Coinsult

Advanced Manual Smart Contract Audit

Project: Senshi
Website: Senshigame.com

🟢 **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

0xe4a414237e4c3d126f9c9048e1b7364f0a6de26d

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	0xa6567bfb27f0612443a7a19bcf4e179e3a258b86	1,000,000,000	100.00%

Source code

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

https://bscscan.com/address/0xe4a414237e4c3d126f9c9048e1b7364f0a6de26d#code

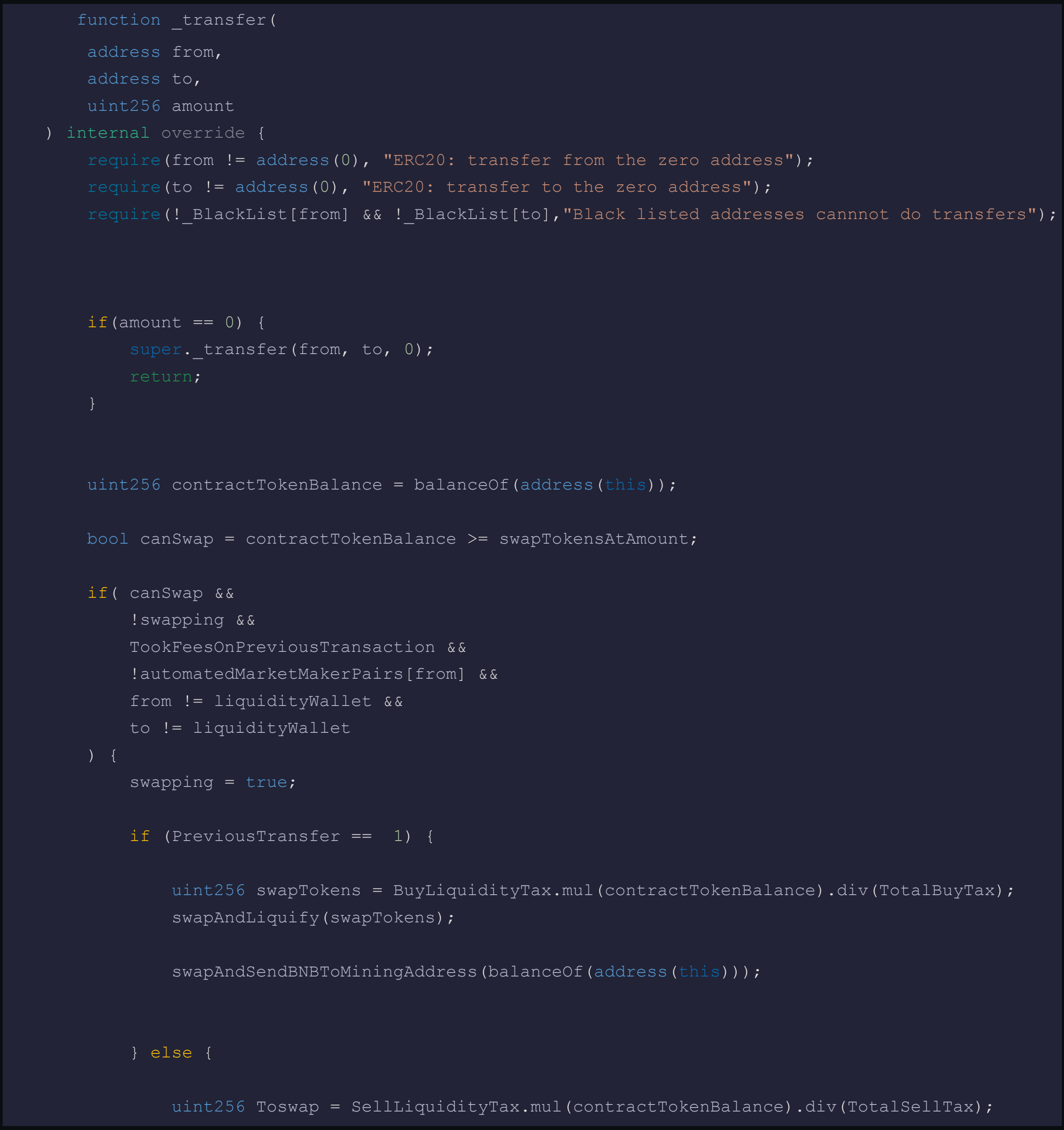
Note: This project uses imports. While we do check the full contract for vulnerabilities at the time of the audit, we can not ensure the correctness of these imported modules.

Manual Code Review

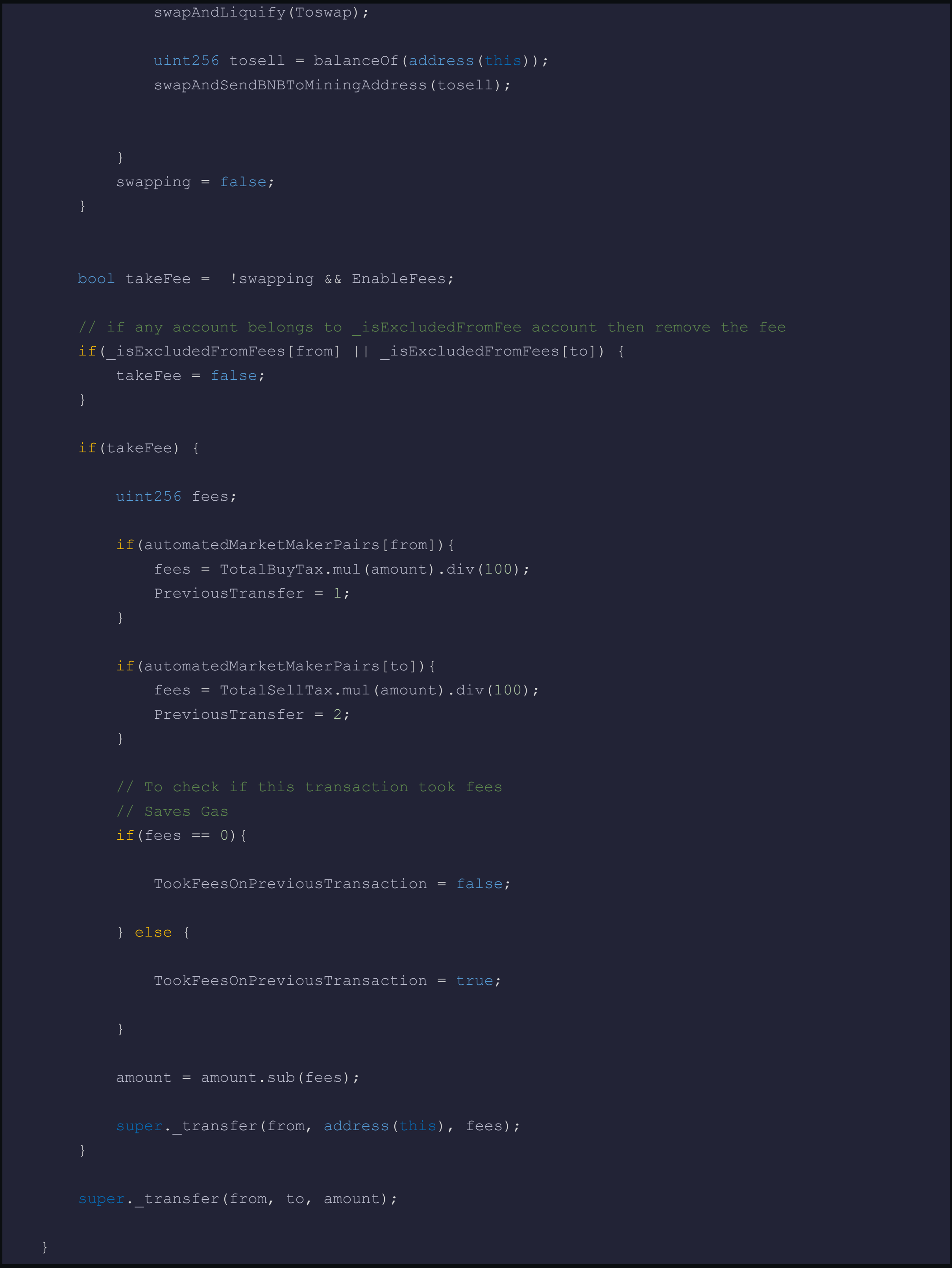
🟢 Low-risk

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 from,
    address to,
    uint256 amount
) internal override {
    require(from != address(0), "ERC20: transfer from the zero address");
    require(to != address(0), "ERC20: transfer to the zero address");
    require(!_BlackList[from] && !_BlackList[to],"Black listed addresses cannnot do transfers");



    if(amount == 0) {
        super._transfer(from, to, 0);
        return;
    }


    uint256 contractTokenBalance = balanceOf(address(this));

    bool canSwap = contractTokenBalance >= swapTokensAtAmount;

    if( canSwap &&
        !swapping &&
        TookFeesOnPreviousTransaction &&
        !automatedMarketMakerPairs[from] &&
        from != liquidityWallet &&
        to != liquidityWallet
    ) {
        swapping = true;

        if (PreviousTransfer ==  1) {

            uint256 swapTokens = BuyLiquidityTax.mul(contractTokenBalance).div(TotalBuyTax);
            swapAndLiquify(swapTokens);

            swapAndSendBNBToMiningAddress(balanceOf(address(this)));


        } else {

            uint256 Toswap = SellLiquidityTax.mul(contractTokenBalance).div(TotalSellTax);
```



```
                swapAndLiquify(Toswap);

                uint256 tosell = balanceOf(address(this));
                swapAndSendBNBToMiningAddress(tosell);


            }
            swapping = false;
        }


        bool takeFee =  !swapping && EnableFees;

        // if any account belongs to _isExcludedFromFee account then remove the fee
        if(_isExcludedFromFees[from] || _isExcludedFromFees[to]) {
            takeFee = false;
        }

        if(takeFee) {

            uint256 fees;

            if(automatedMarketMakerPairs[from]){
                fees = TotalBuyTax.mul(amount).div(100);
                PreviousTransfer = 1;
            }

            if(automatedMarketMakerPairs[to]){
                fees = TotalSellTax.mul(amount).div(100);
                PreviousTransfer = 2;
            }

            // To check if this transaction took fees
            // Saves Gas
            if(fees == 0){

                TookFeesOnPreviousTransaction = false;

            } else {

                TookFeesOnPreviousTransaction = true;

            }

            amount = amount.sub(fees);

            super._transfer(from, address(this), fees);
        }

        super._transfer(from, to, amount);

    }
```

- Avoid relying on block.timestamp

  block.timestamp can be manipulated by miners.

```
function swapTokensForEth(uint256 tokenAmount) internal {


        // generate the uniswap pair path of token -> weth
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = uniswapV2Router.WETH();

        _approve(address(this), address(uniswapV2Router), tokenAmount);

        // make the swap

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            tokenAmount,
            0, // accept any amount of ETH
            path,
            address(this),
            block.timestamp
        );

    }
```

- Literals with many digits are difficult to read and review.

  Recommendation: Use Ether suffix, Time suffix, or The scientific notation

```
_mint(owner(), 1000000000 * (10**18));
```

- Missing zero address validation

  Check that the new address is not the zero address.

```
function SetMiningAddress(address NewAddress) public onlyOwner
returns(bool){
        require(MiningAddress != NewAddress,"Same value");
        MiningAddress = NewAddress;
        return(true);
    }
```

🟡 Medium-risk

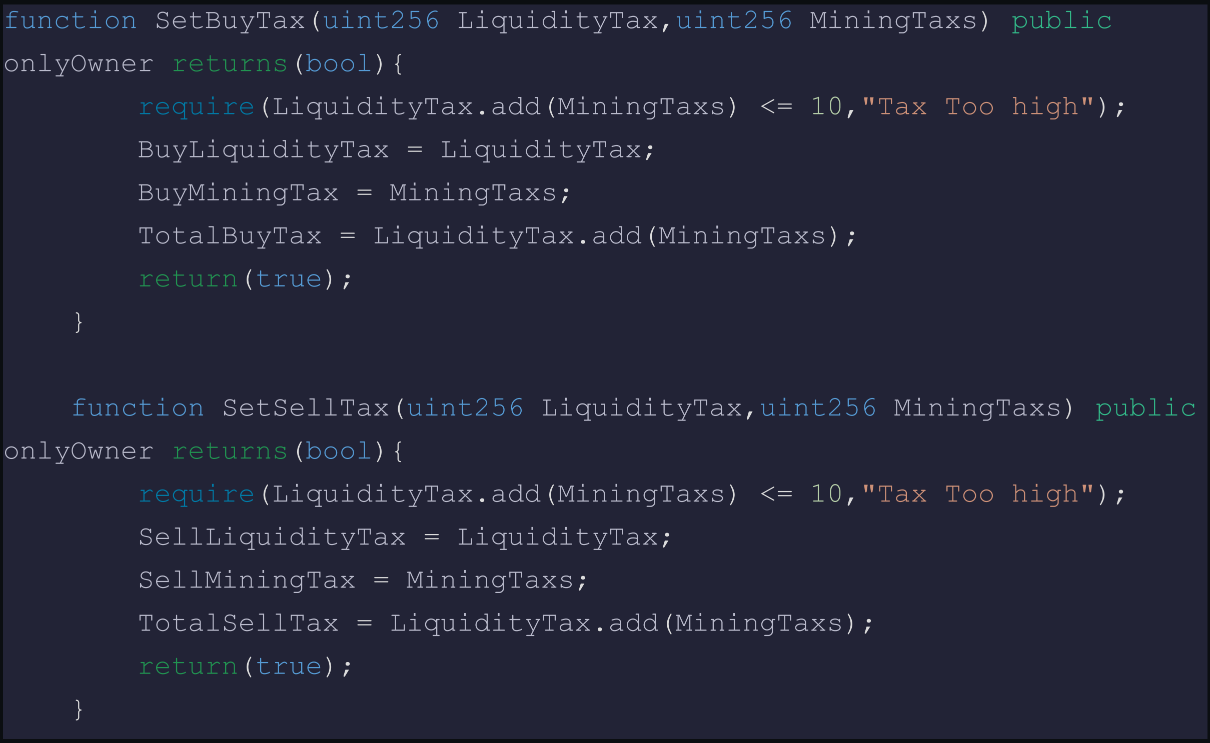
0 medium-risk code issues found.
Should be fixed, could bring problems.

🔴 High-risk

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

Extra notes by the team

🟢 Fees can be set up to 10% for both buy and sell fees.



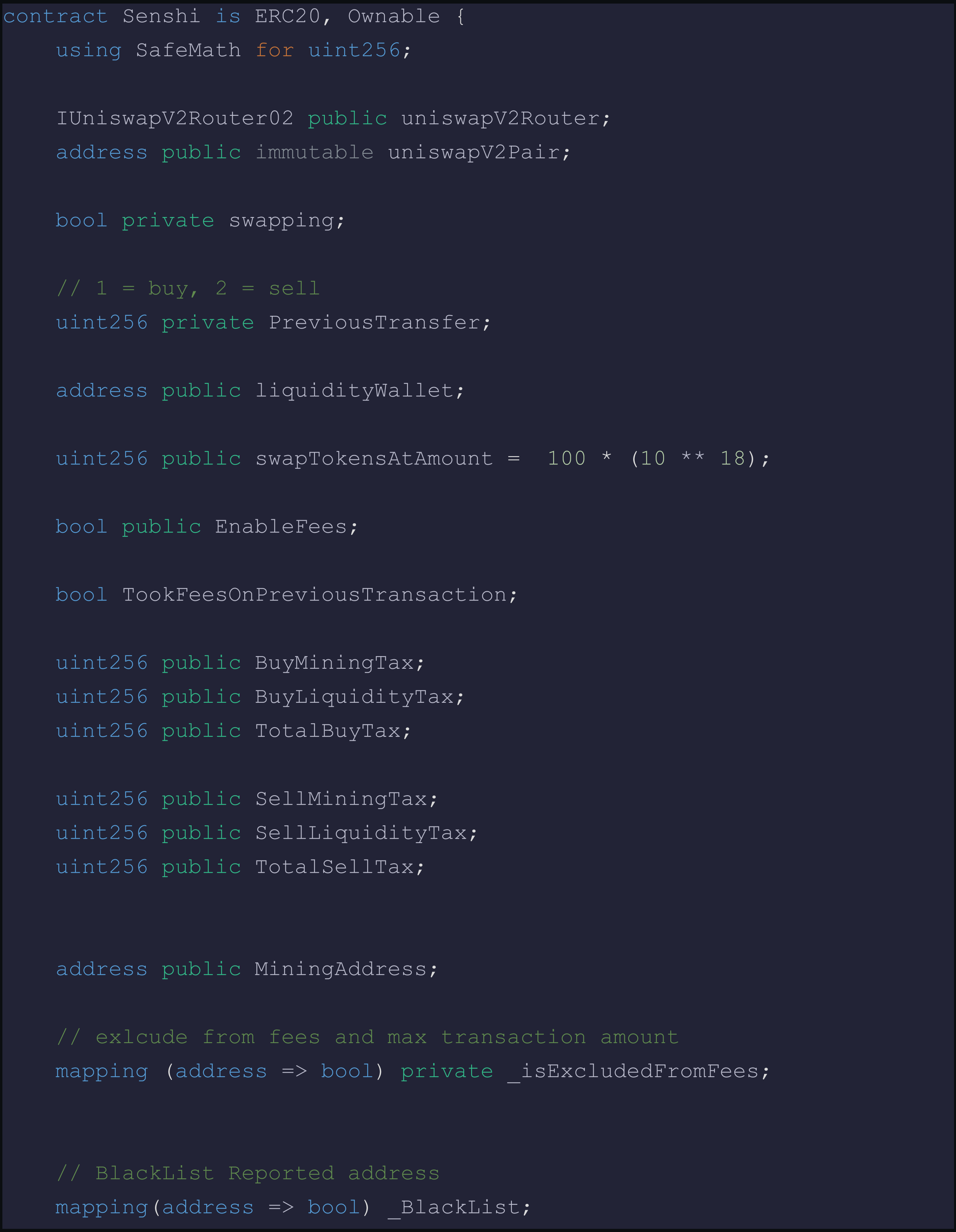
```
function SetBuyTax(uint256 LiquidityTax,uint256 MiningTaxs) public
onlyOwner returns(bool){
        require(LiquidityTax.add(MiningTaxs) <= 10,"Tax Too high");
        BuyLiquidityTax = LiquidityTax;
        BuyMiningTax = MiningTaxs;
        TotalBuyTax = LiquidityTax.add(MiningTaxs);
        return(true);
    }

    function SetSellTax(uint256 LiquidityTax,uint256 MiningTaxs) public
onlyOwner returns(bool){
        require(LiquidityTax.add(MiningTaxs) <= 10,"Tax Too high");
        SellLiquidityTax = LiquidityTax;
        SellMiningTax = MiningTaxs;
        TotalSellTax = LiquidityTax.add(MiningTaxs);
        return(true);
    }
```

🟡 Owner can exclude addresses from fees.

🟡 The ownership of the contract isn’t renounced.

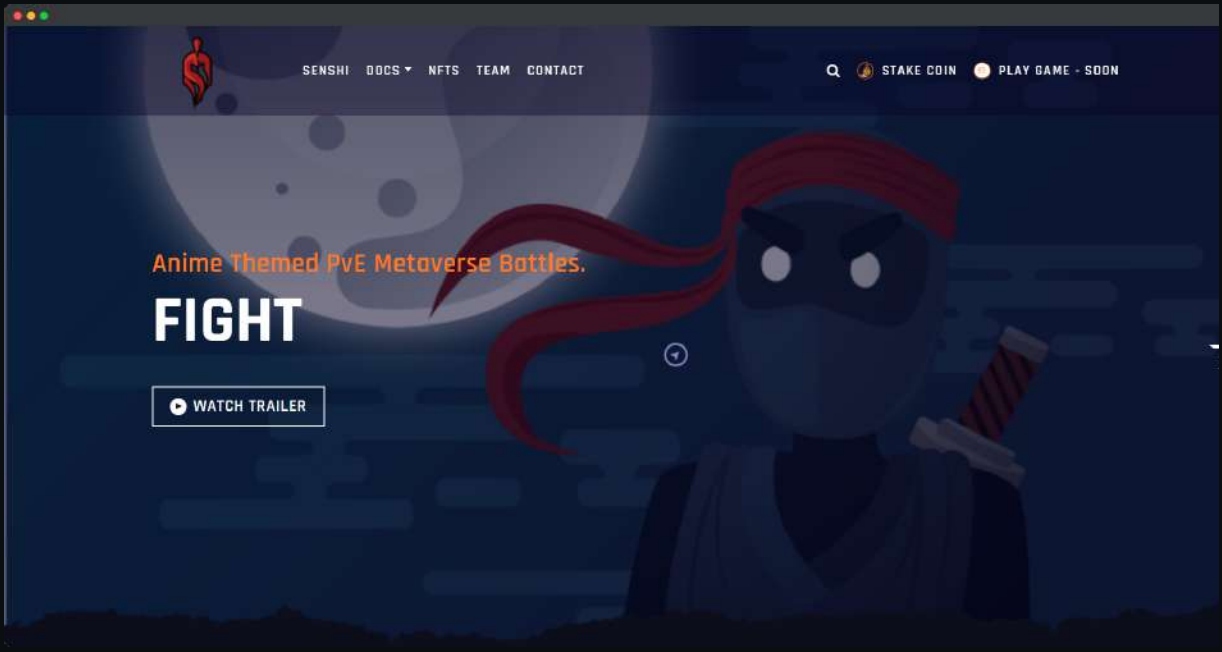
🔴 Owner is able to blacklist addresses

Contract Snapshot



```
contract Senshi is ERC20, Ownable {
    using SafeMath for uint256;

    IUniswapV2Router02 public uniswapV2Router;
    address public immutable uniswapV2Pair;

    bool private swapping;

    // 1 = buy, 2 = sell
    uint256 private PreviousTransfer;

    address public liquidityWallet;

    uint256 public swapTokensAtAmount =  100 * (10 ** 18);

    bool public EnableFees;

    bool TookFeesOnPreviousTransaction;

    uint256 public BuyMiningTax;
    uint256 public BuyLiquidityTax;
    uint256 public TotalBuyTax;

    uint256 public SellMiningTax;
    uint256 public SellLiquidityTax;
    uint256 public TotalSellTax;


    address public MiningAddress;

    // exlcude from fees and max transaction amount
    mapping (address => bool) private _isExcludedFromFees;


    // BlackList Reported address
    mapping(address => bool) _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
🟢 Contains no jQuery errors
🟢 SSL Secured
🟢 No major spelling errors

Loading speed: 65%

Rug-pull Review

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

🟢 Locked Liquidity

🟢 Large unlocked wallets

- Note: Tokens not distributed yet

🟢 Doxxed Team (KYC)

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 cannot 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.