-risk**
4 low-risk code issues found

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

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

Contract address
0x379906705fE1195ff1119800ee1B69D9CDbc225e

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	0x529729ec44f5f33dd33177d0827d8046d2b34a40	590,560,000	59.0560%
2	0x29992e82a07263ca991dcbeae1531aaa62021931	409,440,000	40.9440%

Source code

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

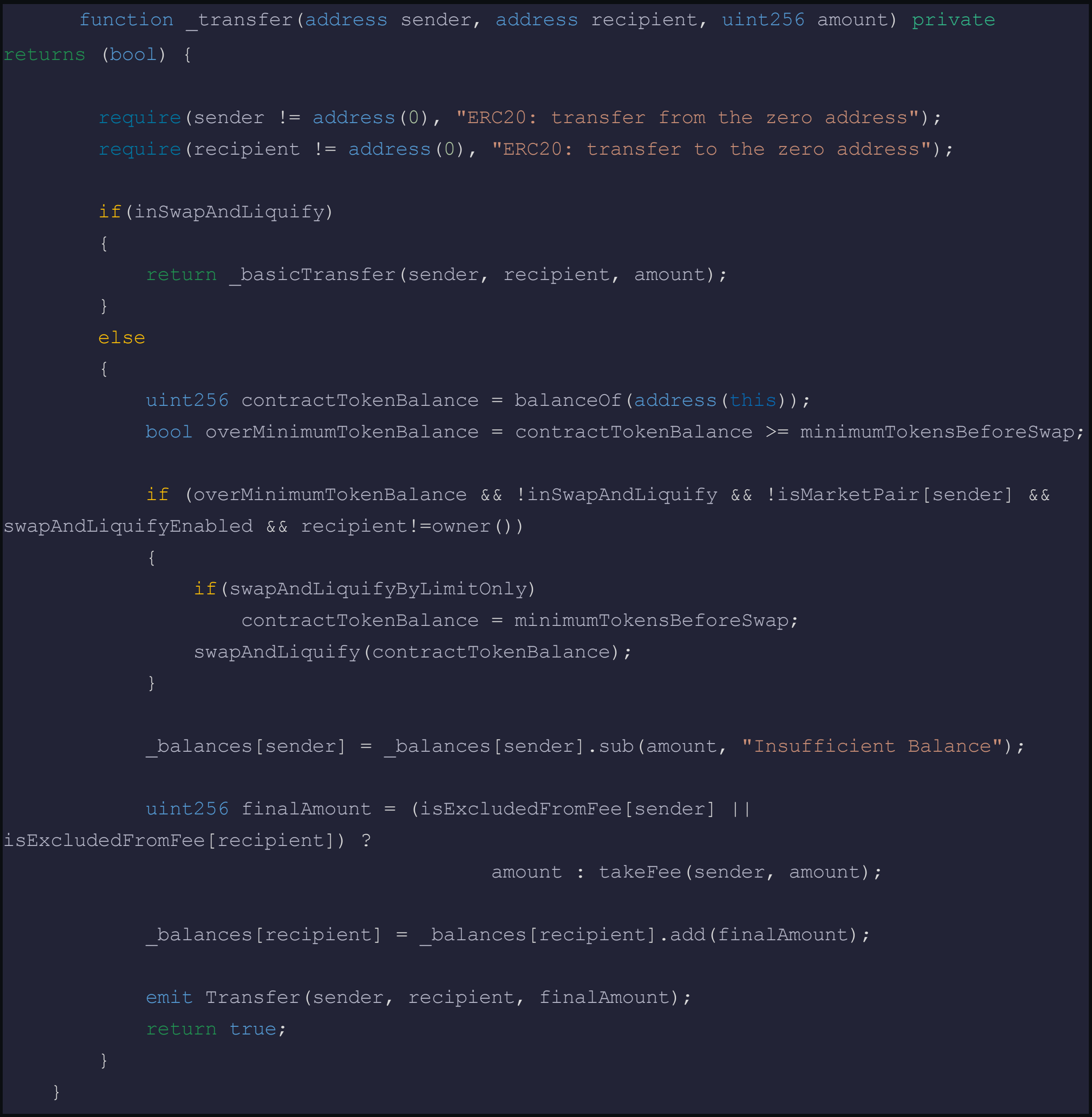
https://bscscan.com/address/0x379906705fE1195ff1119800ee1B69D9CDbc225e#code

Manual Code Review

● Low-risk

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

- Contract contains Reentrancy vulnerabilities:
  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) private
returns (bool) {

        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");

        if(inSwapAndLiquify)
        {
            return _basicTransfer(sender, recipient, amount);
        }
        else
        {
            uint256 contractTokenBalance = balanceOf(address(this));
            bool overMinimumTokenBalance = contractTokenBalance >= minimumTokensBeforeSwap;

            if (overMinimumTokenBalance && !inSwapAndLiquify && !isMarketPair[sender] &&
swapAndLiquifyEnabled && recipient!=owner())
            {
                if(swapAndLiquifyByLimitOnly)
                    contractTokenBalance = minimumTokensBeforeSwap;
                swapAndLiquify(contractTokenBalance);
            }

            _balances[sender] = _balances[sender].sub(amount, "Insufficient Balance");

            uint256 finalAmount = (isExcludedFromFee[sender] ||
isExcludedFromFee[recipient]) ?
                                         amount : takeFee(sender, amount);

            _balances[recipient] = _balances[recipient].add(finalAmount);

            emit Transfer(sender, recipient, finalAmount);
            return true;
        }
    }
```

- Avoid relying on block.timestamp

block.timestamp can be manipulated by miners.

```
function getTime() public view returns (uint256) {
        return block.timestamp;
    }
```

- Missing zero address validation
  Check that the new address is not the zero address.

```
       function setIsExcludedFromFee(address account, bool newValue)
public onlyOwner {
        isExcludedFromFee[account] = newValue;
    }
```

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

```
uint256 private _totalSupply = 1000000000 * 10**_decimals;
```

● 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 change the router address.

- Fees can be set up to 100% for both buy and sell fees.

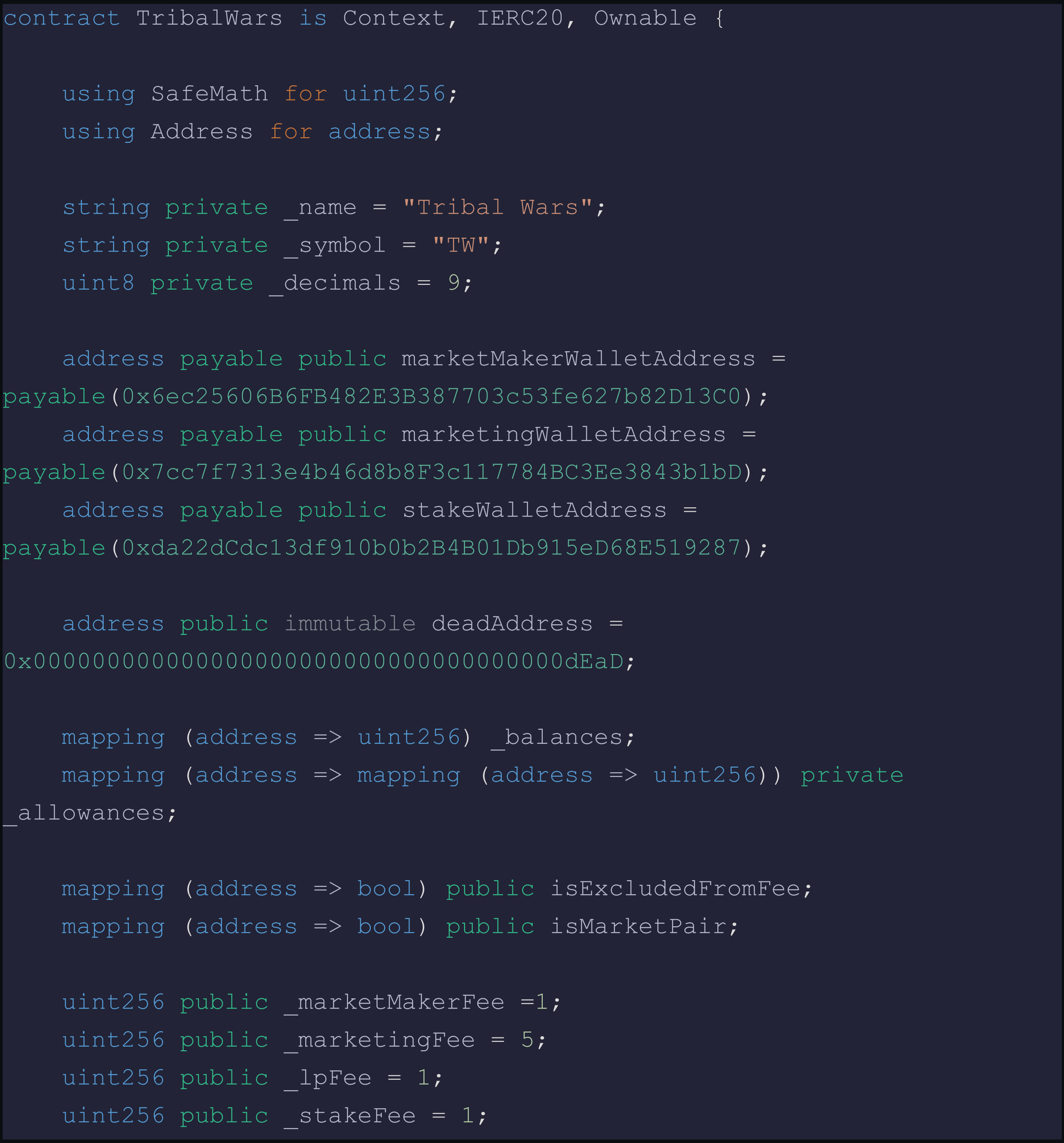
```
function setBuyTaxes(uint256 marketMakerFeeNew, uint256
marketingFeeNew, uint256 lpFeeNew, uint256 stakeFeeNew) external
onlyOwner() {
        _marketMakerFee = marketMakerFeeNew;
        _marketingFee = marketingFeeNew;
        _lpFee = lpFeeNew;
        _stakeFee = stakeFeeNew;
        _totalTax =
_marketMakerFee.add(_marketingFee).add(_lpFee).add(_stakeFee);
    }
```

- Owner can exclude addresses from fees.

- The ownership of the contract isn’t renounced.

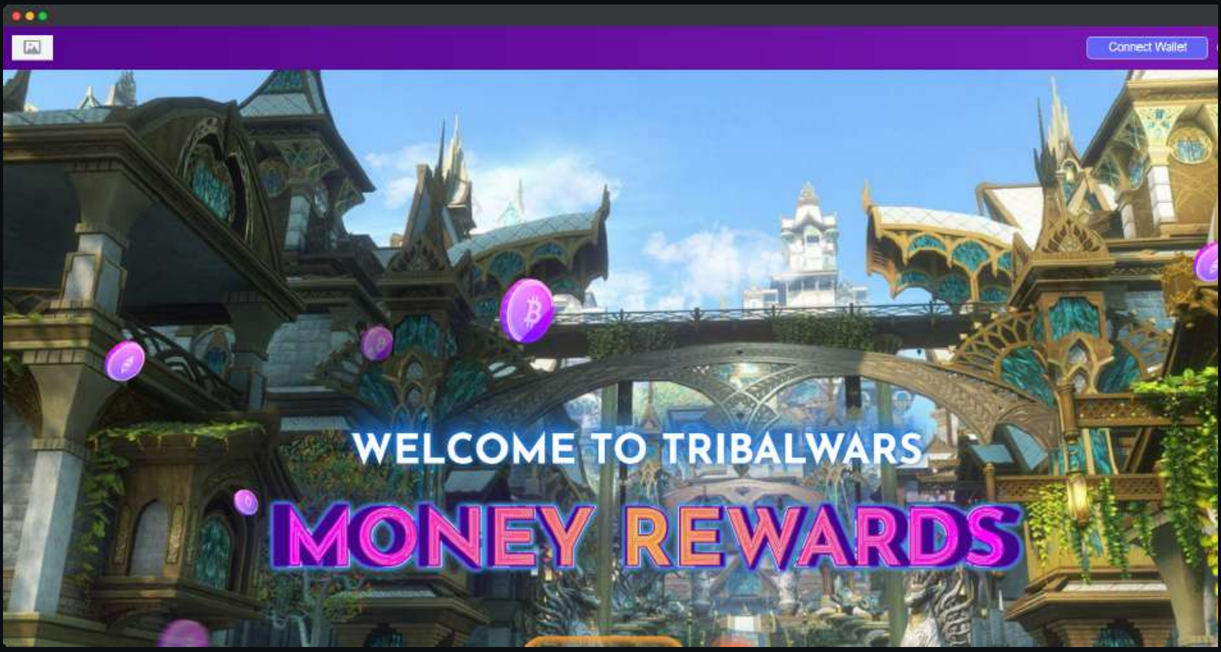
- Owner can pause swap and liquify.

Contract Snapshot



```
contract TribalWars is Context, IERC20, Ownable {

    using SafeMath for uint256;
    using Address for address;

    string private _name = "Tribal Wars";
    string private _symbol = "TW";
    uint8 private _decimals = 9;

    address payable public marketMakerWalletAddress =
payable(0x6ec25606B6FB482E3B387703c53fe627b82D13C0);
    address payable public marketingWalletAddress =
payable(0x7cc7f7313e4b46d8b8F3c117784BC3Ee3843b1bD);
    address payable public stakeWalletAddress =
payable(0xda22dCdc13df910b0b2B4B01Db915eD68E519287);

    address public immutable deadAddress =
0x000000000000000000000000000000000000dEaD;

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

    mapping (address => bool) public isExcludedFromFee;
    mapping (address => bool) public isMarketPair;

    uint256 public _marketMakerFee =1;
    uint256 public _marketingFee = 5;
    uint256 public _lpFee = 1;
    uint256 public _stakeFee = 1;
```

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: 64%

Rug-pull Review

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

🟢 Locked Liquidity

  - Note: Tokens not yet distributed

🟢 Large unlocked wallets

  - Note: Tokens not yet distributed

🟢 Doxxed Team (KYC at pinksale)

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

🔴 Router can be changed

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.